Music of the Primes

In Search of Order

Contents

Articles

References

Article Licenses

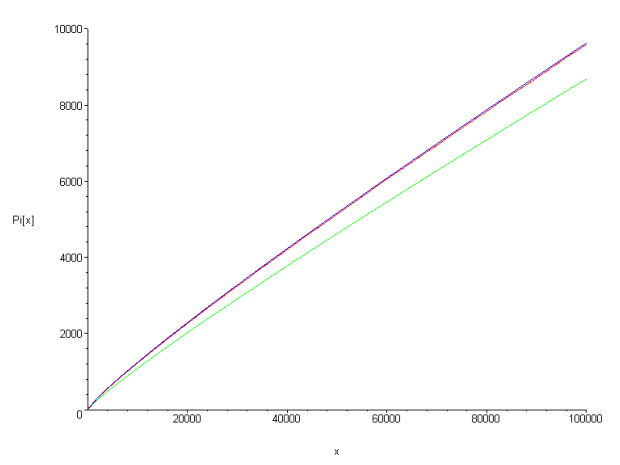
Prime number theorem

In number theory, the **prime number theorem** (**PNT**) describes the asymptotic distribution of the prime numbers. The prime number theorem gives a rough description of how the primes are distributed.

Roughly speaking, the prime number theorem states that if a random number nearby some large number N is selected, the chance of it being prime is about $1 / \ln(N)$, where $\ln(N)$ denotes the natural logarithm of N. For example, near $N = 10{,}000$, about one in nine numbers is prime, whereas near $N = 1{,}000{,}000{,}000$, only one in every 21 numbers is prime. In other words, the average gap between prime numbers near N is roughly $\ln(N)$.[1]

Statement of the theorem

Let $\pi(x)$ be the prime-counting function that gives the number of primes less than or equal to x, for any real number x. For example, $\pi(10) = 4$ because there are four prime numbers (2, 3, 5 and 7) less than or equal to 10. The prime number theorem then states that the limit of the *quotient* of the two functions $\pi(x)$ and $x / \ln(x)$ as x approaches infinity is 1, which is expressed by the formula



Graph comparing $\pi(x)$ (red), $x / \ln x$ (green) and $\mathrm{Li}(x)$ (blue)

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1,$$

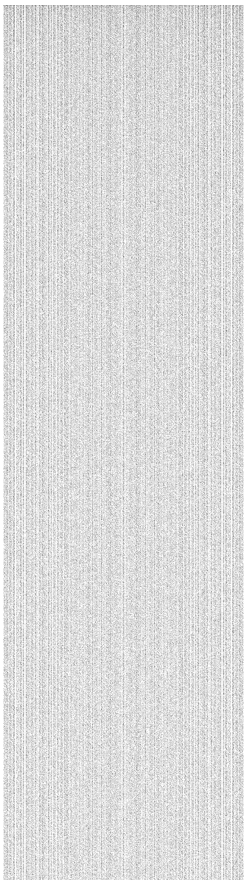
known as **the asymptotic law of distribution of prime numbers**. Using asymptotic notation this result can be restated as

$$\pi(x) \sim \frac{x}{\ln x}.$$

This notation (and the theorem) does *not* say anything about the limit of the *difference* of the two functions as x approaches infinity. (Indeed, the behavior of this difference is very complicated and related to the Riemann hypothesis.) Instead, the theorem states that $x/\ln(x)$ approximates $\pi(x)$ in the sense that the relative error of this approximation approaches 0 as x approaches infinity.

The prime number theorem is equivalent to the statement that the nth prime number p_n is approximately equal to $n \ln(n)$, again with the relative error of this approximation approaching 0 as n approaches infinity.

History of the asymptotic law of distribution of prime numbers and its proof



Distribution of primes up to 19# (9699690).

Based on the tables by Anton Felkel and Jurij Vega, Adrien-Marie Legendre conjectured in 1796 that $\pi(x)$ is approximated by the function $x/(\ln(x)-B)$, where B=1.08... is a constant close to 1. Carl Friedrich Gauss considered the same question and, based on the computational evidence available to him and on some heuristic reasoning, he came up with his own approximating function, the logarithmic integral $\mathrm{li}(x)$, although he did not publish his results. Both Legendre's and Gauss's formulas imply the same conjectured asymptotic equivalence of $\pi(x)$ and $x \,/\, \ln(x)$ stated above, although it turned out that Gauss's approximation is considerably better if one considers the differences instead of quotients.

In two papers from 1848 and 1850, the Russian mathematician Pafnuty L'vovich Chebyshev attempted to prove the asymptotic law of distribution of prime numbers. His work is notable for the use of the zeta function $\zeta(s)$ predating Riemann's celebrated memoir of 1859, and he succeeded in proving a slightly weaker form of the asymptotic law, namely, that if the limit of $\pi(x)/(x/\ln(x))$ as x goes to infinity exists at all, then it is necessarily equal to one.[2] He was able to prove unconditionally that this ratio is bounded above and below by two explicitly given constants near to 1 for all x.[3] Although Chebyshev's paper did not prove the Prime Number Theorem, his estimates for $\pi(x)$ were strong enough for him to prove Bertrand's postulate that there exists a prime number between n and $2n$ for any integer $n \geq 2$.

Without doubt, the single most significant paper concerning the distribution of prime numbers was Riemann's 1859 memoir *On the Number of Primes Less Than a Given Magnitude*, the only paper he ever wrote on the subject. Riemann introduced revolutionary ideas into the subject, the chief of them being that the distribution of prime numbers is intimately connected with the zeros of the analytically extended Riemann zeta function of a complex variable. In particular, it is in this paper of Riemann that the idea to apply methods of complex analysis to the study of the real function $\pi(x)$ originates. Extending these deep ideas of Riemann, two proofs of the asymptotic law of the distribution of prime numbers were obtained independently by Hadamard and de la Vallée Poussin and appeared in the same year (1896). Both proofs used methods from complex analysis, establishing as a main step of the proof that the Riemann zeta function $\zeta(s)$ is non-zero for all complex values of the variable s that have the form $s = 1 + it$ with $t > 0$.[4]

During the 20th century, the theorem of Hadamard and de la Vallée-Poussin also became known as the Prime Number Theorem. Several different proofs of it were found, including the "elementary" proofs of Atle Selberg and Paul Erdős (1949). While the original proofs of Hadamard and de la Vallée-Poussin are long and elaborate, and later proofs have introduced various simplifications through the use of Tauberian theorems but remained difficult to digest, a surprisingly short proof [5] [6] was discovered in 1980 by American mathematician Donald J. Newman. Newman's proof is arguably the simplest known proof of the theorem, although it is non-elementary in the sense that it uses Cauchy's integral theorem from complex analysis.

Proof methodology

In a lecture on prime numbers for a general audience, Fields medalist Terence Tao described one approach to proving the prime number theorem in poetic terms: listening to the "music" of the primes. We start with a "sound wave" that is "noisy" at the prime numbers and silent at other numbers; this is the von Mangoldt function. Then we analyze its notes or frequencies by subjecting it to a process akin to Fourier transform; this is the Mellin transform. Then we prove, and this is the hard part, that certain "notes" cannot occur in this music. This exclusion of certain

notes leads to the statement of the prime number theorem. According to Tao, this proof yields much deeper insights into the distribution of the primes than the "elementary" proofs discussed below.[7]

Proof sketch

Here is a sketch of the proof referred to in Tao's lecture mentioned above. Like most proofs of the PNT, it starts out by reformulating the problem in terms of a less intuitive, but better-behaved, prime-counting function. The idea is to count the primes (or a related set such as the set of prime powers) with *weights* to arrive at a function with smoother asymptotic behavior. The most common such generalized counting function is the Chebyshev function $\psi(x)$, defined by

$$\psi(x) = \sum_{p^k \le x} \log p.$$

Here the summation is over all prime powers up to *x*. This is sometimes written as $\psi(x) = \sum_{n \le x} \Lambda(n)$, where $\Lambda(n)$ is the von Mangoldt function, namely

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \ge 1, \\ 0 & \text{otherwise.} \end{cases}$$

It is now relatively easy to check that the PNT is equivalent to the claim that $\lim_{x \to \infty} \psi(x)/x = 1$. Indeed, this follows from the easy estimates

$$\psi(x) = \sum_{p \le x} \log p \left\lfloor \frac{\log x}{\log p} \right\rfloor \le \sum_{p \le x} \log x = \pi(x) \log x$$

and (using big O notation) for any ε > 0,

$$\psi(x) \ge \sum_{x^{1-\epsilon} \le p \le x} \log p \ge \sum_{x^{1-\epsilon} \le p \le x} (1-\epsilon) \log x = (1-\epsilon)(\pi(x) + O(x^{1-\epsilon})) \log x.$$

The next step is to find a useful representation for $\psi(x)$. Let $\zeta(s)$ be the Riemann zeta function. It can be shown that $\zeta(s)$ is related to the von Mangoldt function $\Lambda(n)$, and hence to $\psi(x)$, via the relation

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \Lambda(n) n^{-s}.$$

A delicate analysis of this equation and related properties of the zeta function, using the Mellin transform and Perron's formula, shows that for non-integer *x* the equation

$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \log(2\pi)$$

holds, where the sum is over all zeros (trivial and non-trivial) of the zeta function. This striking formula is one of the so-called explicit formulas of number theory, and is already suggestive of the result we wish to prove, since the term *x* (claimed to be the correct asymptotic order of $\psi(x)$) appears on the right-hand side, followed by (presumably) lower-order asymptotic terms.

The next step in the proof involves a study of the zeros of the zeta function. The trivial zeros –2, –4, –6, –8, ... can be handled separately:

$$\sum_{n=1}^{\infty} \frac{1}{2n\, x^{2n}} = -\frac{1}{2} \ln\left(1 - \frac{1}{x^2}\right),$$

which vanishes for a large *x*. The nontrivial zeros, namely those on the critical strip $0 \le \Re(s) \le 1$, can potentially be of an asymptotic order comparable to the main term *x* if $\Re(\rho) = 1$, so a crucial fact that needs to be shown is that all zeros have real part strictly less than 1. See Zagier's paper in the references for a short proof of this fact.

Finally, we can conclude that the PNT is "morally" true. To rigorously complete the proof there are still serious technicalities to overcome, due to the fact that the summation over zeta zeros in the explicit formula for $\psi(x)$ does not converge absolutely but only conditionally and in a "principal value" sense. There are several ways around this problem but all of them require rather delicate complex-analytic estimates that are beyond the scope of this article. Edwards's book[8] provides the details.

The prime-counting function in terms of the logarithmic integral

Carl Friedrich Gauss conjectured that an even better approximation to $\pi(x)$ is given by the offset logarithmic integral function $\mathrm{Li}(x)$, defined by

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\ln t}\,\mathrm{d}t = \mathrm{li}(x) - \mathrm{li}(2).$$

Indeed, this integral is strongly suggestive of the notion that the 'density' of primes around t should be $1/\ln t$. This function is related to the logarithm by the asymptotic expansion

$$\mathrm{Li}(x) \sim \frac{x}{\ln x}\sum_{k=0}^{\infty}\frac{k!}{(\ln x)^k} = \frac{x}{\ln x} + \frac{x}{(\ln x)^2} + \frac{2x}{(\ln x)^3} + \cdots.$$

So, the prime number theorem can also be written as $\pi(x) \sim \mathrm{Li}(x)$. In fact, it follows from the proof of Hadamard and de la Vallée Poussin that

$$\pi(x) = \mathrm{Li}(x) + O\left(x\mathrm{e}^{-a\sqrt{\ln x}}\right) \quad \text{as } x \to \infty$$

for some positive constant a, where $O(\ldots)$ is the big O notation. This has been improved to

$$\pi(x) = \mathrm{Li}(x) + O\left(x\,\exp\left(-\frac{A(\ln x)^{3/5}}{(\ln\ln x)^{1/5}}\right)\right).$$

Because of the connection between the Riemann zeta function and $\pi(x)$, the Riemann hypothesis has considerable importance in number theory: if established, it would yield a far better estimate of the error involved in the prime number theorem than is available today. More specifically, Helge von Koch showed in 1901[9] that, if and only if the Riemann hypothesis is true, the error term in the above relation can be improved to

$$\pi(x) = \mathrm{Li}(x) + O\left(\sqrt{x}\ln x\right).$$

The constant involved in the big O notation was estimated in 1976 by Lowell Schoenfeld:[10] assuming the Riemann hypothesis,

$$|\pi(x) - \mathrm{li}(x)| < \frac{\sqrt{x}\,\ln x}{8\pi}$$

for all $x \geq 2657$. He also derived a similar bound for the Chebyshev prime-counting function ψ:

$$|\psi(x) - x| < \frac{\sqrt{x}\,\ln^2 x}{8\pi}$$

for all $x \geq 73.2$.

The logarithmic integral $\mathrm{Li}(x)$ is larger than $\pi(x)$ for "small" values of x. This is because it is (in some sense) counting not primes, but prime powers, where a power p^n of a prime p is counted as $1/n$ of a prime. This suggests that $\mathrm{Li}(x)$ should usually be larger than $\pi(x)$ by roughly $\mathrm{Li}(x^{1/2})/2$, and in particular should usually be larger than $\pi(x)$. However, in 1914, J. E. Littlewood proved that this is not always the case. The first value of x where $\pi(x)$ exceeds $\mathrm{Li}(x)$ is probably around $x = 10^{316}$; see the article on Skewes' number for more details.

Elementary proofs

In the first half of the twentieth century, some mathematicians (notably G. H. Hardy) believed that there exists a hierarchy of proof methods in mathematics depending on what sorts of numbers (integers, reals, complex) a proof requires, and that the prime number theorem (PNT) is a "deep" theorem by virtue of requiring complex analysis.[11] This belief was somewhat shaken by a proof of the PNT based on Wiener's tauberian theorem, though this could be set aside if Wiener's theorem were deemed to have a "depth" equivalent to that of complex variable methods. There is no rigorous and widely accepted definition of the notion of elementary proof in number theory. One definition is "a proof that can be carried out in first order Peano arithmetic." There are theorems of Peano arithmetic (for example, the Paris-Harrington theorem) provable using second order but not first order methods, but such theorems are rare to date.

In 1949, Atle Selberg proved the PNT using only standard number-theoretic techniques.[12] At about the same time, Paul Erdős produced a slightly different elementary proof of the same theorem.[11] These proofs effectively laid to rest the notion that the PNT was "deep," and showed that technically "elementary" methods (in other words Peano arithmetic) were more powerful than had been believed to be the case. In 1994, Charalambos Cornaros and Costas Dimitracopoulos proved the PNT using only $I\Delta_0 + \exp$,[13] a formal system far weaker than Peano arithmetic.

On the history of the elementary proofs of the PNT, including the Erdős–Selberg priority dispute, see Dorian Goldfeld.[11]

Computer proofs

In 2005, Avigad *et al.* employed the Isabelle theorem prover to devise a computer-verified variant of Selberg's proof of the PNT.[14] This was the first machine-verified proof of the PNT. Avigad chose to formalize Selberg's proof rather than an analytic one because while Isabelle's library at the time could implement the notions of limit, derivative, and transcendental function, it had almost no theory of integration to speak of (Avigad et al. p. 19).

In 2009, John Harrison employed HOL Light to formalize a proof employing complex analysis.[15] By developing the necessary analytic machinery, including the Cauchy integral formula, Harrison was able to formalize "a direct, modern and elegant proof instead of the more involved 'elementary' Erdös-Selberg argument."

The prime number theorem for arithmetic progressions

Let $\pi_{n,a}(x)$ denote the number of primes in the arithmetic progression a, $a + n$, $a + 2n$, $a + 3n$, … less than x. Dirichlet and Legendre conjectured, and Vallée-Poussin proved, that, if a and n are coprime, then

$$\pi_{n,a}(x) \sim \frac{1}{\phi(n)}\mathrm{Li}(x),$$

where $\varphi(\cdot)$ is the Euler's totient function. In other words, the primes are distributed evenly among the residue classes $[a]$ modulo n with $\gcd(a, n) = 1$. This can be proved using similar methods used by Newman for his proof of the prime number theorem.[16]

Although we have in particular

$$\pi_{4,1}(x) \sim \pi_{4,3}(x),$$

empirically the primes congruent to 3 are more numerous and are nearly always ahead in this "prime number race"; the first reversal occurs at $x = 26{,}861$.[17] :1–2 However Littlewood showed in 1914[17] :2 that there are infinitely many sign changes for the function

$$\pi_{4,1}(x) - \pi_{4,3}(x),$$

so the lead in the race switches back and forth infinitely many times. The prime number race generalizes to other moduli and is the subject of much research; Granville and Martin give a thorough exposition and survey.[17]

Bounds on the prime-counting function

The prime number theorem is an *asymptotic* result. Hence, it cannot be used to *bound* $\pi(x)$.

However, some bounds on $\pi(x)$ are known, for instance Pierre Dusart's

$$\frac{x}{\ln x}\left(1+\frac{1}{\ln x}\right) < \pi(x) < \frac{x}{\ln x}\left(1+\frac{1}{\ln x}+\frac{2.51}{(\ln x)^2}\right).$$

The first inequality holds for all $x \geq 599$ and the second one for $x \geq 355991$.[18]

A weaker but sometimes useful bound is

$$\frac{x}{\ln x + 2} < \pi(x) < \frac{x}{\ln x - 4}$$

for $x \geq 55$.[19] In Dusart's thesis there are stronger versions of this type of inequality that are valid for larger x.

The proof by de la Vallée-Poussin implies the following. For every $\varepsilon > 0$, there is an S such that for all $x > S$,

$$\frac{x}{\ln x - (1-\varepsilon)} < \pi(x) < \frac{x}{\ln x - (1+\varepsilon)}.$$

Approximations for the *n*th prime number

As a consequence of the prime number theorem, one gets an asymptotic expression for the nth prime number, denoted by p_n:

$$p_n \sim n \ln n.$$

A better approximation is

$$p_n = n\ln n + n\ln\ln n - n + \frac{n}{\ln n}(\ln\ln n - 2) - \frac{n\ln\ln n}{2(\ln n)^2}(\ln\ln n - 6) + O\left(\frac{n}{(\ln n)^2}\right).$$ [20]

Rosser's theorem states that p_n is larger than $n \ln n$. This can be improved by the following pair of bounds:[21] [22]

$$n\ln n + n(\ln\ln n - 1) < p_n < n\ln n + n\ln\ln n \quad \text{for } n \geq 6.$$

Table of $\pi(x)$, x / ln x, and li(x)

The table compares exact values of $\pi(x)$ to the two approximations x / ln x and li(x). The last column, x / $\pi(x)$, is the average prime gap below x.

x	$\pi(x)$[23]	$\pi(x) - x / \ln x$[24]	$\pi(x) / (x / \ln x)$	li(x) − $\pi(x)$[25]	$x / \pi(x)$
10	4	−0.3	0.921	2.2	2.500
10^2	25	3.3	1.151	5.1	4.000
10^3	168	23	1.161	10	5.952
10^4	1,229	143	1.132	17	8.137
10^5	9,592	906	1.104	38	10.425
10^6	78,498	6,116	1.084	130	12.740
10^7	664,579	44,158	1.071	339	15.047
10^8	5,761,455	332,774	1.061	754	17.357
10^9	50,847,534	2,592,592	1.054	1,701	19.667
10^{10}	455,052,511	20,758,029	1.048	3,104	21.975

10^{11}	4,118,054,813	169,923,159	1.043	11,588	24.283
10^{12}	37,607,912,018	1,416,705,193	1.039	38,263	26.590
10^{13}	346,065,536,839	11,992,858,452	1.034	108,971	28.896
10^{14}	3,204,941,750,802	102,838,308,636	1.033	314,890	31.202
10^{15}	29,844,570,422,669	891,604,962,452	1.031	1,052,619	33.507
10^{16}	279,238,341,033,925	7,804,289,844,393	1.029	3,214,632	35.812
10^{17}	2,623,557,157,654,233	68,883,734,693,281	1.027	7,956,589	38.116
10^{18}	24,739,954,287,740,860	612,483,070,893,536	1.025	21,949,555	40.420
10^{19}	234,057,667,276,344,607	5,481,624,169,369,960	1.024	99,877,775	42.725
10^{20}	2,220,819,602,560,918,840	49,347,193,044,659,701	1.023	222,744,644	45.028
10^{21}	21,127,269,486,018,731,928	446,579,871,578,168,707	1.022	597,394,254	47.332
10^{22}	201,467,286,689,315,906,290	4,060,704,006,019,620,994	1.021	1,932,355,208	49.636
10^{23}	1,925,320,391,606,803,968,923	37,083,513,766,578,631,309	1.020	7,250,186,216	51.939

Analogue for irreducible polynomials over a finite field

There is an analogue of the prime number theorem that describes the "distribution" of irreducible polynomials over a finite field; the form it takes is strikingly similar to the case of the classical prime number theorem.

To state it precisely, let $F = \mathrm{GF}(q)$ be the finite field with q elements, for some fixed q, and let N_n be the number of monic *irreducible* polynomials over F whose degree is equal to n. That is, we are looking at polynomials with coefficients chosen from F, which cannot be written as products of polynomials of smaller degree. In this setting, these polynomials play the role of the prime numbers, since all other monic polynomials are built up of products of them. One can then prove that

$$N_n \sim \frac{q^n}{n}.$$

If we make the substitution $x = q^n$, then the right hand side is just

$$\frac{x}{\log_q x},$$

which makes the analogy clearer. Since there are precisely q^n monic polynomials of degree n (including the reducible ones), this can be rephrased as follows: if a monic polynomial of degree n is selected randomly, then the probability of it being irreducible is about $1/n$.

One can even prove an analogue of the Riemann hypothesis, namely that

$$N_n = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

The proofs of these statements are far simpler than in the classical case. It involves a short combinatorial argument, summarised as follows. Every element of the degree n extension of F is a root of some irreducible polynomial whose degree d divides n; by counting these roots in two different ways one establishes that

$$q^n = \sum_{d|n} dN_d,$$

where the sum is over all divisors d of n. Möbius inversion then yields

$$N_n = \frac{1}{n}\sum_{d|n}\mu(n/d)q^d,$$

where μ(k) is the Möbius function. (This formula was known to Gauss.) The main term occurs for $d = n$, and it is not difficult to bound the remaining terms. The "Riemann hypothesis" statement depends on the fact that the largest proper divisor of n can be no larger than $n/2$.

See also

- Abstract analytic number theory for information about generalizations of the theorem.
- Landau prime ideal theorem for a generalization to prime ideals in algebraic number fields.

Notes

[1] Hoffman, Paul (1998). *The Man Who Loved Only Numbers*. Hyperion. p. 227. ISBN 0-7868-8406-1.

[2] N. Costa Pereira (August-September 1985). "A Short Proof of Chebyshev's Theorem" (http://www.jstor.org/stable/2322510). *The American Mathematical Monthly* (The American Mathematical Monthly, Vol. 92, No. 7) **92** (7): 494–495. doi:10.2307/2322510. .

[3] M. Nair (February 1982). "On Chebyshev-Type Inequalities for Primes" (http://www.jstor.org/stable/2320934). *The American Mathematical Monthly* (The American Mathematical Monthly, Vol. 89, No. 2) **89** (2): 126–129. doi:10.2307/2320934. .

[4] Ingham, A.E. (1990). *The Distribution of Prime Numbers*. Cambridge University Press. pp. 2–5. ISBN 0-521-39789-8.

[5] D. J. Newman (1980). "Simple analytic proof of the prime number theorem" (http://jstor.org/stable/2321853). *Amer. Math. Monthly* (The American Mathematical Monthly, Vol. 87, No. 9) **87** (9): 693–696. doi:10.2307/2321853. .

[6] D. Zagier (1997). "Newman's short proof of the prime number theorem" (http://mathdl.maa.org/images/upload_library/22/Chauvenet/Zagier.pdf). *Amer. Math. Monthly* (The American Mathematical Monthly, Vol. 104, No. 8) **104** (8): 705–708. doi:10.2307/2975232. .

[7] Video (http://164.67.141.39:8080/ramgen/specialevents/math/tao/tao-20070117.smil) and slides (http://www.math.ucla.edu/~tao/preprints/Slides/primes.pdf) of Tao's lecture on primes, UCLA January 2007.

[8] Edwards, Harold M. (2001). *Riemann's zeta function*. Courier Dover Publications. ISBN 0-4864-1740-9.

[9] Helge von Koch (December 1901). "Sur la distribution des nombres premiers". *Acta Mathematica* **24** (1): 159–182. doi:10.1007/BF02403071. **(French)**

[10] Schoenfeld, Lowell (1976). "Sharper Bounds for the Chebyshev Functions θ(x) and ψ(x). II" (http://jstor.org/stable/2005976). *Mathematics of Computation* (Mathematics of Computation, Vol. 30, No. 134) **30** (134): 337–360. doi:10.2307/2005976. .

[11] D. Goldfeld The elementary proof of the prime number theorem: an historical perspective (http://www.math.columbia.edu/~goldfeld/ErdosSelbergDispute.pdf).

[12] Baas, Nils A.; Skau, Christian F. (2008). "The lord of the numbers, Atle Selberg. On his life and mathematics" (http://www.ams.org/bull/2008-45-04/S0273-0979-08-01223-8/S0273-0979-08-01223-8.pdf). *Bull. Amer. Math. Soc.* **45**: 617–649. doi:10.1090/S0273-0979-08-01223-8. .

[13] Cornaros, Charalambos; Dimitracopoulos, Costas (1994). "The prime number theorem and fragments of *PA*". *Archive for Mathematical Logic* **33** (4): 265–281. doi:10.1007/BF01270626.

[14] Jeremy Avigad, Kevin Donnelly, David Gray, Paul Raff (2005). "A formally verified proof of the prime number theorem" (http://arxiv.org/abs/cs.AI/0509025). *E-print cs. AI/0509025 in the ArXiv*. .

[15] "Formalizing an analytic proof of the Prime Number Theorem" (http://www.cl.cam.ac.uk/~jrh13/papers/mikefest.html). *Journal of Automated Reasoning*. 2009, volume = 43, pages = 243--261. .

[16] Ivan Soprounov (1998). *A short proof of the Prime Number Theorem for arithmetic progressions* (http://www.math.umass.edu/~isoprou/pdf/primes.pdf). .

[17] Granville, Andrew; Martin, Greg (January 2006). "Prime Number Races" (http://www.dms.umontreal.ca/~andrew/PDF/PrimeRace.pdf). *American Mathematical Monthly* (Washington, DC: Mathematical Association of American) **113** (1): 1–33. doi:10.2307/27641834. ISSN 0002-9890. .

[18] Dusart, Pierre (1998). *Autour de la fonction qui compte le nombre de nombres premiers* (http://www.unilim.fr/laco/theses/1998/T1998_01.html). doctoral thesis for l'Université de Limoges. . **(French)**

[19] Barkley Rosser (January 1941). "Explicit Bounds for Some Functions of Prime Numbers" (http://jstor.org/stable/2371291). *American Journal of Mathematics* (American Journal of Mathematics, Vol. 63, No. 1) **63** (1): 211–232. doi:10.2307/2371291. .

[20] Ernest Cesàro (1894). "Sur une formule empirique de M. Pervouchine" (http://gallica.bnf.fr/ark:/12148/bpt6k30752). *Comptes rendus hebdomadaires des séances de l'Académie des sciences* **119**: 848–849. . **(French)**

[21] Eric Bach, Jeffrey Shallit (1996). *Algorithmic Number Theory*. **1**. MIT Press. p. 233. ISBN 0-262-02405-5.

[22] Pierre Dusart (1999). "The *k*th prime is greater than *k(ln k + ln ln k-1)* for *k*>=2" (http://www.ams.org/mcom/1999-68-225/S0025-5718-99-01037-6/S0025-5718-99-01037-6.pdf). *Mathematics of Computation* **68**: 411–415. .

[23] A006880 (http://en.wikipedia.org/wiki/Oeis:a006880)

[24] A057835 (http://en.wikipedia.org/wiki/Oeis:a057835)

[25] A057752 (http://en.wikipedia.org/wiki/Oeis:a057752)

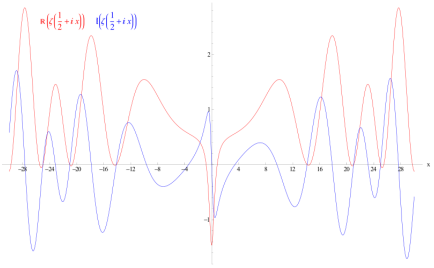
References

- Hardy, G. H.; Littlewood, J. E. (1916). "Contributions to the Theory of the Riemann Zeta-Function and the Theory of the Distribution of Primes". *Acta Mathematica* **41**: 119–196. doi:10.1007/BF02422942.
- Granville, Andrew (1995). "Harald Cramér and the distribution of prime numbers" (http://www.dartmouth.edu/~chance/chance_news/for_chance_news/Riemann/cramer.pdf). *Scandinavian Actuarial Journal* **1**: 12–28.

External links

- Table of Primes by Anton Felkel (http://www.scs.uiuc.edu/~mainzv/exhibitmath/exhibit/felkel.htm).
- Prime formulas (http://mathworld.wolfram.com/PrimeFormulas.html) and Prime number theorem (http://mathworld.wolfram.com/PrimeNumberTheorem.html) at MathWorld.
- Prime number theorem (http://planetmath.org/?op=getobj&from=objects&id=199) on PlanetMath
- How Many Primes Are There? (http://primes.utm.edu/howmany.shtml) and The Gaps between Primes (http://primes.utm.edu/notes/gaps.html) by Chris Caldwell, University of Tennessee at Martin.
- Tables of prime-counting functions (http://www.ieeta.pt/~tos/primes.html) by Tomás Oliveira e Silva

Riemann hypothesis



The real part (red) and imaginary part (blue) of the Riemann zeta function along the critical line Re(s) = 1/2. The first non-trivial zeros can be seen at Im(s) = ±14.135, ±21.022 and ±25.011.

Millennium Prize Problems
P versus NP problem
Hodge conjecture
Poincaré conjecture (solution)
Riemann hypothesis
Yang–Mills existence and mass gap
Navier–Stokes existence and smoothness
Birch and Swinnerton-Dyer conjecture

In mathematics, the **Riemann hypothesis**, proposed by Bernhard Riemann (1859), is a conjecture about the distribution of the zeros of the Riemann zeta function which states that all non-trivial zeros have real part 1/2. The name is also used for some closely related analogues, such as the Riemann hypothesis for curves over finite fields.

The Riemann hypothesis implies results about the distribution of prime numbers that are in some ways as good as possible. Along with suitable generalizations, it is considered by some mathematicians to be the most important unresolved problem in pure mathematics (Bombieri 2000).

The Riemann zeta function $\zeta(s)$ is defined for all complex numbers $s \neq 1$. It has zeros at the negative even integers (i.e. at $s = -2,\ -4,\ -6,\ ...$). These are called the **trivial zeros**. The Riemann hypothesis is concerned with the non-trivial zeros, and states that:

> The real part of any non-trivial zero of the Riemann zeta function is 1/2.

Thus the non-trivial zeros should lie on the **critical line**, $1/2 + it$, where t is a real number and i is the imaginary unit.

The Riemann hypothesis is part of Problem 8, along with the Goldbach conjecture, in Hilbert's list of 23 unsolved problems, and is also one of the Clay Mathematics Institute Millennium Prize Problems. Since it was formulated, it has withstood concentrated efforts from many outstanding mathematicians. In 1973, Pierre Deligne proved that the Riemann hypothesis held true over finite fields. The full version of the hypothesis remains unsolved, although modern computer calculations have shown that the first 10 trillion zeros lie on the critical line.

There are several popular books on the Riemann hypothesis, such as Derbyshire (2003), Rockmore (2005), Sabbagh (2003), du Sautoy (2003). The books Edwards (1974), Patterson (1988) and Borwein et al. (2008) give mathematical introductions, while Titchmarsh (1986), Ivić (1985) and Karatsuba & Voronin (1992) are advanced monographs.

The Riemann zeta function

The Riemann zeta function is given for complex s with real part greater than 1 by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots.$$

Leonhard Euler showed that it is given by the Euler product

$$\zeta(s) = \prod_{p\ \text{prime}} \frac{1}{1 - p^{-s}} = \frac{1}{1 - 2^{-s}} \cdot \frac{1}{1 - 3^{-s}} \cdot \frac{1}{1 - 5^{-s}} \cdot \frac{1}{1 - 7^{-s}} \cdots \frac{1}{1 - p^{-s}} \cdots$$

where the infinite product extends over all prime numbers p, and again converges for complex s with real part greater than 1. The convergence of the Euler product shows that $\zeta(s)$ has no zeros in this region, as none of the factors have zeros.

The Riemann hypothesis discusses zeros outside the region of convergence of this series, so it needs to be analytically continued to all complex s. This can be done by expressing it in terms of the Dirichlet eta function as follows. If s has positive real part, then the zeta function satisfies

$$\left(1 - \frac{2}{2^s}\right)\zeta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s} = \frac{1}{1^s} - \frac{1}{2^s} + \frac{1}{3^s} - \cdots$$

where the series on the right converges whenever s has positive real part. Thus, this alternative series extends the zeta function from $\mathrm{Re}(s) > 1$ to the larger domain $\mathrm{Re}(s) > 0$.

In the strip $0 < \mathrm{Re}(s) < 1$ the zeta function satisfies the functional equation

$$\zeta(s) = 2^s \pi^{s-1}\ \sin\left(\frac{\pi s}{2}\right)\ \Gamma(1 - s)\ \zeta(1 - s).$$

One may then define $\zeta(s)$ for all remaining nonzero complex numbers s by assuming that this equation holds outside the strip as well, and letting $\zeta(s)$ equal the right-hand side of the equation whenever s has non-positive real part. If s is a negative even integer then $\zeta(s) = 0$ because the factor $\sin(\pi s/2)$ vanishes; these are the **trivial zeros** of the zeta function. (If s is a positive even integer this argument does not apply because the zeros of sin are cancelled by the poles of the gamma function.) The value $\zeta(0) = -1/2$ is not determined by the functional equation, but is the limiting value of $\zeta(s)$ as s approaches zero. The functional equation also implies that the zeta function has no zeros with negative real part other than the trivial zeros, so all non-trivial zeros lie in the **critical strip** where s has real part

between 0 and 1.

History

"…es ist sehr wahrscheinlich, dass alle Wurzeln reell sind. Hiervon wäre allerdings ein strenger Beweis zu wünschen; ich habe indess die Aufsuchung desselben nach einigen flüchtigen vergeblichen Versuchen vorläufig bei Seite gelassen, da er für den nächsten Zweck meiner Untersuchung entbehrlich schien."
"…it is very probable that all roots are real. Of course one would wish for a rigorous proof here; I have for the time being, after some fleeting vain attempts, provisionally put aside the search for this, as it appears dispensable for the next objective of my investigation."

Riemann's statement of the Riemann hypothesis, from (Riemann 1859). (He was discussing a version of the zeta function, modified so that its roots are real rather than on the critical line.)

In his 1859 paper *On the Number of Primes Less Than a Given Magnitude* Riemann found an explicit formula for the number of primes $\pi(x)$ less than a given number x. His formula was given in terms of the related function

$$\Pi(x) = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \cdots$$

which counts primes where a prime power p^n counts as $1/n$ of a prime. The number of primes can be recovered from this function by

$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \Pi(x^{1/n}) = \Pi(x) - \frac{1}{2}\Pi(x^{1/2}) - \frac{1}{3}\Pi(x^{1/3}) - \cdots,$$

where μ is the Möbius function. Riemann's formula is then

$$\Pi_0(x) = \mathrm{Li}(x) - \sum_{\rho} \mathrm{Li}(x^{\rho}) - \log(2) + \int_x^{\infty} \frac{dt}{t(t^2-1)\log(t)}$$

where the sum is over the nontrivial zeros of the zeta function and where Π_0 is a slightly modified version of Π that replaces its value at its points of discontinuity by the average of its upper and lower limits:

$$\Pi_0(x) = \lim_{\varepsilon \to 0} \frac{\Pi(x-\varepsilon) + \Pi(x+\varepsilon)}{2}.$$

The summation in Riemann's formula is not absolutely convergent, but may be evaluated by taking the zeros ρ in order of the absolute value of their imaginary part. The function Li occurring in the first term is the (unoffset) logarithmic integral function given by the Cauchy principal value of the divergent integral

$$\mathrm{Li}(x) = \int_0^x \frac{dt}{\log(t)}.$$

The terms $\mathrm{Li}(x^{\rho})$ involving the zeros of the zeta function need some care in their definition as Li has branch points at 0 and 1, and are defined (for $x > 1$) by analytic continuation in the complex variable ρ in the region $\mathrm{Re}(\rho) > 0$, i.e. they should be considered as $\mathrm{Ei}(\rho \ln x)$. The other terms also correspond to zeros: the dominant term $\mathrm{Li}(x)$ comes from the pole at $s = 1$, considered as a zero of multiplicity −1, and the remaining small terms come from the trivial zeros. For some graphs of the sums of the first few terms of this series see Riesel & Göhl (1970) or Zagier (1977).

This formula says that the zeros of the Riemann zeta function control the oscillations of primes around their "expected" positions. Riemann knew that the non-trivial zeros of the zeta function were symmetrically distributed about the line $s = 1/2 + it$, and he knew that all of its non-trivial zeros must lie in the range $0 \le \mathrm{Re}(s) \le 1$. He checked that a few of the zeros lay on the critical line with real part 1/2 and suggested that they all do; this is the Riemann hypothesis.

Consequences of the Riemann hypothesis

The practical uses of the Riemann hypothesis include many propositions which are known to be true under the Riemann hypothesis, and some which can be shown to be equivalent to the Riemann hypothesis.

Distribution of prime numbers

Riemann's explicit formula for the number of primes less than a given number in terms of a sum over the zeros of the Riemann zeta function says that the magnitude of the oscillations of primes around their expected position is controlled by the real parts of the zeros of the zeta function. In particular the error term in the prime number theorem is closely related to the position of the zeros: for example, the supremum of real parts of the zeros is the infimum of numbers β such that the error is $O(x^{\beta})$ (Ingham 1932).

Von Koch (1901) proved that the Riemann hypothesis is equivalent to the "best possible" bound for the error of the prime number theorem.

A precise version of Koch's result, due to Schoenfeld (1976), says that the Riemann hypothesis is equivalent to

$$|\pi(x) - \operatorname{Li}(x)| < \frac{1}{8\pi}\sqrt{x}\,\log(x), \qquad \text{for all } x \geq 2657.$$

Growth of arithmetic functions

The Riemann hypothesis implies strong bounds on the growth of many other arithmetic functions, in addition to the primes counting function above.

One example involves the Möbius function μ. The statement that the equation

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

is valid for every s with real part greater than 1/2, with the sum on the right hand side converging, is equivalent to the Riemann hypothesis. From this we can also conclude that if the Mertens function is defined by

$$M(x) = \sum_{n \leq x} \mu(n)$$

then the claim that

$$M(x) = O(x^{1/2+\varepsilon})$$

for every positive ε is equivalent to the Riemann hypothesis (Titchmarsh 1986). (For the meaning of these symbols, see Big O notation.) The determinant of the order n Redheffer matrix is equal to $M(n)$, so the Riemann hypothesis can also be stated as a condition on the growth of these determinants. The Riemann hypothesis puts a rather tight bound on the growth of M, since Odlyzko & te Riele (1985) disproved the slightly stronger Mertens conjecture

$$|M(x)| \leq \sqrt{x}.$$

The Riemann hypothesis is equivalent to many other conjectures about the rate of growth of other arithmetic functions aside from $\mu(n)$. A typical example is Robin's theorem (Robin 1984), which states that if $\sigma(n)$ is the divisor function, given by

$$\sigma(n) = \sum_{d|n} d$$

then

$$\sigma(n) < e^{\gamma} n \log\log n$$

for all $n > 5040$ if and only if the Riemann hypothesis is true, where γ is the Euler–Mascheroni constant.

Another example was found by Franel & Landau (1924) showing that the Riemann hypothesis is equivalent to a statement that the terms of the Farey sequence are fairly regular. More precisely, if F_n is the Farey sequence of order

n, beginning with $1/n$ and up to $1/1$, then the claim that for all $\varepsilon > 0$

$$\sum_{i=1}^{m} |F_n(i) - i/m| = O(n^{1/2+\epsilon})$$

is equivalent to the Riemann hypothesis. Here $m = \sum_{i=1}^{n} \phi(i)$ is the number of terms in the Farey sequence of order n.

For an example from group theory, if $g(n)$ is Landau's function given by the maximal order of elements of the symmetric group S_n of degree n, then Massias, Nicolas & Robin (1988) showed that the Riemann hypothesis is equivalent to the bound

$$\log g(n) < \sqrt{\mathrm{Li}^{-1}(n)}$$ for all sufficiently large n.

Lindelöf hypothesis and growth of the zeta function

The Riemann hypothesis has various weaker consequences as well; one is the **Lindelöf hypothesis** on the rate of growth of the zeta function on the critical line, which says that, for any $\varepsilon > 0$,

$$\zeta\left(\frac{1}{2} + it\right) = O(t^{\varepsilon}),$$

as t tends to infinity.

The Riemann hypothesis also implies quite sharp bounds for the growth rate of the zeta function in other regions of the critical strip. For example, it implies that

$$e^{\gamma} \leq \limsup_{t\to+\infty} \frac{|\zeta(1+it)|}{\log\log t} \leq 2e^{\gamma}$$

$$\frac{6}{\pi^2} e^{\gamma} \leq \limsup_{t\to+\infty} \frac{1/|\zeta(1+it)|}{\log\log t} \leq \frac{12}{\pi^2} e^{\gamma}$$

so the growth rate of $\zeta(1+it)$ and its inverse would be known up to a factor of 2 (Titchmarsh 1986).

Large prime gap conjecture

The prime number theorem implies that on average, the gap between the prime p and its successor is $\log p$. However, some gaps between primes may be much larger than the average. Cramér proved that, assuming the Riemann hypothesis, every gap is $O(\sqrt{p} \log p)$. This is a case when even the best bound that can currently be proved using the Riemann hypothesis is far weaker than what seems to be true: Cramér's conjecture implies that every gap is $O((\log p)^2)$ which, while larger than the average gap, is far smaller than the bound implied by the Riemann hypothesis. Numerical evidence supports Cramér's conjecture (Nicely 1999).

Criteria equivalent to the Riemann hypothesis

Many statements equivalent to the Riemann hypothesis have been found, though so far none of them have led to much progress in solving it. Some typical examples are as follows.

The Riesz criterion was given by Riesz (1916), to the effect that the bound

$$-\sum_{k=1}^{\infty} \frac{(-x)^k}{(k-1)!\,\zeta(2k)} = O\left(x^{1/4+\epsilon}\right)$$

holds for all $\epsilon > 0$ if and only if the Riemann hypothesis holds.

Nyman (1950) proved that the Riemann Hypothesis is true if and only if the space of functions of the form

$$f(x) = \sum_{\nu=1}^{n} c_\nu \rho(\theta_\nu / x)$$

where $\rho(z)$ is the fractional part of z, $0 \le \theta_\nu \le 1$, and

$$\sum_{\nu=1}^{n} c_\nu \theta_\nu = 0,$$

is dense in the Hilbert space $L^2(0,1)$ of square-integrable functions on the unit interval. Beurling (1955) extended this by showing that the zeta function has no zeros with real part greater than $1/p$ if and only if this function space is dense in $L^p(0,1)$

Salem (1953) showed that the Riemann hypothesis is true if and only if the integral equation

$$\int_0^\infty \frac{z^{-\sigma-1}\phi(z)\,dz}{e^{x/z}+1} = 0$$

has no non-trivial bounded solutions φ for $1/2<\sigma<1$.

Weil's criterion is the statement that the positivity of a certain function is equivalent to the Riemann hypothesis. Related is Li's criterion, a statement that the positivity of a certain sequence of numbers is equivalent to the Riemann hypothesis.

Speiser (1934) proved that the Riemann hypothesis is equivalent to the statement that $\zeta'(s)$, the derivative of $\zeta(s)$, has no zeros in the strip

$$0 < \Re(s) < \frac{1}{2}.$$

That ζ has only simple zeros on the critical line is equivalent to its derivative having no zeros on the critical line.

Consequences of the generalized Riemann hypothesis

Several applications use the generalized Riemann hypothesis for Dirichlet L-series or zeta functions of number fields rather than just the Riemann hypothesis. Many basic properties of the Riemann zeta function can easily be generalized to all Dirichlet L-series, so it is plausible that a method that proves the Riemann hypothesis for the Riemann zeta function would also work for the generalized Riemann hypothesis for Dirichlet L-functions. Several results first proved using the generalized Riemann hypothesis were later given unconditional proofs without using it, though these were usually much harder. Many of the consequences on the following list are taken from Conrad (2010).

- In 1913, Gronwall showed that the generalized Riemann hypothesis implies that Gauss's list of imaginary quadratic fields with class number 1 is complete, though Baker, Stark and Heegner later gave unconditional proofs of this without using the generalized Riemann hypothesis.
- In 1917, Hardy and Littlewood showed that the generalized Riemann hypothesis implies a conjecture of Chebyshev that

  $$\lim_{x\to 1^-} \sum_{p>2} (-1)^{(p+1)/2} x^p = +\infty$$

  which says that in some sense primes 3 mod 4 are more common than primes 1 mod 4.
- In 1923 Hardy and Littlewood showed that the generalized Riemann hypothesis implies a weak form of the Goldbach conjecture for odd numbers: that every sufficiently large odd number is the sum of 3 primes, though in 1937 Vinogradov gave an unconditional proof. In 1997 Deshouillers, Effinger, te Riele, and Zinoviev showed that the generalized Riemann hypothesis implies that every odd number greater than 5 is the sum of 3 primes.
- In 1934, Chowla showed that the generalized Riemann hypothesis implies that the first prime in the arithmetic progression a mod m is at most $Km^2\log(m)^2$ for some fixed constant K.
- In 1967, Hooley showed that the generalized Riemann hypothesis implies Artin's conjecture on primitive roots.
- In 1973, Weinberger showed that the generalized Riemann hypothesis implies that Euler's list of idoneal numbers is complete.

- Weinberger (1973) showed that the generalized Riemann hypothesis for the zeta functions of all algebraic number fields implies that any number field with class number 1 is either Euclidean or an imaginary quadratic number field of discriminant −19, −43, −67, or −163.
- In 1976, G. Miller showed that the generalized Riemann hypothesis implies that one can test if a number is prime in polynomial times. In 2002, Manindra Agrawal, Neeraj Kayal and Nitin Saxena proved this result unconditionally using the AKS primality test.
- Odlyzko (1990) discussed how the generalized Riemann hypothesis can be used to give sharper estimates for discriminants and class numbers of number fields.
- In 1997 Ono and Soundararajan showed that the generalized Riemann hypothesis implies that Ramanujan's integral quadratic form $x^2+y^2+10z^2$ represents all integers that it represents locally, with exactly 18 exceptions.

Generalizations and analogues of the Riemann hypothesis

Dirichlet L-series and other number fields

The Riemann hypothesis can be generalized by replacing the Riemann zeta function by the formally similar, but much more general, global L-functions. In this broader setting, one expects the non-trivial zeros of the global *L*-functions to have real part 1/2. It is these conjectures, rather than the classical Riemann hypothesis only for the single Riemann zeta function, which accounts for the true importance of the Riemann hypothesis in mathematics.

The generalized Riemann hypothesis extends the Riemann hypothesis to all Dirichlet L-functions. In particular it implies the conjecture that Siegel zeros (zeros of *L* functions between 1/2 and 1) do not exist.

The extended Riemann hypothesis extends the Riemann hypothesis to all Dedekind zeta functions of algebraic number fields. The extended Riemann hypothesis for abelian extension of the rationals is equivalent to the generalized Riemann hypothesis. The Riemann hypothesis can also be extended to the L-functions of Hecke characters of number fields.

The grand Riemann hypothesis extends it to all automorphic zeta functions, such as Mellin transforms of Hecke eigenforms.

Function fields and zeta functions of varieties over finite fields

Artin (1924) introduced global zeta functions of (quadratic) function fields and conjectured an analogue of the Riemann hypothesis for them, which has been proven by Hasse in the genus 1 case and by Weil (1948) in general. For instance, the fact that the Gauss sum, of the quadratic character of a finite field of size q (with q odd), has absolute value

$$\sqrt{q}$$

is actually an instance of the Riemann hypothesis in the function field setting. This led Weil (1949) to conjecture a similar statement for all algebraic varieties; the resulting Weil conjectures were proven by Pierre Deligne (1974, 1980).

Selberg zeta functions

Selberg (1956) introduced the Selberg zeta function of a Riemann surface. These are similar to the Riemann zeta function: they have a functional equation, and an infinite product similar to the Euler product but taken over closed geodesics rather than primes. The Selberg trace formula is the analogue for these functions of the explicit formulas in prime number theory. Selberg proved that the Selberg zeta functions satisfy the analogue of the Riemann hypothesis, with the imaginary parts of their zeros related to the eigenvalues of the Laplacian operator of the Riemann surface.

Ihara zeta functions

The Ihara zeta function of a finite graph is an analogue of the Selberg zeta function introduced by Yasutaka Ihara. A regular finite graph is a Ramanujan graph, a mathematical model of efficient communication networks, if and only if its Ihara zeta function satisfies the analogue of the Riemann hypothesis as was pointed out by T. Sunada.

Montgomery's pair correlation conjecture

Montgomery (1973) suggested the pair correlation conjecture that the correlation functions of the (suitably normalized) zeros of the zeta function should be the same as those of the eigenvalues of a random hermitian matrix. Odlyzko (1987) showed that this is supported by large scale numerical calculations of these correlation functions.

Montgomery showed that (assuming the Riemann hypothesis) at least 2/3 of all zeros are simple, and a related conjecture is that all zeros of the zeta function are simple (or more generally have no non-trivial integer linear relations between their imaginary parts). Dedekind zeta functions of algebraic number fields, which generalize the Riemann zeta function, often do have multiple complex zeros. This is because the Dedekind zeta functions factorize as a product of powers of Artin L-functions, so zeros of Artin L-functions sometimes give rise to multiple zeros of Dedekind zeta functions. Other examples of zeta functions with multiple zeros are the L-functions of some elliptic curves: these can have multiple zeros at the real point of their critical line; the Birch-Swinnerton-Dyer conjecture predicts that the multiplicity of this zero is the rank of the elliptic curve.

Other zeta functions

There are many other examples of zeta functions with analogues of the Riemann hypothesis, some of which have been proved. Goss zeta functions of function fields have a Riemann hypothesis, proved by Sheats (1998). The main conjecture of Iwasawa theory, proved by Barry Mazur and Andrew Wiles for cyclotomic fields, and Wiles for totally real fields, identifies the zeros of a *p*-adic *L*-function with the eigenvalues of an operator, so can be thought of as an analogue of the Hilbert–Pólya conjecture for *p*-adic *L*-functions (Wiles 2000).

Attempts to prove the Riemann hypothesis

Several mathematicians have addressed the Riemann hypothesis, but none of their attempts have yet been accepted as correct solutions. Watkins (2007) lists some incorrect solutions, and more are frequently announced [1].

Operator theory

Hilbert and Polya suggested that one way to derive the Riemann hypothesis would be to find a self-adjoint operator, from the existence of which the statement on the real parts of the zeros of $\zeta(s)$ would follow when one applies the criterion on real eigenvalues. Some support for this idea comes from several analogues of the Riemann zeta functions whose zeros correspond to eigenvalues of some operator: the zeros of a zeta function of a variety over a finite field correspond to eigenvalues of a Frobenius element on an etale cohomology group, the zeros of a Selberg zeta function are eigenvalues of a Laplacian operator of a Riemann surface, and the zeros of a p-adic zeta function correspond to eigenvectors of a Galois action on ideal class groups.

Odlyzko (1987) showed that the distribution of the zeros of the Riemann zeta function shares some statistical properties with the eigenvalues of random matrices drawn from the Gaussian unitary ensemble. This gives some support to the Hilbert–Pólya conjecture.

In 1999, Michael Berry and Jon Keating conjectured that there is some unknown quantization $\hat{H}$ of the classical Hamiltonian $H = xp$ so that

$$\zeta(1/2 + i\hat{H}) = 0$$

and even more strongly, that the Riemann zeros coincide with the spectrum of the operator $1/2 + i\hat{H}$. This is to be contrasted to canonical quantization which leads to the Heisenberg uncertainty principle $[x, p] = 1/2$ and the natural numbers as spectrum of the quantum harmonic oscillator. The crucial point is that the Hamiltonian should be a self-adjoint operator so that the quantization would be a realization of the Hilbert–Pólya program. In a connection with this Quantum mechanical problem Berry and Connes had proposed that the inverse of the potential of the Hamiltonian is connected to the half-derivative of the function $N(s) = \frac{1}{\pi} Arg\xi(1/2 + is)$ then, in Berry-Connes approach $V^{-1}(x) = \sqrt{(4\pi)} \frac{d^{1/2}N(x)}{dx^{1/2}}$ (Connes 1999).

The analogy with the Riemann hypothesis over finite fields suggests that the Hilbert space containing eigenvectors corresponding to the zeros might be some sort of first cohomology group of the spectrum Spec(**Z**) of the integers. Deninger (1998) described some of the attempts to find such a cohomology theory.

Zagier (1983) constructed a natural space of invariant functions on the upper half plane which has eigenvalues under the Laplacian operator corresponding to zeros of the Riemann zeta function, and remarked that in the unlikely event that one could show the existence of a suitable positive definite inner product on this space the Riemann hypothesis would follow. Cartier (1982) discussed a related example, where due to a bizarre bug a computer program listed zeros of the Riemann zeta function as eigenvalues of the same Laplacian operator.

Lee–Yang theorem

The Lee–Yang theorem states that the zeros of certain partition functions in statistical mechanics all lie on a "critical line" with real part 0, and this has led to some speculation about a relationship with the Riemann hypothesis (Knauf 1999).

Turán's result

Pál Turán (1948) showed that if the functions

$$\sum_{n=1}^{N} n^{-s}$$

have no zeros when the real part of s is greater than one then

$$T(x) = \sum_{n \le x} \frac{\lambda(n)}{n} \ge 0 \text{ for all } x > 0,$$

where $\lambda(n)$ is the Liouville function given by $(-1)^r$ if n has r prime factors. He showed that this in turn would imply that the Riemann hypothesis is true. However Haselgrove (1958) proved that $T(x)$ is negative for infinitely many x (and also disproved the closely related Polya conjecture), and Borwein, Ferguson & Mossinghoff (2008) showed that the smallest such x is 72185376951205. Spira (1968) showed by numerical calculation that the finite Dirichlet series above for N=19 has a zero with real part greater than 1. Turán also showed that a somewhat weaker assumption, the nonexistence of zeros with real part greater than $1+N^{-1/2+\varepsilon}$ for large N in the finite Dirichlet series above, would also imply the Riemann hypothesis, but Montgomery (1983) showed that for all sufficiently large N these series have zeros with real part greater than 1 + (log log N)/(4 log N). Therefore, Turán's result is vacuously true and cannot be used to help prove the Riemann hypothesis.

Noncommutative geometry

Connes (1999, 2000) has described a relationship between the Riemann hypothesis and noncommutative geometry, and shows that a suitable analogue of the Selberg trace formula for the action of the idèle class group on the adèle class space would imply the Riemann hypothesis. Some of these ideas are elaborated in Lapidus (2008).

Hilbert spaces of entire functions

Louis de Branges (1992) showed that the Riemann hypothesis would follow from a positivity condition on a certain Hilbert space of entire functions. However Conrey & Li (2000) showed that the necessary positivity conditions are not satisfied.

Quasicrystals

The Riemann hypothesis implies that the zeros of the zeta function form a quasicrystal, meaning a distribution with discrete support whose Fourier transform also has discrete support. Dyson (2009) suggested trying to prove the Riemann hypothesis by classifying, or at least studying, 1-dimensional quasicrystals.

Multiple zeta functions

Deligne's proof of the Riemann hypothesis over finite fields used the zeta functions of product varieties, whose zeros and poles correspond to sums of zeros and poles of the original zeta function, in order to bound the real parts of the zeros of the original zeta function. By analogy, Kurokawa (1992) introduced multiple zeta functions whose zeros and poles correspond to sums of zeros and poles of the Riemann zeta function. To make the series converge he restricted to sums of zeros or poles all with non-negative imaginary part. So far, the known bounds on the zeros and poles of the multiple zeta functions are not strong enough to give useful estimates for the zeros of the Riemann zeta function.

Location of the zeros

Number of zeros

The functional equation combined with the argument principle implies that the number of zeros of the zeta function with imaginary part between 0 and T is given by

$$N(T) = \frac{1}{\pi}\mathrm{Arg}(\xi(s)) = \frac{1}{\pi}\mathrm{Arg}(\Gamma(s/2)\pi^{-s/2}\zeta(s)s(s-1)/2)$$

for s=1/2+iT, where the argument is defined by varying it continuously along the line with Im(s)=T, starting with argument 0 at ∞+iT. This is the sum of a large but well understood term

$$\frac{1}{\pi}\mathrm{Arg}(\Gamma(s/2)\pi^{-s/2}s(s-1)/2) = \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + 7/8 + O(1/T)$$

and a small but rather mysterious term

$$S(T) = \frac{1}{\pi}\mathrm{Arg}(\zeta(1/2+iT)) = O(\log(T)).$$

So the density of zeros with imaginary part near T is about $\log(T)/2\pi$, and the function S describes the small deviations from this. The function $S(t)$ jumps by 1 at each zero of the zeta function, and for $t \geq 8$ it decreases monotonically between zeros with derivative close to $-\log t$.

Selberg (1946) showed that the average moments of even powers of S are given by

$$\int_0^T |S(t)|^{2k}dt = \frac{(2k)!}{k!(2\pi)^{2k}}T(\log\log T)^k + O(T(\log\log T)^{k-1/2}).$$

This suggests that $S(T)/(\log\log T)^{1/2}$ resembles a Gaussian random variable with mean 0 and variance $2\pi^2$ (Ghosh (1983) proved this fact). In particular $|S(T)|$ is usually somewhere around $(\log\log T)^{1/2}$, but occasionally much

larger. The exact order of growth of $S(T)$ is not known. There has been no unconditional improvement to Riemann's original bound $S(T)$=O(log T), though the Riemann hypothesis implies the slightly smaller bound $S(T)$=O(log T/log log T) (Titchmarsh 1985). The true order of magnitude may be somewhat less than this, as random functions with the same distribution as $S(T)$ tend to have growth of order about $\log(T)^{1/2}$. In the other direction it cannot be too small: Selberg (1946) showed that $S(T) \neq o((\log T)^{1/3}/(\log \log T)^{7/3})$, and assuming the Riemann hypothesis Montgomery showed that $S(T) \neq o((\log T)^{1/2}/(\log \log T)^{1/2})$.

Numerical calculations confirm that S grows very slowly: $|S(T)| < 1$ for $T < 280$, $|S(T)| < 2$ for $T < 6800000$, and the largest value of $|S(T)|$ found so far is not much larger than 3 (Odlyzko 2002).

Riemann's estimate $S(T) = O(\log T)$ implies that the gaps between zeros are bounded, and Littlewood improved this slightly, showing that the gaps between their imaginary parts tends to 0.

The theorem of Hadamard and de la Vallée-Poussin

Hadamard (1896) and de la Vallée-Poussin (1896) independently proved that no zeros could lie on the line $\mathrm{Re}(s) = 1$. Together with the functional equation and the fact that there are no zeros with real part greater than 1, this showed that all non-trivial zeros must lie in the interior of the critical strip $0 < \mathrm{Re}(s) < 1$. This was a key step in their first proofs of the prime number theorem.

Both the original proofs that the zeta function has no zeros with real part 1 are similar, and depend on showing that if $\zeta(1+it)$ vanishes, then $\zeta(1+2it)$ is singular, which is not possible. One way of doing this is by using the inequality

$$|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)| \geq 1 \text{ for } \sigma>1, t \text{ real},$$

and looking at the limit as σ tends to 1. This inequality follows by taking the real part of the log of the Euler product to see that

$$|\zeta(\sigma+it)| = \exp \Re \sum_{p^n} \frac{p^{-n(\sigma+it)}}{n} = \exp \sum_{p^n} \frac{p^{-n\sigma}\cos(t\log p^n)}{n}$$

(where the sum is over all prime powers p^n) so that

$$|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)| = \exp \sum_{p^n} p^{-n\sigma} \frac{3+4\cos(t\log p^n)+\cos(2t\log p^n)}{n}$$

which is at least 1 because all the terms in the sum are positive, due to the inequality

$$3+4\cos(\theta)+\cos(2\theta) = 2(1+\cos(\theta))^2 \geq 0.$$

Zero-free regions

De la Vallée-Poussin (1899-1900) proved that if $\sigma+it$ is a zero of the Riemann zeta function, then $1-\sigma \geq C/\log(t)$ for some positive constant C. In other words zeros cannot be too close to the line σ=1: there is a zero-free region close to this line. This zero-free region has been enlarged by several authors. Ford (2002) gave a version with explicit numerical constants: $\zeta(\sigma + it) \neq 0$ whenever $|t| \geq 3$ and

$$\sigma \geq 1 - \frac{1}{57.54(\log|t|)^{2/3}(\log\log|t|)^{1/3}}.$$

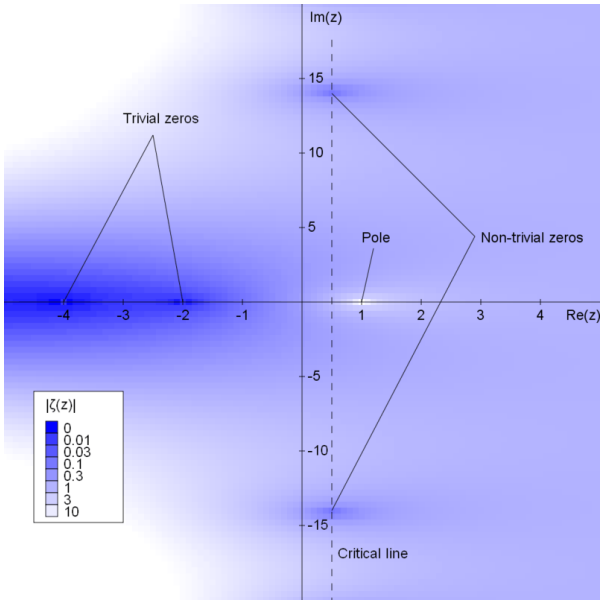
Zeros on the critical line

Hardy (1914) and Hardy & Littlewood (1921) showed there are infinitely many zeros on the critical line, by considering moments of certain functions related to the zeta function. Selberg (1942) proved that at least a (small) positive proportion of zeros lie on the line. Levinson (1974) improved this to one-third of the zeros by relating the zeros of the zeta function to those of its derivative, and Conrey (1989) improved this further to two-fifths.

Most zeros lie close to the critical line. More precisely, Bohr & Landau (1914) showed that for any positive ε, all but an infinitely small proportion of zeros lie within a distance ε of the critical line. Ivić (1985) gives several more precise versions of this result, called **zero density estimates**, which bound the number of zeros in regions with imaginary part at most *T* and real part at least 1/2+ε.

Numerical calculations

The function



Absolute value of the ξ-function

$$\pi^{-s/2}\Gamma(s/2)\zeta(s)$$

has the same zeros as the zeta function in the critical strip, and is real on the critical line because of the functional equation, so one can prove the existence of zeros exactly on the real line between two points by checking numerically that the function has opposite signs at these points. Usually one writes

$$\zeta(1/2+it) = Z(t)e^{-i\pi\theta(t)}$$

where Hardy's function *Z* and the Riemann-Siegel theta function θ are uniquely defined by this and the condition that they are smooth real functions with θ(0)=0. By finding many intervals where the function *Z* changes sign one can show that there are many zeros on the critical line. To verify the Riemann hypothesis up to a given imaginary part *T* of the zeros, one also has to check that there are no further zeros off the line in this region. This can be done by calculating the total number of zeros in the region and checking that it is the same as the number of zeros found on the line. This allows one to verify the Riemann hypothesis computationally up to any desired value of *T* (provided all the zeros of the zeta function in this region are simple and on the critical line).

Some calculations of zeros of the zeta function are listed below. So far all zeros that have been checked are on the critical line and are simple. (A multiple zero would cause problems for the zero finding algorithms, which depend on finding sign changes between zeros.) For tables of the zeros, see Haselgrove & Miller (1960) or Odlyzko.

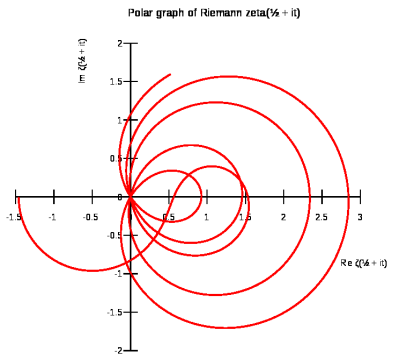
Year	Number of zeros	Author
1859?	3	B. Riemann used the Riemann-Siegel formula (unpublished, but reported in Siegel 1932).
1903	15	J. P. Gram (1903) used Euler-Maclaurin summation and discovered Gram's law. He showed that all 10 zeros with imaginary part at most 50 range lie on the critical line with real part 1/2 by computing the sum of the inverse 10th powers of the roots he found.
1914	79 ($\gamma_n \le 200$)	R. J. Backlund (1914) introduced a better method of checking all the zeros up to that point are on the line, by studying the argument $S(T)$ of the zeta function.
1925	138 ($\gamma_n \le 300$)	J. I. Hutchinson (1925) found the first failure of Gram's law, at the Gram point g_{126}.
1935	195	E. C. Titchmarsh (1935) used the recently rediscovered Riemann-Siegel formula, which is much faster than Euler-Maclaurin summation.It takes about $O(T^{3/2+\varepsilon})$ steps to check zeros with imaginary part less than T, while the Euler-Maclaurin method takes about $O(T^{2+\varepsilon})$ steps.
1936	1041	E. C. Titchmarsh (1936) and L. J. Comrie were the last to find zeros by hand.
1953	1104	A. M. Turing (1953) found a more efficient way to check that all zeros up to some point are accounted for by the zeros on the line, by checking that Z has the correct sign at several consecutive Gram points and using the fact that $S(T)$ has average value 0. This requires almost no extra work because the sign of Z at Gram points is already known from finding the zeros, and is still the usual method used. This was the first use of a digital computer to calculate the zeros.
1956	15000	D. H. Lehmer (1956) discovered a few cases where the zeta function has zeros that are "only just" on the line: two zeros of the zeta function are so close together that it is unusually difficult to find a sign change between them. This is called "Lehmer's phenomenon", and first occurs at the zeros with imaginary parts 7005.063 and 7005.101, which differ by only .04 while the average gap between other zeros near this point is about 1.
1956	25000	D. H. Lehmer
1958	35337	N. A. Meller
1966	250000	R. S. Lehman
1968	3500000	Rosser, Yohe & Schoenfeld (1969) stated Rosser's rule (described below).
1977	40000000	R. P. Brent
1979	81000001	R. P. Brent
1982	200000001	R. P. Brent, J. van de Lune, H. J. J. te Riele, D. T. Winter
1983	300000001	J. van de Lune, H. J. J. te Riele
1986	1500000001	van de Lune, te Riele & Winter (1986) gave some statistical data about the zeros and give several graphs of Z at places where it has unusual behavior.
1987	A few of large height	A. M. Odlyzko (1987) computed smaller numbers of zeros of much larger height, around 10^{12}, to high precision to check Montgomery's pair correlation conjecture.
1992	A few of large height	A. M. Odlyzko (1992) computed a few zeros of heights up to 10^{20}, and gave an extensive discussion of the results.
2001	10000000000	J. van de Lune (unpublished)
2004	900000000000	S. Wedeniwski (ZetaGrid distributed computing)
2004	10000000000000	X. Gourdon (2004) and Patrick Demichel used the Odlyzko–Schönhage algorithm. They also checked a few zeros of much larger height.

Gram points

A Gram point is a value of t such that $\zeta(1/2 + it) = Z(t)e^{-i\theta(t)}$ is a non-zero real; these are easy to find because they are the points where the Euler factor at infinity $\pi^{-s/2}\Gamma(s/2)$ is real at $s = 1/2 + it$, or equivalently $\theta(t)$ is a multiple $n\pi$ of π. They are usually numbered as g_n for $n = -1, 0, 1, ...$, where g_n is the unique solution of $\theta(t) = n\pi$ with $t \geq 8$ (θ is increasing beyond this point; there is a second point with $\theta(t) = -\pi$ near 3.4, and $\theta(0) = 0$). Gram observed that there was often exactly one zero of the zeta function between any two Gram points; Hutchinson called this observation **Gram's law**. There are several other closely related statements that are also sometimes called Gram's law: for example, $(-1)^n Z(g_n)$ is usually positive, or $Z(t)$ usually has opposite sign at consecutive Gram points. The imaginary parts γ_n of the first few zeros (in blue) and the first few Gram points g_n are given in the following table

		g_{-1}	γ_1	g_0	γ_2	g_1	γ_3	g_2	γ_4	g_3	γ_5	g_4	γ_6	g_5
0	3.4	9.667	14.135	17.846	21.022	23.170	25.011	27.670	30.425	31.718	32.935	35.467	37.586	38.999

The first failure of Gram's law occurs at the 127'th zero and the Gram point g_{126}, which are in the "wrong" order.



This shows the values of ζ(1/2+it) in the complex plane for 0 ≤ t ≤ 34. (For t=0, ζ(1/2) ≈ -1.460 corresponds to the leftmost point of the red curve.) Gram's law states that the curve usually crosses the real axis once between zeros.

g_{124}	γ_{126}	g_{125}	g_{126}	γ_{127}	γ_{128}	g_{127}	γ_{129}	g_{128}
279.148	279.229	280.802	282.455	**282.465**	283.211	284.104	284.836	285.752

A Gram point t is called good if the zeta function is positive at $1/2 + it$. The indices of the "bad" Gram points where Z has the "wrong" sign are 126, 134, 195, 211,... (sequence A114856 [2] in OEIS). A **Gram block** is an interval bounded by two good Gram points such that all the Gram points between them are bad. A refinement of Gram's law called Rosser's rule due to Rosser, Yohe & Schoenfeld (1969) says that Gram blocks often have the expected number of zeros in them (the same as the number of Gram intervals), even though some of the individual Gram intervals in the block may not have exactly one zero in them. For example, the interval bounded by g_{125} and g_{127} is a Gram block containing a unique bad Gram point g_{126}, and contains the expected number 2 of zeros although neither of its two Gram intervals contains a unique zero. Rosser et al. checked that there were no exceptions to Rosser's rule in the first 3 million zeros, though there are infinitely many exceptions for larger imaginary part.

Gram's rule and Rosser's rule both say that in some sense zeros do not stray too far from their expected positions. The distance of a zero from its expected position is controlled by the function S defined above, which grows extremely slowly: its average value is of the order of $(\log \log T)^{1/2}$, which only reaches 2 for T around 10^{24}. This means that both rules hold most of the time for small T but eventually break down often.

Arguments for and against the Riemann hypothesis

Mathematical papers about the Riemann hypothesis tend to be cautiously noncommittal about its truth. Of authors who express an opinion, most of them, such as Riemann (1859) or Bombieri (2000), imply that they expect (or at least hope) that it is true. The few authors who express serious doubt about it include Ivić (2008) who lists some reasons for being skeptical, and Littlewood (1962) who flatly states that he believes it to be false, and that there is no evidence whatever for it and no imaginable reason for it to be true. The consensus of the survey articles (Bombieri 2000, Conrey 2003, and Sarnak 2008) is that the evidence for it is strong but not overwhelming, so that while it is probably true there is some reasonable doubt about it.

Some of the arguments for (or against) the Riemann hypothesis are listed by Sarnak (2008), Conrey (2003), and Ivić (2008), and include the following reasons.

- Several analogues of the Riemann hypothesis have already been proved. The proof of the Riemann hypothesis for varieties over finite fields by Deligne (1974) is possibly the single strongest theoretical reason in favor of the Riemann hypothesis. This provides some evidence for the more general conjecture that all zeta functions associated with automorphic forms satisfy a Riemann hypothesis, which includes the classical Riemann hypothesis as a special case. Similarly Selberg zeta functions satisfy the analogue of the Riemann hypothesis, and are in some ways similar to the Riemann zeta function, having a functional equation and an infinite product expansion analogous to the Euler product expansion. However there are also some major differences; for example they are not given by Dirichlet series. The Riemann hypothesis for the Goss zeta function was proved by Sheats (1998). In contrast to these positive examples, however, some Epstein zeta functions do not satisfy the Riemann hypothesis, even though they have an infinite number of zeros on the critical line (Titchmarsh 1986). These functions are quite similar to the Riemann zeta function, and have a Dirichlet series expansion and a functional equation, but the ones known to fail the Riemann hypothesis do not have an Euler product and are not directly related to automorphic representations.
- The numerical verification that many zeros lie on the line seems at first sight to be strong evidence for it. However analytic number theory has had many conjectures supported by large amounts of numerical evidence that turn out to be false. See Skewes number for a notorious example, where the first exception to a plausible conjecture related to the Riemann hypothesis probably occurs around 10^{316}; a counterexample to the Riemann hypothesis with imaginary part this size would be far beyond anything that can currently be computed. The problem is that the behavior is often influenced by very slowly increasing functions such as log log T, that tend to infinity, but do so so slowly that this cannot be detected by computation. Such functions occur in the theory of the zeta function controlling the behavior of its zeros; for example the function $S(T)$ above has average size around $(\log\log T)^{1/2}$. As $S(T)$ jumps by at least 2 at any counterexample to the Riemann hypothesis, one might expect any counterexamples to the Riemann hypothesis to start appearing only when $S(T)$ becomes large. It is never much more than 3 as far as it has been calculated, but is known to be unbounded, suggesting that calculations may not have yet reached the region of typical behavior of the zeta function.
- Denjoy's probabilistic argument for the Riemann hypothesis (Edwards 1974): If $\mu(x)$ is a random sequence of "1"s and "−1"s then, for every $\varepsilon > 0$, the function

$$M(x) = \sum_{n \le x} \mu(n)$$

  (the values of which are positions in a simple random walk) satisfies the bound

$$M(x) = O(x^{1/2+\varepsilon})$$

  with probability 1. The Riemann hypothesis is equivalent to this bound for the Möbius function μ and the Mertens function M derived in the same way from it. In other words, the Riemann hypothesis is in some sense equivalent to saying that $\mu(x)$ behaves like a random sequence of coin tosses. When $\mu(x)$ is non-zero its sign gives the parity of the number of prime factors of x, so informally the Riemann hypothesis says that the parity of the number of prime factors of an integer behaves randomly. Such probabilistic arguments in number theory

often give the right answer, but tend to be very hard to make rigorous, and occasionally give the wrong answer for some results, such as Maier's theorem.

- The calculations in Odlyzko (1987) show that the zeros of the zeta function behave very much like the eigenvalues of a random Hermitian matrix, suggesting that they are the eigenvalues of some self-adjoint operator, which would imply the Riemann hypothesis. However all attempts to find such an operator have failed.
- There are several theorems, such as Goldbach's conjecture for sufficiently large odd numbers, that were first proved using the generalized Riemann hypothesis, and later shown to be true unconditionally. This could be considered as weak evidence for the generalized Riemann hypothesis, as several of its "predictions" turned out to be true.
- Lehmer's phenomenon (Lehmer 1956) where two zeros are sometimes very close is sometimes given as a reason to disbelieve in the Riemann hypothesis. However one would expect this to happen occasionally just by chance even if the Riemann hypothesis were true, and Odlyzko's calculations suggest that nearby pairs of zeros occur just as often as predicted by Montgomery's conjecture.
- Patterson (1988) suggests that the most compelling reason for the Riemann hypothesis for most mathematicians is the hope that primes are distributed as regularly as possible.

References

[1] http://arxiv.org/find/grp_math/1/AND+ti:+AND+Riemann+hypothesis+subj:+AND+General+mathematics/0/1/0/all/0/1

[2] http://en.wikipedia.org/wiki/Oeis%3Aa114856

- Artin, Emil (1924), "Quadratische Körper im Gebiete der höheren Kongruenzen. II. Analytischer Teil", *Mathematische Zeitschrift* **19** (1): 207–246, doi:10.1007/BF01181075, ISSN 0025-5874
- Beurling, Arne (1955), "A closure problem related to the Riemann zeta-function" (http://www.pnas.org/content/41/5/312.short), *Proceedings of the National Academy of Sciences of the United States of America* **41**: 312–314, doi:10.1073/pnas.41.5.312, MR0070655, ISSN 0027-8424
- Bohr, H.; Landau, E. (1914), "Ein Satz über Dirichletsche Reihen mit Anwendung auf die ζ-Funktion und die *L*-Funktionen", *Rendiconti del Circolo Matematico di Palermo* **37** (1): 269–272, doi:10.1007/BF03014823, ISSN 0009-725X
- Bombieri, Enrico (2000) (PDF), *The Riemann Hypothesis - official problem description* (http://www.claymath.org/millennium/Riemann_Hypothesis/riemann.pdf), Clay Mathematics Institute, retrieved 2008-10-25 Reprinted in (Borwein et al. 2008).
- Borwein, Peter; Choi, Stephen; Rooney, Brendan et al., eds. (2008), *The Riemann Hypothesis: A Resource for the Afficionado and Virtuoso Alike*, CMS Books in Mathematics, New York: Springer, doi:10.1007/978-0-387-72126-2, ISBN 978-0387721255
- Borwein, Peter; Ferguson, Ron; Mossinghoff, Michael J. (2008), "Sign changes in sums of the Liouville function", *Mathematics of Computation* **77** (263): 1681–1694, doi:10.1090/S0025-5718-08-02036-X, MR2398787, ISSN 0025-5718
- de Branges, Louis (1992), "The convergence of Euler products", *Journal of Functional Analysis* **107** (1): 122–210, doi:10.1016/0022-1236(92)90103-P, MR1165869, ISSN 0022-1236
- Cartier, P. (1982), "Comment l'hypothèse de Riemann ne fut pas prouvée", *Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981)*, Progr. Math., **22**, Boston, MA: Birkhäuser Boston, pp. 35–48, MR693308
- Connes, Alain (1999), "Trace formula in noncommutative geometry and the zeros of the Riemann zeta function", *Selecta Mathematica. New Series* **5** (1): 29–106, doi:10.1007/s000290050042, arXiv:math/9811068, MR1694895, ISSN 1022-1824
- Connes, Alain (2000), "Noncommutative geometry and the Riemann zeta function", *Mathematics: frontiers and perspectives*, Providence, R.I.: American Mathematical Society, pp. 35–54, MR1754766
- Conrey, J. B. (1989), "More than two fifths of the zeros of the Riemann zeta function are on the critical line" (http://www.digizeitschriften.de/resolveppn/GDZPPN002206781), *J. Reine angew. Math.* **399**: 1–16,

MR1004130

- Conrey, J. Brian (2003), "The Riemann Hypothesis" (http://www.ams.org/notices/200303/fea-conrey-web.pdf) (PDF), *Notices of the American Mathematical Society*: 341–353 Reprinted in (Borwein et al. 2008).
- Conrey, J. B.; Li, Xian-Jin (2000), "A note on some positivity conditions related to zeta and L-functions", *International Mathematics Research Notices* **2000** (18): 929–940, doi:10.1155/S1073792800000489, arXiv:math/9812166, MR1792282, ISSN 1073-7928
- Deligne, Pierre (1974), "La conjecture de Weil. I." (http://www.numdam.org/item?id=PMIHES_1974__43__273_0), *Publications Mathématiques de l'IHÉS* **43**: 273–307, doi:10.1007/BF02684373, MR0340258, ISSN 1618-1913
- Deligne, Pierre (1980), "La conjecture de Weil : II." (http://www.numdam.org/item?id=PMIHES_1980__52__137_0), *Publications Mathématiques de l'IHÉS* **52**: 137–252, doi:10.1007/BF02684780, ISSN 1618-1913
- Deninger, Christopher (1998), *Some analogies between number theory and dynamical systems on foliated spaces* (http://www.mathematik.uni-bielefeld.de/documenta/xvol-icm/00/Deninger.MAN.html), "Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998)", *Documenta Mathematica*: 163–186, MR1648030, ISSN 1431-0635
- Derbyshire, John (2003), *Prime Obsession*, Joseph Henry Press, Washington, DC, MR1968857, ISBN 978-0-309-08549-6
- Dyson, Freeman (2009), "Birds and frogs" (http://www.ams.org/notices/200902/rtx090200212p.pdf), *Notices of the American Mathematical Society* **56** (2): 212–223, MR2483565, ISSN 0002-9920
- Edwards, H. M. (1974), *Riemann's Zeta Function*, New York: Dover Publications, MR0466039, ISBN 978-0-486-41740-0
- Ford, Kevin (2002), "Vinogradov's integral and bounds for the Riemann zeta function", *Proceedings of the London Mathematical Society. Third Series* **85** (3): 565–633, doi:10.1112/S0024611502013655, MR1936814, ISSN 0024-6115
- Franel, J.; Landau, E. (1924), "Les suites de Farey et le problème des nombres premiers", *Göttinger Nachr.*: 198–206
- Ghosh, Amit (1983), "On the Riemann zeta function---mean value theorems and the distribution of |S(T)|", *J. Number Theory* **17**: 93–102, doi:10.1016/0022-314X(83)90010-0
- Gourdon, Xavier (2004) (PDF), *The 10^{13} first zeros of the Riemann Zeta function, and zeros computation at very large height* (http://numbers.computation.free.fr/Constants/Miscellaneous/zetazeros1e13-1e24.pdf)
- Gram, J. P. (1903), "Note sur les zéros de la fonction ζ(s) de Riemann", *Acta Mathematica* **27**: 289–304, doi:10.1007/BF02421310
- Hadamard, Jacques (1896), "Sur la distribution des zéros de la fonction ζ(s) et ses conséquences arithmétiques" (http://www.numdam.org/item?id=BSMF_1896__24__199_1), *Bulletin Société Mathématique de France* **14**: 199–220 Reprinted in (Borwein et al. 2008).
- Hardy, G. H. (1914), "Sur les Zéros de la Fonction ζ(s) de Riemann" (http://gallica.bnf.fr/ark:/12148/bpt6k3111d.image.f1014.langEN), *C. R. Acad. Sci. Paris* **158**: 1012–1014, JFM 45.0716.04 Reprinted in (Borwein et al. 2008).
- Hardy, G. H.; Littlewood, J. E. (1921), "The zeros of Riemann's zeta-function on the critical line", *Math. Z.* **10**: 283–317, doi:10.1007/BF01211614
- Haselgrove, C. B. (1958), "A disproof of a conjecture of Pólya", *Mathematika* **5**: 141–145, doi:10.1112/S0025579300001480, MR0104638 Reprinted in (Borwein et al. 2008).
- Haselgrove, C. B.; Miller, J. C. P. (1960), *Tables of the Riemann zeta function*, Royal Society Mathematical Tables, Vol. 6, Cambridge University Press, MR0117905, ISBN 978-0-521-06152-0 Review (http://www.jstor.org/stable/2003098)

- Hutchinson, J. I. (1925), "On the Roots of the Riemann Zeta-Function" (http://www.jstor.org/stable/1989163), *Transactions of the American Mathematical Society* **27** (1): 49–60, doi:10.2307/1989163, ISSN 0002-9947
- Ingham, A.E. (1932), *The Distribution of Prime Numbers*, Cambridge Tracts in Mathematics and Mathematical Physics, **30**, Cambridge University Press. Reprinted 1990, ISBN 978-0-521-39789-6, MR1074573
- Ivić, A. (1985), *The Riemann Zeta Function*, New York: John Wiley & Sons, MR0792089, ISBN 978-0-471-80634-9 (Reprinted by Dover 2003)
- Ivić, Aleksandar (2008), "On some reasons for doubting the Riemann hypothesis", in Borwein, Peter; Choi, Stephen; Rooney, Brendan et al., *The Riemann Hypothesis: A Resource for the Afficionado and Virtuoso Alike*, CMS Books in Mathematics, New York: Springer, pp. 131–160, arXiv:math.NT/0311162, ISBN 978-0387721255
- Karatsuba, A. A.; Voronin, S. M. (1992), *The Riemann zeta-function*, de Gruyter Expositions in Mathematics, **5**, Berlin: Walter de Gruyter & Co., MR1183467, ISBN 978-3-11-013170-3
- Keating, Jonathan P.; Snaith, N. C. (2000), "Random matrix theory and ζ(1/2+it)", *Communications in Mathematical Physics* **214** (1): 57–89, doi:10.1007/s002200000261, MR1794265, ISSN 0010-3616
- Knauf, Andreas (1999), "Number theory, dynamical systems and statistical mechanics", *Reviews in Mathematical Physics. A Journal for Both Review and Original Research Papers in the Field of Mathematical Physics* **11** (8): 1027–1060, doi:10.1142/S0129055X99000325, MR1714352, ISSN 0129-055X
- von Koch, Helge (1901), "Sur la distribution des nombres premiers", *Acta Mathematica* **24**: 159–182, doi:10.1007/BF02403071
- Kurokawa, Nobushige (1992), "Multiple zeta functions: an example", *Zeta functions in geometry (Tokyo, 1990)*, Adv. Stud. Pure Math., **21**, Tokyo: Kinokuniya, pp. 219–226, MR1210791
- Lapidus, Michel L. (2008), *In search of the Riemann zeros* (http://www.ams.org/bookstore-getitem/item=mbk-51), Providence, R.I.: American Mathematical Society, MR2375028, ISBN 978-0-8218-4222-5
- Lavrik, A. F. (2001), "Zeta-function" (http://eom.springer.de/Z/z099260.htm), in Hazewinkel, Michiel, *Encyclopaedia of Mathematics*, Springer, ISBN 978-1556080104
- Lehmer, D. H. (1956), "Extended computation of the Riemann zeta-function", *Mathematika. A Journal of Pure and Applied Mathematics* **3**: 102–108, doi:10.1112/S0025579300001753, MR0086083, ISSN 0025-5793
- Levinson, N. (1974), "More than one-third of the zeros of Riemann's zeta function are on σ = 1/2", *Adv. In Math.* **13**: 383–436, doi:10.1016/0001-8708(74)90074-7, MR0564081
- Littlewood, J. E. (1962), "The Riemann hypothesis", *The scientist speculates: an anthology of partly baked idea*, New York: Basic books
- van de Lune, J.; te Riele, H. J. J.; Winter, D. T. (1986), "On the zeros of the Riemann zeta function in the critical strip. IV" (http://www.jstor.org/stable/2008005), *Mathematics of Computation* **46** (174): 667–681, doi:10.2307/2008005, MR829637, ISSN 0025-5718
- Massias, J.-P.; Nicolas, Jean-Louis; Robin, G. (1988), "Évaluation asymptotique de l'ordre maximum d'un élément du groupe symétrique" (http://matwbn.icm.edu.pl/tresc.php?wyd=6&tom=50&jez=), *Polska Akademia Nauk. Instytut Matematyczny. Acta Arithmetica* **50** (3): 221–242, MR960551, ISSN 0065-1036
- Montgomery, Hugh L. (1973), "The pair correlation of zeros of the zeta function", *Analytic number theory*, Proc. Sympos. Pure Math., **XXIV**, Providence, R.I.: American Mathematical Society, pp. 181–193, MR0337821 Reprinted in (Borwein et al. 2008).
- Montgomery, Hugh L. (1983), "Zeros of approximations to the zeta function", in Erdős, Paul, *Studies in pure mathematics. To the memory of Paul Turán.*, Basel, Boston, Berlin: Birkhäuser, pp. 497–506, MR820245, ISBN 978-3-7643-1288-6
- Nicely, Thomas R. (1999), "New maximal prime gaps and first occurrences" (http://www.trnicely.net/gaps/gaps.html), *Mathematics of Computation* **68** (227): 1311–1315, doi:10.1090/S0025-5718-99-01065-0, MR1627813.

- Nyman, Bertil (1950), *On the One-Dimensional Translation Group and Semi-Group in Certain Function Spaces*, PhD Thesis, University of Uppsala: University of Uppsala, MR0036444
- Odlyzko, A. M.; te Riele, H. J. J. (1985), "Disproof of the Mertens conjecture" (http://gdz.sub.uni-goettingen.de/no_cache/dms/load/img/?IDDOC=262633), *Journal für die reine und angewandte Mathematik* **357**: 138–160, MR783538, ISSN 0075-4102
- Odlyzko, A. M. (1987), "On the distribution of spacings between zeros of the zeta function" (http://www.jstor.org/stable/2007890), *Mathematics of Computation* **48** (177): 273–308, doi:10.2307/2007890, MR866115, ISSN 0025-5718
- Odlyzko, A. M. (1990), "Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results" (http://www.numdam.org/item?id=JTNB_1990__2_1_119_0), *Séminaire de Théorie des Nombres de Bordeaux. Série 2* **2** (1): 119–141, MR1061762, ISSN 0989-5558
- Odlyzko, A. M. (1992), *The 10^{20}-th zero of the Riemann zeta function and 175 million of its neighbors* (http://www.dtc.umn.edu/~odlyzko/unpublished/index.html) This unpublished book describes the implementation of the algorithm and discusses the results in detail.
- Patterson, S. J. (1988), *An introduction to the theory of the Riemann zeta-function*, Cambridge Studies in Advanced Mathematics, **14**, Cambridge University Press, MR933558, ISBN 978-0-521-33535-5
- Riemann, Bernhard (1859), "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse" (http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/), *Monatsberichte der Berliner Akademie*. In *Gesammelte Werke*, Teubner, Leipzig (1892), Reprinted by Dover, New York (1953). Original manuscript (http://www.claymath.org/millennium/Riemann_Hypothesis/1859_manuscript/) (with English translation). Reprinted in (Borwein et al. 2008) and (Edwards 1874)
- Riesel, Hans; Göhl, Gunnar (1970), "Some calculations related to Riemann's prime number formula" (http://jstor.org/stable/2004630), *Mathematics of Computation* **24** (112): 969–983, doi:10.2307/2004630, MR0277489, ISSN 0025-5718
- Riesz, M. (1916), "Sur l'hypothèse de Riemann", *Acta Mathematica* **40**: 185–190, doi:10.1007/BF02418544
- Robin, G. (1984), "Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann", *Journal de Mathématiques Pures et Appliquées. Neuvième Série* **63** (2): 187–213, MR774171, ISSN 0021-7824
- Rockmore, Dan (2005), *Stalking the Riemann hypothesis*, Pantheon Books, MR2269393, ISBN 978-0-375-42136-5
- Rosser, J. Barkley; Yohe, J. M.; Schoenfeld, Lowell (1969), "Rigorous computation and the zeros of the Riemann zeta-function. (With discussion)", *Information Processing 68 (Proc. IFIP Congress, Edinburgh, 1968), Vol. 1: Mathematics, Software*, Amsterdam: North-Holland, pp. 70–76, MR0258245
- Sabbagh, Karl (2003), *The Riemann hypothesis*, Farrar, Straus and Giroux, New York, MR1979664, ISBN 978-0-374-25007-2
- Salem, Raphaël (1953), "Sur une proposition équivalente à l'hypothèse de Riemann", *Les Comptes rendus de l'Académie des sciences* **236**: 1127–1128, MR0053148
- Sarnak, Peter (2008), "Problems of the Millennium: The Riemann Hypothesis" (http://www.claymath.org/millennium/Riemann_Hypothesis/Sarnak_RH.pdf), in Borwein, Peter; Choi, Stephen; Rooney, Brendan et al. (PDF), *The Riemann Hypothesis: A Resource for the Afficionado and Virtuoso Alike*, CMS Books in Mathematics, New York: Springer, pp. 107–115, ISBN 978-0387721255
- du Sautoy, Marcus (2003), *The music of the primes*, HarperCollins Publishers, MR2060134, ISBN 978-0-06-621070-4
- Schoenfeld, Lowell (1976), "Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II" (http://jstor.org/stable/2005976), *Mathematics of Computation* **30** (134): 337–360, doi:10.2307/2005976, MR0457374, ISSN 0025-5718
- Selberg, Atle (1942), "On the zeros of Riemann's zeta-function.", *Skr. Norske Vid. Akad. Oslo I.* **10**: 59 pp, MR0010712

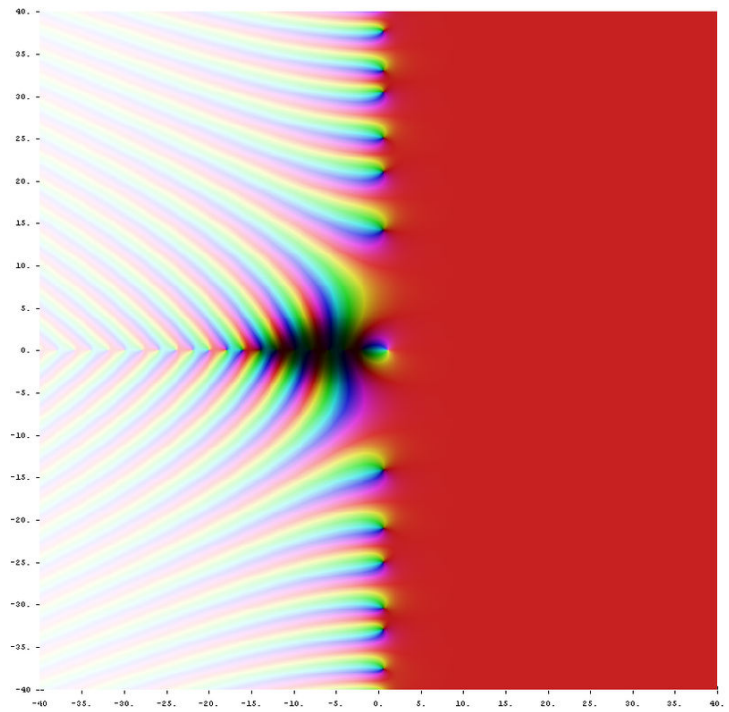
- Selberg, Atle (1946), "Contributions to the theory of the Riemann zeta-function", *Arch. Math. Naturvid.* **48** (5): 89–155, MR0020594
- Selberg, Atle (1956), "Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series", *J. Indian Math. Soc. (N.S.)* **20**: 47–87, MR0088511
- Sheats, Jeffrey T. (1998), "The Riemann hypothesis for the Goss zeta function for $\mathbf{F}_q[T]$", *Journal of Number Theory* **71** (1): 121–157, doi:10.1006/jnth.1998.2232, MR1630979, ISSN 0022-314X
- Siegel, C. L. (1932), "Über Riemanns Nachlaß zur analytischen Zahlentheorie", *Quellen Studien zur Geschichte der Math. Astron. und Phys. Abt. B: Studien 2*: 45–80 Reprinted in Gesammelte Abhandlungen, Vol. 1. Berlin: Springer-Verlag, 1966.
- Stein, William; Mazur, Barry (2007) (PDF), *What is Riemann's Hypothesis?* (http://modular.math.washington.edu/edu/2007/simuw07/notes/rh.pdf)
- Titchmarsh, Edward Charles (1935), "The Zeros of the Riemann Zeta-Function" (http://www.jstor.org/stable/96545), *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences* (The Royal Society) **151** (873): 234–255, doi:10.1098/rspa.1935.0146, ISSN 0080-4630
- Titchmarsh, Edward Charles (1936), "The Zeros of the Riemann Zeta-Function" (http://www.jstor.org/stable/96692), *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences* (The Royal Society) **157** (891): 261–263, doi:10.1098/rspa.1936.0192, ISSN 0080-4630
- Titchmarsh, Edward Charles (1986), *The theory of the Riemann zeta-function* (2nd ed.), The Clarendon Press Oxford University Press, MR882550, ISBN 978-0-19-853369-6
- Turán, Paul (1948), "On some approximative Dirichlet-polynomials in the theory of the zeta-function of Riemann", *Danske Vid. Selsk. Mat.-Fys. Medd.* **24** (17): 36, MR0027305 Reprinted in (Borwein et al. 2008).
- Turing, Alan M. (1953), "Some calculations of the Riemann zeta-function", *Proceedings of the London Mathematical Society. Third Series* **3**: 99–117, doi:10.1112/plms/s3-3.1.99, MR0055785, ISSN 0024-6115
- de la Vallée-Poussin, Ch.J. (1896), "Recherches analytiques sur la théorie des nombers premiers", *Ann. Soc. Sci. Bruxelles* **20**: 183–256
- de la Vallée-Poussin, Ch.J. (1899–1900), "Sur la fonction $\zeta(s)$ de Riemann et la nombre des nombres premiers inférieurs à une limite donnée", *Mem. Couronnes Acad. Sci. Belg.* **59** (1) Reprinted in (Borwein et al. 2008).
- Weil, André (1948), *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945), Hermann et Cie., Paris, MR0027151
- Weil, André (1949), "Numbers of solutions of equations in finite fields" (http://www.ams.org/bull/1949-55-05/S0002-9904-1949-09219-4/home.html), *Bulletin of the American Mathematical Society* **55**: 497–508, doi:10.1090/S0002-9904-1949-09219-4, MR0029393, ISSN 0002-9904 Reprinted in Oeuvres Scientifiques/Collected Papers by Andre Weil ISBN 0-387-90330-5
- Weinberger, Peter J. (1973), "On Euclidean rings of algebraic integers", *Analytic number theory (St. Louis Univ., 1972)*, Proc. Sympos. Pure Math., **24**, Providence, R.I.: Amer. Math. Soc., pp. 321–332, MR0337902
- Wiles, Andrew (2000), "Twenty years of number theory", *Mathematics: frontiers and perspectives*, Providence, R.I.: American Mathematical Society, pp. 329–342, MR1754786, ISBN 978-0-8218-2697-3
- Zagier, Don (1977), "The first 50 million prime numbers" (http://modular.math.washington.edu/edu/2007/simuw07/misc/zagier-the_first_50_million_prime_numbers.pdf) (PDF), *Math. Intelligencer* (Springer) **0**: 7–19, doi:10.1007/BF03039306, MR643810
- Zagier, Don (1981), "Eisenstein series and the Riemann zeta function", *Automorphic forms, representation theory and arithmetic (Bombay, 1979)*, Tata Inst. Fund. Res. Studies in Math., **10**, Tata Inst. Fundamental Res., Bombay, pp. 275–301, MR633666

External links

- American institute of mathematics, Riemann hypothesis (http://www.aimath.org/WWN/rh/)
- Apostol, Tom, *Where are the zeros of zeta of s?* (http://www.math.wisc.edu/~robbin/funnysongs.html#Zeta) Poem about the Riemann hypothesis, sung (http://www.olimu.com/RIEMANN/Song.htm) by John Derbyshire.
- Borwein, Peter (PDF), *The Riemann Hypothesis* (http://oldweb.cecm.sfu.ca/~pborwein/COURSE/MATH08/LECTURE.pdf) (Slides for a lecture)
- Conrad, K. (2010), *Consequences of the Riemann hypothesis* (http://mathoverflow.net/questions/17232)
- Conrey, J. Brian; Farmer, David W, *Equivalences to the Riemann hypothesis* (http://aimath.org/pl/rhequivalences)
- Gourdon, Xavier; Sebah, Pascal (2004), *Computation of zeros of the Zeta function* (http://numbers.computation.free.fr/Constants/Miscellaneous/zetazeroscompute.html) (Reviews the GUE hypothesis, provides an extensive bibliography as well).
- Odlyzko, Andrew, *Home page* (http://www.dtc.umn.edu/~odlyzko/) including papers on the zeros of the zeta function (http://www.dtc.umn.edu/~odlyzko/doc/zeta.html) and tables of the zeros of the zeta function (http://www.dtc.umn.edu/~odlyzko/zeta_tables/index.html)
- Odlyzko, Andrew (2002) (PDF), *Zeros of the Riemann zeta function: Conjectures and computations* (http://www.dtc.umn.edu/~odlyzko/talks/riemann-conjectures.pdf) Slides of a talk
- Pegg, Ed (2004), *Ten Trillion Zeta Zeros* (http://www.maa.org/editorial/mathgames/mathgames_10_18_04.html), Math Games website A discussion of Xavier Gourdon's calculation of the first ten trillion non-trivial zeros
- Pugh, Glen, *Java applet for plotting Z(t)* (http://web.viu.ca/pughg/RiemannZeta/RiemannZetaLong.html)
- Rubinstein, Michael, *algorithm for generating the zeros* (http://pmmac03.math.uwaterloo.ca/~mrubinst/l_function_public/L.html).
- du Sautoy, Marcus (2006), *Prime Numbers Get Hitched* (http://www.seedmagazine.com/news/2006/03/prime_numbers_get_hitched.php), Seed Magazine (http://www.seedmagazine.com)
- Stein, William A., *What is Riemann's hypothesis* (http://modular.math.washington.edu/edu/2007/simuw07/index.html)
- de Vries, Andreas (2004), *The Graph of the Riemann Zeta function $\zeta(s)$* (http://math-it.org/Mathematik/Riemann/RiemannApplet.html), a simple animated Java applet.
- Watkins, Matthew R. (2007-07-18), *Proposed proofs of the Riemann Hypothesis* (http://secamlocal.ex.ac.uk/~mwatkins/zeta/RHproofs.htm)
- *Zetagrid* (http://www.zetagrid.net/) (2002) A distributed computing project that attempted to disprove Riemann's hypothesis; closed in November 2005

Riemann zeta function

The **Riemann zeta function**, ζ(s), is a function of a complex variable *s* that analytically continues the sum of the infinite series



Riemann zeta function ζ(*s*) in the complex plane. The color of a point *s* encodes the value of ζ(*s*): dark colors denote values close to zero and hue encodes the value's argument. The white spot at *s* = 1 is the pole of the zeta function; the black spots on the negative real axis and on the critical line Re(*s*) = 1/2 are its zeros. Positive real values are presented in red.

$$\sum_{n=1}^{\infty} \frac{1}{n^s},$$

which converges when the real part of *s* is greater than 1. The Zeta function is represented above as an infinite p-series. It plays a pivotal role in analytic number theory and has applications in physics, probability theory, and applied statistics.

First results about this function were obtained by Leonhard Euler in the eighteenth century. It is named after Bernhard Riemann, who in the memoir "On the Number of Primes Less Than a Given Magnitude", published in 1859, established a relation between its zeros and the distribution of prime numbers.[1]

The values of the Riemann zeta function at even positive integers were computed by Euler. The first of them, ζ(2), provides a solution to the Basel problem. In 1979 Apéry proved the irrationality of ζ(3). The values at negative integer points, also found by Euler, are rational numbers and play an important role in the theory of modular forms. Many generalizations of the Riemann zeta function, such as Dirichlet series and L-functions, are known.

Definition

The **Riemann zeta function** $\zeta(s)$ is a function of a complex variable $s = \sigma + it$ (here, s, σ and t are traditional notations associated to the study of the ζ-function). The following infinite series converges for all complex numbers s with real part greater than 1, and defines $\zeta(s)$ in this case:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots \qquad \sigma = \Re(s) > 1.$$

The Riemann zeta function is defined as the analytic continuation of the function defined for σ > 1 by the sum of the preceding series.

Leonhard Euler considered the above series in 1740 for positive integer values of s, and later Chebyshev extended the definition to real $s > 1$.[2]

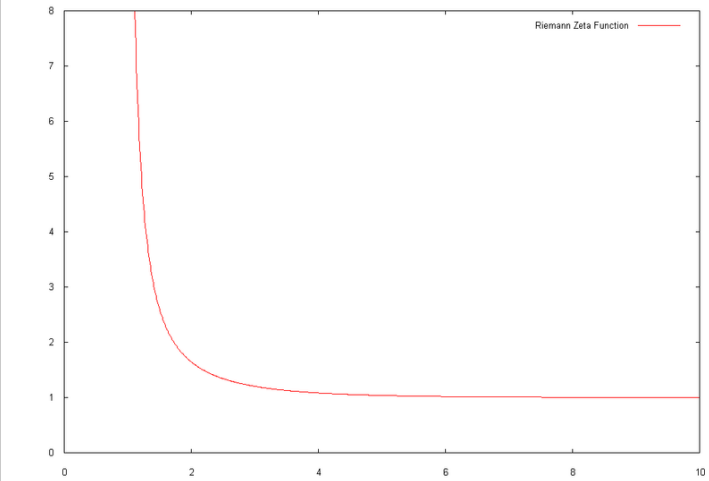
The above series is a prototypical Dirichlet series that converges absolutely to an analytic function for s such that $\sigma > 1$ and diverges for all other values of s. Riemann showed that the function defined by the series on the half-plane of convergence can be continued analytically to all complex values $s \neq 1$. For $s = 1$ the series is the harmonic series which diverges to +∞, and

$$\lim_{s \to 1} (s-1)\zeta(s) = 1.$$

Thus the Riemann zeta function is a meromorphic function on the whole complex s-plane, which is holomorphic everywhere except for a simple pole at $s = 1$ with residue 1.

Specific values

For any positive even number $2n$,



Riemann zeta function for real $s > 1$

$$\zeta(2n) = (-1)^{n+1} \frac{B_{2n}(2\pi)^{2n}}{2(2n)!}$$

where B_{2n} is a Bernoulli number; for negative integers, one has

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}$$

for $n \geq 1$, so in particular ζ vanishes at the negative even integers because $B_m = 0$ for all odd m other than 1. No such simple expression is known for odd positive integers.

The values of the zeta function obtained from integral arguments are called zeta constants. The following are the most commonly used values of the Riemann zeta function.

$$\zeta(0) = -\frac{1}{2},$$

$$\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots = \infty;$$

this is the harmonic series.

$$\zeta(3/2) \approx 2.612;$$

this is employed in calculating the critical temperature for a Bose–Einstein condensate in a box with periodic boundary conditions, and for spin wave physics in magnetic systems.

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6} \approx 1.645;$$

the demonstration of this equality is known as the Basel problem. The reciprocal of this sum answers the question: What is the probability that two numbers selected at random are relatively prime?[3]

$$\zeta(3) = 1 + \frac{1}{2^3} + \frac{1}{3^3} + \cdots \approx 1.202;$$

this is called Apéry's constant.

$$\zeta(4) = 1 + \frac{1}{2^4} + \frac{1}{3^4} + \cdots = \frac{\pi^4}{90} \approx 1.0823;$$

Stefan–Boltzmann law and Wien approximation in physics.

Euler product formula

The connection between the zeta function and prime numbers was discovered by Leonhard Euler, who proved the identity

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

where, by definition, the left hand side is $\zeta(s)$ and the infinite product on the right hand side extends over all prime numbers p (such expressions are called Euler products):

$$\prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} = \frac{1}{1 - 2^{-s}} \cdot \frac{1}{1 - 3^{-s}} \cdot \frac{1}{1 - 5^{-s}} \cdot \frac{1}{1 - 7^{-s}} \cdot \frac{1}{1 - 11^{-s}} \cdots \frac{1}{1 - p^{-s}} \cdots.$$

Both sides of the Euler product formula converge for $\mathrm{Re}(s) > 1$. The proof of Euler's identity uses only the formula for the geometric series and the fundamental theorem of arithmetic. Since the harmonic series, obtained when $s = 1$, diverges, Euler's formula (which becomes $\prod_p p/(p-1)$) implies that there are infinitely many primes.[4]

The Euler product formula can be used to calculate the asymptotic probability that s randomly selected integers are set-wise coprime. Intuitively, the probability that any single number is divisible by a prime (or any integer), p is $1/p$. Hence the probability that s numbers are all divisible by this prime is $1/p^s$, and the probability that at least one of them is *not* is $1 - 1/p^s$. Now, for distinct primes, these divisibility events are mutually independent because the candidate divisors are coprime (a number is divisible by coprime divisors n and m if and only if it is divisible by nm, an event which occurs with probability $1/(nm)$.) Thus the asymptotic probability that s numbers are coprime is given by a product over all primes,

$$\prod_{p}^{\infty} \left(1 - \frac{1}{p^s}\right) = \left(\prod_{p}^{\infty} \frac{1}{1 - p^{-s}}\right)^{-1} = \frac{1}{\zeta(s)}.$$

(More work is required to derive this result formally.)[5]

The functional equation

The Riemann zeta function satisfies the functional equation

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\, \zeta(1-s),$$

where $\Gamma(s)$ is the gamma function, which is an equality of meromorphic functions valid on the whole complex plane. This equation relates values of the Riemann zeta function at the points s and $1 - s$. The gamma function has a simple pole at every non-positive integer, therefore, the functional equation implies that $\zeta(s)$ has a simple zero at each even negative integer $s = -2n$ — these are the **trivial zeros** of $\zeta(s)$.[6]

The functional equation was established by Riemann in his 1859 paper *On the Number of Primes Less Than a Given Magnitude* and used to construct the analytic continuation in the first place. An equivalent relationship had been conjectured by Euler over a hundred years earlier, in 1749, for the Dirichlet eta function (alternating zeta function)

$$\eta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s} = (1 - 2^{1-s})\zeta(s).$$

Incidentally, this relation is interesting also because it actually exhibits $\zeta(s)$ as a Dirichlet series (of the η-function) which is convergent (albeit non-absolutely) in the larger half-plane $\sigma > 0$ (not just $\sigma > 1$), up to an elementary factor.

Riemann also found a symmetric version of the functional equation, given by first defining

$$\xi(s) = \pi^{-s/2}\, \Gamma\left(\frac{s}{2}\right)\, \zeta(s).$$

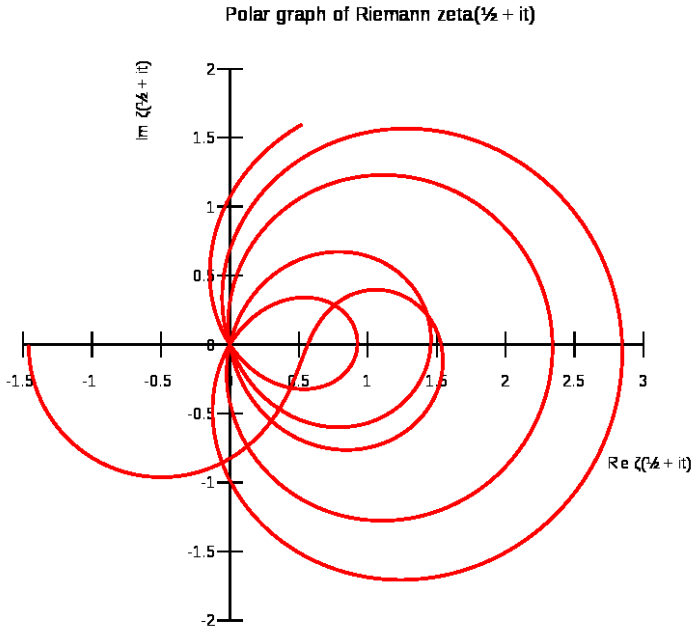
The functional equation is then given by

$$\xi(s) = \xi(1-s).$$

(Riemann defined a similar but different function which he called $\Xi(t)$.)

Zeros, the critical line, and the Riemann hypothesis

The functional equation shows that the Riemann zeta function has zeros at −2, −4, ... These are called the **trivial zeros**. They are trivial in the sense that their existence is relatively easy to prove, for example, from $\sin(\pi s/2)$ being 0 in the functional equation. The non-trivial zeros have captured far more attention because their distribution not only is far less understood but, more importantly, their study yields impressive results concerning prime numbers and related objects in number theory. It is known that any non-trivial zero lies in the open strip $\{s \in \mathbf{C}: 0 < \mathrm{Re}(s) < 1\}$, which is called the **critical strip**. The Riemann hypothesis, considered to be one of the greatest unsolved problems in mathematics, asserts that any



This image shows a plot of the Riemann zeta function along the critical line for real values of t running from 0 to 34. The first five zeros in the critical strip are clearly visible as the place where the spirals pass through the origin.

non-trivial zero s has Re(s) = 1/2. In the theory of the Riemann zeta function, the set $\{s \in \mathbf{C}: \mathrm{Re}(s) = 1/2\}$ is called the **critical line**. For the Riemann zeta function on the critical line, see Z-function.

The location of the Riemann zeta function's zeros is of great importance in the theory of numbers. From the fact that all non-trivial zeros lie in the critical strip one can deduce the prime number theorem. A better result[7] is that $\zeta(\sigma + it) \neq 0$ whenever $|t| \geq 3$ and

$$\sigma \geq 1 - \frac{1}{57.54(\log|t|)^{2/3}(\log\log|t|)^{1/3}}.$$

The strongest result of this kind one can hope for is the truth of the Riemann hypothesis, which would have many profound consequences in the theory of numbers.

It is known that there are infinitely many zeros on the critical line. Littlewood showed that if the sequence (γ_n) contains the imaginary parts of all zeros in the upper half-plane in ascending order, then

$$\lim_{n\to\infty}(\gamma_{n+1} - \gamma_n) = 0.$$

The critical line theorem asserts that a positive percentage of the nontrivial zeros lies on the critical line.

In the critical strip, the zero with smallest non-negative imaginary part is 1/2 + i14.13472514... Directly from the functional equation one sees that the non-trivial zeros are symmetric about the axis Re(s) = 1/2. Furthermore, the fact that $\zeta(s) = \zeta(s^*)^*$ for all complex $s \neq 1$ (* indicating complex conjugation) implies that the zeros of the Riemann zeta function are symmetric about the real axis.

The statistics of the Riemann zeta zeros are a topic of interest to mathematicians because of their connection to big problems like the Riemann hypothesis, distribution of prime numbers, etc. Through connections with random matrix theory and quantum chaos, the appeal is even broader. The fractal structure of the Riemann zeta zero distribution has been studied using rescaled range analysis.[8] The self-similarity of the zero distribution is quite remarkable, and is characterized by a large fractal dimension of 1.9. This rather large fractal dimension is found over zeros covering at least fifteen orders of magnitude, and also for the zeros of other L-functions.

Various properties

For sums involving the zeta-function at integer and half-integer values, see rational zeta series.

Reciprocal

The reciprocal of the zeta function may be expressed as a Dirichlet series over the Möbius function $\mu(n)$:

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$$

for every complex number s with real part > 1. There are a number of similar relations involving various well-known multiplicative functions; these are given in the article on the Dirichlet series.

The Riemann hypothesis is equivalent to the claim that this expression is valid when the real part of s is greater than 1/2.

Universality

The critical strip of the Riemann zeta function has the remarkable property of **universality**. This zeta-function universality states that there exists some location on the critical strip that approximates any holomorphic function arbitrarily well. Since holomorphic functions are very general, this property is quite remarkable.

Representations

Mellin transform

The Mellin transform of a function $f(x)$ is defined as

$$\int_0^\infty f(x)x^{s-1}\,dx,$$

in the region where the integral is defined. There are various expressions for the zeta-function as a Mellin transform. If the real part of s is greater than one, we have

$$\Gamma(s)\zeta(s) = \int_0^\infty \frac{x^{s-1}}{e^x-1}\,dx,$$

where Γ denotes the Gamma function. By modifying the contour Riemann showed that

$$2\sin(\pi s)\Gamma(s)\zeta(s) = i\oint_C \frac{(-x)^{s-1}}{e^x-1}\,dx$$

for all s, where the contour C starts and ends at +∞ and circles the origin once.

We can also find expressions which relate to prime numbers and the prime number theorem. If $\pi(x)$ is the prime-counting function, then

$$\log\zeta(s) = s\int_0^\infty \frac{\pi(x)}{x(x^s-1)}\,dx,$$

for values with Re(s) > 1.

A similar Mellin transform involves the Riemann prime-counting function $J(x)$, which counts prime powers p^n with a weight of 1/n, so that

$$J(x) = \sum \frac{\pi(x^{1/n})}{n}.$$

Now we have

$$\log\zeta(s) = s\int_0^\infty J(x)x^{-s-1}\,dx.$$

These expressions can be used to prove the prime number theorem by means of the inverse Mellin transform. Riemann's prime-counting function is easier to work with, and $\pi(x)$ can be recovered from it by Möbius inversion.

Theta functions

The Riemann zeta function can be given formally by a divergent Mellin transform

$$2\pi^{-s/2}\Gamma(s/2)\zeta(s) = \int_0^\infty \theta(it)t^{s/2-1}\,dt,$$

in terms of Jacobi's theta function

$$\theta(\tau) = \sum_{n=-\infty}^{\infty} \exp(\pi i n^2\tau).$$

However this integral does not converge for any value of s and so needs to be regularized: this gives the following expression for the zeta function:

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \frac{1}{s-1} - \frac{1}{s} + \frac{1}{2}\int_0^1 (\theta(it) - t^{-1/2}) t^{s/2-1}\,dt + \frac{1}{2}\int_1^\infty (\theta(it) - 1) t^{s/2-1}\,dt.$$

Laurent series

The Riemann zeta function is meromorphic with a single pole of order one at $s = 1$. It can therefore be expanded as a Laurent series about $s = 1$; the series development then is

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} \gamma_n (s-1)^n.$$

The constants γ_n here are called the Stieltjes constants and can be defined by the limit

$$\gamma_n = \lim_{m\to\infty} \left(\left(\sum_{k=1}^{m} \frac{(\log k)^n}{k} \right) - \frac{(\log m)^{n+1}}{n+1} \right).$$

The constant term γ_0 is the Euler–Mascheroni constant.

Rising factorial

Another series development using the rising factorial valid for the entire complex plane is

$$\zeta(s) = \frac{s}{s-1} - \sum_{n=1}^{\infty} (\zeta(s+n) - 1) \frac{s(s+1)\cdots(s+n-1)}{(n+1)!}.$$

This can be used recursively to extend the Dirichlet series definition to all complex numbers.

The Riemann zeta function also appears in a form similar to the Mellin transform in an integral over the Gauss–Kuzmin–Wirsing operator acting on x^{s-1}; that context gives rise to a series expansion in terms of the falling factorial.

Hadamard product

On the basis of Weierstrass's factorization theorem, Hadamard gave the infinite product expansion

$$\zeta(s) = \frac{e^{(\log(2\pi) - 1 - \gamma/2)s}}{2(s-1)\Gamma(1+s/2)} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{s/\rho},$$

where the product is over the non-trivial zeros ρ of ζ and the letter γ again denotes the Euler–Mascheroni constant. A simpler infinite product expansion is

$$\zeta(s) = \pi^{s/2} \frac{\prod_\rho \left(1 - \frac{s}{\rho}\right)}{2(s-1)\Gamma(1+s/2)}.$$

This form clearly displays the simple pole at $s = 1$, the trivial zeros at −2, −4, ... due to the gamma function term in the denominator, and the non-trivial zeros at $s = \varrho$.

Logarithmic derivative on the critical strip

$$\pi \frac{dN}{dx}(x) = \frac{1}{2i}\frac{d}{dx}\big(\log(\zeta(1/2+ix)) - \log(\zeta(1/2-ix))\big) - \frac{2}{1+4x^2} - \sum_{n=0}^{\infty} \frac{2n+1/2}{(2n+1/2)^2 + x^2}$$

where $\frac{dN(x)}{dx} = \sum_\rho \delta(x-\rho)$ is the density of zeros of ζ on the critical strip $0 < \mathrm{Re}(s) < 1$ (δ is the Dirac delta distribution, and the sum is over the nontrivial zeros ρ of ζ).

Globally convergent series

A globally convergent series for the zeta function, valid for all complex numbers s except $s = 1 + 2\pi in/\log(2)$ for some integer n, was conjectured by Konrad Knopp and proved by Helmut Hasse in 1930 (cf. Euler summation):

$$\zeta(s) = \frac{1}{1-2^{1-s}} \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \sum_{k=0}^{n} (-1)^k \binom{n}{k} (k+1)^{-s}.$$

The series only appeared in an Appendix to Hasse's paper, and did not become generally known until it was rediscovered more than 60 years later (see Sondow, 1994).

Peter Borwein has shown a very rapidly convergent series suitable for high precision numerical calculations. The algorithm, making use of Chebyshev polynomials, is described in the article on the Dirichlet eta function.

Applications

The zeta function occurs in applied statistics (see Zipf's law and Zipf–Mandelbrot law).

Zeta function regularization is used as one possible means of regularization of divergent series in quantum field theory. In one notable example, the Riemann zeta-function shows up explicitly in the calculation of the Casimir effect.

Generalizations

There are a number of related zeta functions that can be considered to be generalizations of the Riemann zeta function. These include the Hurwitz zeta function

$$\zeta(s,q) = \sum_{k=0}^{\infty} (k+q)^{-s},$$

which coincides with the Riemann zeta function when $q = 1$ (note that the lower limit of summation in the Hurwitz zeta function is 0, not 1), the Dirichlet L-functions and the Dedekind zeta-function. For other related functions see the articles Zeta function and L-function.

The polylogarithm is given by

$$\mathrm{Li}_s(z) = \sum_{k=1}^{\infty} \frac{z^k}{k^s}$$

which coincides with the Riemann zeta function when $z = 1$.

The Lerch transcendent is given by

$$\Phi(z,s,q) = \sum_{k=0}^{\infty} \frac{z^k}{(k+q)^s}$$

which coincides with the Riemann zeta function when $z = 1$ and $q = 1$ (note that the lower limit of summation in the Lerch transcendent is 0, not 1).

The Clausen function $\mathrm{Cl}_s(\theta)$ that can be chosen as the real or imaginary part of $\mathrm{Li}_s(e^{i\theta})$.

The multiple zeta functions are defined by

$$\zeta(s_1, s_2, \ldots, s_n) = \sum_{k_1 > k_2 > \cdots > k_n > 0} k_1^{-s_1} k_2^{-s_2} \cdots k_n^{-s_n}.$$

One can analytically continue these functions to the n-dimensional complex space. The special values of these functions are called multiple zeta values by number theorists and have been connected to many different branches in mathematics and physics.

Notes

[1] This paper also contained the Riemann hypothesis, a conjecture about the distribution of complex zeros of the Riemann zeta function that is considered by many mathematicians to be the most important unsolved problem in pure mathematics.Bombieri, Enrico. "The Riemann Hypothesis - official problem description" (http://www.claymath.org/millennium/Riemann_Hypothesis/riemann.pdf). Clay Mathematics Institute. . Retrieved 2008-10-25.

[2] Devlin, Keith (2002). *The Millennium Problems: The Seven Greatest Unsolved Mathematical Puzzles of Our Time*. New York: Barnes & Noble. pp. 43–47. ISBN 978-0760786598.

[3] C. S. Ogilvy & J. T. Anderson *Excursions in Number Theory*, pp. 29–35, Dover Publications Inc., 1988 ISBN 0-486-25778-9

[4] Charles Edward Sandifer, *How Euler did it*, The Mathematical Association of America, 2007, p. 193. ISBN 978-0-88385-563-8

[5] J. E. Nymann (1972). "On the probability that k positive integers are relatively prime". *Journal of Number Theory* **4** (5): 469–473. doi:10.1016/0022-314X(72)90038-8.

[6] For s an even positive integer, the product $\sin(\pi s/2)\Gamma(1-s)$ is regular and the functional equation relates the values of the Riemann zeta function at odd negative integers and even positive integers.

[7] Ford, K. *Vinogradov's integral and bounds for the Riemann zeta function*, Proc. London Math. Soc. (3) **85** (2002), pp. 565–633

[8] O. Shanker (2006). "Random matrices, generalized zeta functions and self-similarity of zero distributions". *J. Phys. A: Math. Gen.* **39**: 13983–13997. doi:10.1088/0305-4470/39/45/008.

References

- Apostol, T. M. (2010), "Zeta and Related Functions" (http://dlmf.nist.gov/25), in Olver, Frank W. J.; Lozier, Daniel M.; Boisvert, Ronald F. et al., *NIST Handbook of Mathematical Functions*, Cambridge University Press, ISBN 978-0521192255
- Riemann, Bernhard (1859). "Über die Anzahl der Primzahlen unter einer gegebenen Grösse" (http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/). *Monatsberichte der Berliner Akademie*.. In *Gesammelte Werke*, Teubner, Leipzig (1892), Reprinted by Dover, New York (1953).
- Jacques Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques*, Bulletin de la Societé Mathématique de France **14** (1896) pp 199–220.
- Helmut Hasse, *Ein Summierungsverfahren für die Riemannsche ζ-Reihe*, (1930) Math. Z. **32** pp 458–464. *(Globally convergent series expression.)*
- E. T. Whittaker and G. N. Watson (1927). *A Course in Modern Analysis*, fourth edition, Cambridge University Press (Chapter XIII).
- H. M. Edwards (1974). *Riemann's Zeta Function*. Academic Press. ISBN 0-486-41740-9.
- G. H. Hardy (1949). *Divergent Series*. Clarendon Press, Oxford.
- A. Ivic (1985). *The Riemann Zeta Function*. John Wiley & Sons. ISBN 0-471-80634-X.
- A.A. Karatsuba; S.M. Voronin (1992). *The Riemann Zeta-Function*. W. de Gruyter, Berlin.
- Hugh L. Montgomery; Robert C. Vaughan (2007). *Multiplicative number theory I. Classical theory*. Cambridge tracts in advanced mathematics. **97**. Cambridge University Press. ISBN 0-521-84903-9. Chapter 10.
- Donald J. Newman (1998). *Analytic number theory*. GTM. **177**. Springer-Verlag. ISBN 0-387-98308-2. Chapter 6.
- E. C. Titchmarsh (1986). *The Theory of the Riemann Zeta Function, Second revised (Heath-Brown) edition*. Oxford University Press.
- Jonathan Borwein, David M. Bradley, Richard Crandall (2000). "Computational Strategies for the Riemann Zeta Function" (http://www.maths.ex.ac.uk/~mwatkins/zeta/borwein1.pdf) (PDF). *J. Comp. App. Math.* **121**: p.11. (*links to PDF file*)
- Djurdje Cvijović and Jacek Klinowski (2002). "Integral Representations of the Riemann Zeta Function for Odd-Integer Arguments" (http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6TYH-451NM96-2&_user=10&_coverDate=05/15/2002&_alid=509596586&_rdoc=17&_fmt=summary&_orig=search&_cdi=5619&_sort=d&_docanchor=&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=76a759d8292edc715d10b1cb459992f1). *J. Comp. App. Math.* **142**: pp.435–439. doi:10.1016/S0377-0427(02)00358-8.

- Djurdje Cvijović and Jacek Klinowski (1997). "Continued-fraction expansions for the Riemann zeta function and polylogarithms" (http://www.ams.org/proc/1997-125-09/S0002-9939-97-04102-6/home.html). *Proc. Amer. Math. Soc.* **125**: pp.2543–2550. doi:10.1090/S0002-9939-97-04102-6.
- Jonathan Sondow, " Analytic continuation of Riemann's zeta function and values at negative integers via Euler's transformation of series (http://www.ams.org/journals/proc/1994-120-02/S0002-9939-1994-1172954-7/home.html)", Proc. Amer. Math. Soc. 120 (1994) 421–424.
- Jianqiang Zhao (1999). "Analytic continuation of multiple zeta functions" (http://www.ams.org/journal-getitem?pii=S0002-9939-99-05398-8). *Proc. Amer. Math. Soc.* **128**: pp.1275–1283.
- Guo Raoh: "The Distribution of the Logarithmic Derivative of the Riemann Zeta Function", *Proceedings of the London Mathematical Society* 1996; s3–72: 1–27
- Istvan Mezo and Ayhan Dil, *Hyperharmonic series involving Hurwitz zeta function* (http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6WKD-4XFXX96-3-5&_cdi=6904&_user=1390915&_orig=browse&_coverDate=02/28/2010&_sk=998699997&view=c&wchp=dGLzVzz-zSkWA&md5=95961c8b362bda898d6ef6896e9cd396&ie=/sdarticle.pdf), Journal of Number Theory, (2010) **130** , 2, 360-369.

External links

- Riemann Zeta Function, in Wolfram Mathworld (http://mathworld.wolfram.com/RiemannZetaFunction.html) — an explanation with a more mathematical approach
- Tables of selected zeros (http://dtc.umn.edu/~odlyzko/zeta_tables)
- Prime Numbers Get Hitched (http://seedmagazine.com/news/2006/03/prime_numbers_get_hitched.php) A general, non-technical description of the significance of the zeta function in relation to prime numbers.
- X-Ray of the Zeta Function (http://arxiv.org/abs/math/0309433v1) Visually-oriented investigation of where zeta is real or purely imaginary.
- Formulas and identities for the Riemann Zeta function (http://functions.wolfram.com/ZetaFunctionsandPolylogarithms/Zeta/) functions.wolfram.com
- Riemann Zeta Function and Other Sums of Reciprocal Powers (http://www.math.sfu.ca/~cbm/aands/page_807.htm), section 23.2 of Abramowitz and Stegun
- The Riemann Hypothesis - A Visual Exploration (http://www.youtube.com/watch?v=MsBUTuYI62k) — a visual exploration of the Riemann Hypothesis and Zeta Function

Balanced prime

A **balanced prime** is a prime number that is equal to the arithmetic mean of the nearest primes above and below. Or to put it algebraically, given a prime number p_n, where *n* is its index in the ordered set of prime numbers,

$$p_n = \frac{p_{n-1} + p_{n+1}}{2}.$$

The first few balanced primes are

5, 53, 157, 173, 211, 257, 263, 373, 563, 593, 607, 653, 733, 947, 977, 1103 (sequence A006562 [1] in OEIS).

For example, 53 is the sixteenth prime. The fifteenth and seventeenth primes, 47 and 59, add up to 106, half of which is 53, thus 53 is a balanced prime.

When 1 was considered a prime number, 2 would have correspondingly been considered the first balanced prime since

$$2 = \frac{1 + 3}{2}.$$

It is conjectured that there are infinitely many balanced primes.

Three consecutive primes in arithmetic progression is sometimes called a CPAP-3. A balanced prime is by definition the second prime in a CPAP-3. As of 2009 the largest known CPAP-3 with proven primes has 7535 digits found by David Broadhurst and François Morain:[2]

$$p_n = 197418203 \times 2^{25000} - 1, \quad p_{n-1} = p_n - 6090, \quad p_{n+1} = p_n + 6090.$$

The value of *n* is not known.

Citations

[1] http://en.wikipedia.org/wiki/Oeis%3Aa006562

[2] http://users.cybercity.dk/~dsl522332/math/cpap.htm#k3

Bell number

In combinatorics, the *n*th **Bell number**, named after Eric Temple Bell, is the number of partitions of a set with *n* members, or equivalently, the number of equivalence relations on it. Starting with $B_0 = B_1 = 1$, the first few Bell numbers are:

1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, … (sequence A000110 [1] in OEIS).

(See also breakdown by number of subsets/equivalence classes.)

Partitions of a set

In general, B_n is the number of partitions of a set of size n. A partition of a set S is defined as a set of nonempty, pairwise disjoint subsets of S whose union is S. For example, $B_3 = 5$ because the 3-element set $\{a, b, c\}$ can be partitioned in 5 distinct ways:

$\{ \{a\}, \{b\}, \{c\} \}$

$\{ \{a\}, \{b, c\} \}$

$\{ \{b\}, \{a, c\} \}$

$\{ \{c\}, \{a, b\} \}$

$\{ \{a, b, c\} \}$.

B_0 is 1 because there is exactly one partition of the empty set. Every member of the empty set is a nonempty set (that is vacuously true), and their union is the empty set. Therefore, the empty set is the only partition of itself.

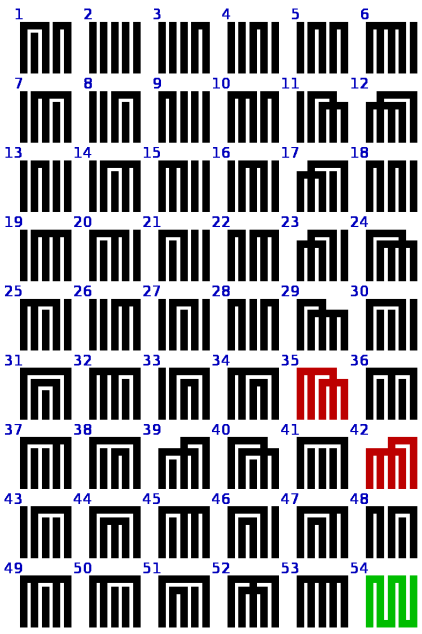
Note that, as suggested by the set notation above, we consider neither the order of the partitions nor the order of elements within each partition. This means the following partitionings are all considered identical:

$\{ \{b\}, \{a, c\} \}$

$\{ \{a, c\}, \{b\} \}$

$\{ \{b\}, \{c, a\} \}$

$\{ \{c, a\}, \{b\} \}$.



The traditional Japanese symbols for the chapters of the *Tale of Genji* are based on the 52 ways of partitioning five elements.

Another view of Bell numbers

Bell numbers can also be viewed as the number of distinct possible ways of putting *n* distinguishable balls into one or more indistinguishable boxes. For example, let us suppose *n* is 3. We have three balls, which we will label **a**, **b**, and **c**, and three boxes. If the boxes can not be distinguished from each other, there are five ways of putting the balls in the boxes:

- All three balls go in to one box. Since the boxes are anonymous, this is only considered one combination.
- **a** goes in to one box; **b** and **c** go in to another box.
- **b** goes in to one box; **a** and **c** go in to another box.
- **c** goes in to one box; **a** and **b** go in to another box.
- Each ball goes in to its own box.

Properties of Bell numbers

The Bell numbers satisfy this recursion formula:

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

They also satisfy "Dobinski's formula":

$$B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}$$

= the *n*th moment of a Poisson distribution with expected value 1.

And they satisfy "Touchard's congruence": If *p* is any prime number then

$$B_{p+n} \equiv B_n + B_{n+1} \pmod{p}.$$

or, generalizing

$$B_{p^m+n} \equiv mB_n + B_{n+1} \pmod{p}.$$

Each Bell number is a sum of Stirling numbers of the second kind

$$B_n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} = \sum_{k=0}^{n} \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n$$

The Stirling number $\left\{ {n \atop k} \right\}$ is the number of ways to partition a set of cardinality *n* into exactly *k* nonempty subsets.

More generally, the Bell numbers satisfy the following recurrence[2] :

$$B_{n+m} = \sum_{k=0}^{n} \sum_{j=0}^{m} \left\{ {m \atop j} \right\} \binom{n}{k} j^{n-k} B_k.$$

The *n*th Bell number is also the sum of the coefficients in the polynomial that expresses the *n*th moment of any probability distribution as a function of the first *n* cumulants; this way of enumerating partitions is not as coarse as that given by the Stirling numbers.

The exponential generating function of the Bell numbers is

$$\sum_{n=0}^{\infty} \frac{B_n}{n!} x^n = e^{e^x - 1}.$$

Asymptotic limit and bounds

Several asymptotic formulae for the Bell numbers are known. One such is

$$B_n \sim \frac{1}{\sqrt{n}} \left[\lambda\left(n\right)\right]^{n+\frac{1}{2}} e^{\lambda(n)-n-1}.$$

Here

$$\lambda(n) = e^{W(n)} = \frac{n}{W(n)},$$

where *W* is the Lambert W function.

(Lovász, 1993)

In (Berend, D. and Tassa, T., 2010), the following bounds were established:

$$B_n < \left(\frac{0.792n}{\ln(n+1)} \right)^n ;$$

moreover, if $\varepsilon > 0$ then for all $n > n_0(\varepsilon)$,

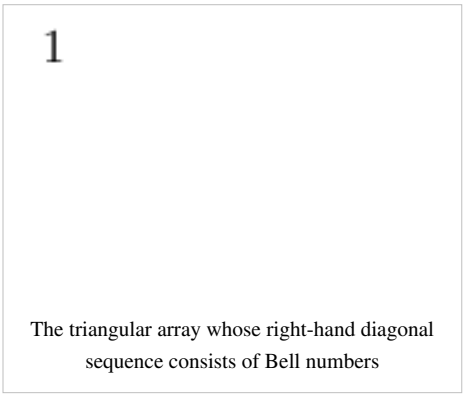
$$B_n < \left(\frac{e^{-0.6+\varepsilon}n}{\ln(n+1)}\right)^n$$

where $n_0(\varepsilon) = \max\left\{e^4, d^{-1}(\varepsilon)\right\}$ and $d(x) := \ln\ln(x+1) - \ln\ln x + \frac{1+e^{-1}}{\ln x}$.

Triangle scheme for calculating Bell numbers

The Bell numbers can easily be calculated by creating the so-called **Bell triangle**, also called **Aitken's array** or the **Peirce triangle**:

1. Start with the number one. Put this on a row by itself.
2. Start a new row with the rightmost element from the previous row as the leftmost number
3. Determine the numbers not on the left column by taking the sum of the number to the left and the number above the number to the left (the number diagonally up and left of the number we are calculating)
4. Repeat step three until there is a new row with one more number than the previous row
5. The number on the left hand side of a given row is the *Bell number* for that row.



The triangular array whose right-hand diagonal sequence consists of Bell numbers

For example, the first row is made by placing one by itself. The next (second) row is made by taking the rightmost number from the previous row (1), and placing it on a new row. We now have a structure like this:

```
1
1  ''x''
```

The value *x* here is determined by adding the number to the left of *x* (one) and the number above the number to the left of *x* (also one).

```
1
1  2
y
```

The value *y* is determined by copying over the number from the right of the previous row. Since the number on the right hand side of the previous row has a value of 2, *y* is given a value of two.

```
1
1  2
2  3  ''x''
```

Again, since *x* is not the leftmost element of a given row, its value is determined by taking the sum of the number to *x*'s left (three) and the number above the number to *x*'s left (two). The sum is five.

Here is the first five rows of this triangle:

```
 1
 1  2
 2  3  5
 5  7 10 15
15 20 27 37 52
```

The fifth row is calculated thus:

- Take 15 from the previous row
- 15 + 5 = 20
- 20 + 7 = 27
- 27 + 10 = 37
- 37 + 15 = 52

Computer program

The following is example code in the Ruby programming language that prints out all the Bell numbers from the 1st to the 300th inclusive (the limits can be adjusted)

```
#!/usr/bin/env ruby

def print_bell_numbers(start, finish)
    # Initialize the Bell triangle as a two-dimensional array
    triangle = Array[Array[1]]

    # Make sure "start" is less than "finish", and both numbers are at
least 1
    (finish, start = start, finish) if finish < start
    start = 1 if start < 1
    finish = 1 if finish < 1

    1.upto(finish-1) do |row_num|

        # Set the first element of the current row to be the last
element
        # of the previous row
        current_row = [triangle[row_num-1][row_num-1]]

        # Calculate the rest of the elements in this row, then add the
row
        # to the Bell triangle
        1.upto(row_num) do |col_num|
            sum = triangle[row_num-1][col_num-1] +
current_row[col_num-1]
            current_row.push(sum)
        end

        triangle[row_num] = current_row

    end

    # Print out the Bell numbers
    start.upto(finish) do |num|
        puts triangle[num-1][0]
    end
end
```

```
# Adjust the limits here
print_bell_numbers(1, 300)
```

The number in the nth row and kth column is the number of partitions of $\{1, ..., n\}$ such that n is not together in one class with any of the elements $k, k + 1, ..., n - 1$. For example, there are 7 partitions of $\{1, ..., 4\}$ such that 4 is not together in one class with either of the elements 2, 3, and there are 10 partitions of $\{1, ..., 4\}$ such that 4 is not together in one class with element 3. The difference is due to 3 partitions of $\{1, ..., 4\}$ such that 4 is together in one class with element 2, but not with element 3. This corresponds to the fact that there are 3 partitions of $\{1, ..., 3\}$ such that 3 is not together in one class with element 2: for counting partitions two elements which are always in one class can be treated as just one element. The 3 appears in the previous row of the table.

Prime Bell numbers

The first few Bell numbers that are primes are:

2, 5, 877, 27644437, 35742549198872617291353508656626642567, 359334085968622831041960188598043661065388726959079837

corresponding to the indices 2, 3, 7, 13, 42 and 55 (sequence A051130 [3] in OEIS).

The next prime is B_{2841}, which is approximately $9.30740105 \times 10^{6538}$. [4] As of 2006, it is the largest known prime Bell number. Phil Carmody showed it was a probable prime in 2002. After 17 months of computation with Marcel Martin's ECPP program Primo, Ignacio Larrosa Cañestro proved it to be prime in 2004. He ruled out any other possible primes below B_{6000}, later extended to B_{30447} by Eric Weisstein.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa000110

[2] Spivey, Michael (2008), "A Generalized Recurrence for Bell Numbers" (http://www.cs.uwaterloo.ca/journals/JIS/VOL11/Spivey/spivey25.pdf), *Journal of Integer Sequences* **11**,

[3] http://en.wikipedia.org/wiki/Oeis%3Aa051130

[4] http://primes.utm.edu/primes/page.php?id=68825

- Gian-Carlo Rota (1964). "The Number of Partitions of a Set". *American Mathematical Monthly* **71** (5): 498–504. doi:10.2307/2312585. MR0161805.
- Lovász, L. (1993). *Combinatorial Problems and Exercises* (2nd ed. ed.). Amsterdam, Netherlands: North-Holland.
- Berend, D.; Tassa, T. (2010). "Improved Bounds on Bell Numbers and on Moments of Sums of Random Variables". *Probability and Mathematical Statistics* (http://www.math.uni.wroc.pl/~pms/index.php) **30** (2): 185–205.

External links

- Robert Dickau. "Diagrams of Bell numbers" (http://mathforum.org/advanced/robertd/bell.html).
- Pat Ballew. "Bell numbers" (http://www.pballew.net/Bellno.html).
- Weisstein, Eric W., " Bell Number (http://mathworld.wolfram.com/BellNumber.html)" from MathWorld.
- Wagstaff, Samuel S. (1996). "Aurifeuillian factorizations and the period of the Bell numbers modulo a prime" (http://homes.cerias.purdue.edu/~ssw/bell/bell.ps). *Mathematics of computation* **65** (213): 383–391. doi:10.1090/S0025-5718-96-00683-7. MR1325876 Bibcode: 1996MaCom..65..383W.
- Gottfried Helms. "Further properties & Generalization of Bell-Numbers" (http://go.helms-net.de/math/binomial/04_5_SummingBellStirling.pdf).

Carol number

A **Carol number** is an integer of the form $4^n - 2^{n+1} - 1$. An equivalent formula is $(2^n - 1)^2 - 2$. The first few Carol numbers are: –1, 7, 47, 223, 959, 3967, 16127, 65023, 261119, 1046527 (sequence A093112 [1] in OEIS). Carol numbers were first studied by Cletus Emmanuel, who named them after a friend, Carol G. Kirnon.[2] [3]

For $n > 2$, the binary representation of the n-th Carol number is $n - 2$ consecutive ones, a single zero in the middle, and $n + 1$ more consecutive ones, or to put it algebraically,

$$\sum_{i \neq n+2}^{2n} 2^{i-1}.$$

So, for example, 47 is 101111 in binary, 223 is 11011111, etc. The difference between the $2n$-th Mersenne number and the n-th Carol number is 2^{n+1}. This gives yet another equivalent expression for Carol numbers, $(2^{2n} - 1) - 2^{n+1}$. The difference between the n-th Kynea number and the n-th Carol number is the $(n + 2)$th power of two.

Starting with 7, every third Carol number is a multiple of 7. Thus, for a Carol number to also be a prime number, its index n cannot be of the form $3x + 2$ for $x > 0$. The first few Carol numbers that are also prime are 7, 47, 223, 3967, 16127 (these are listed in Sloane's A091516 [4]). As of July 2007, the largest known Carol number that is also a prime is the Carol number for $n = 253987$, which has 152916 digits.[5] [6] It was found by Cletus Emmanuel in May 2007, using the programs MultiSieve and PrimeFormGW. It is the 40th Carol prime.

The 7th Carol number and 5th Carol prime, 16127, is also a prime when its digits are reversed, so it is the smallest Carol emirp.[7] The 12th Carol number and 7th Carol prime, 16769023, is also a Carol emirp.[8]

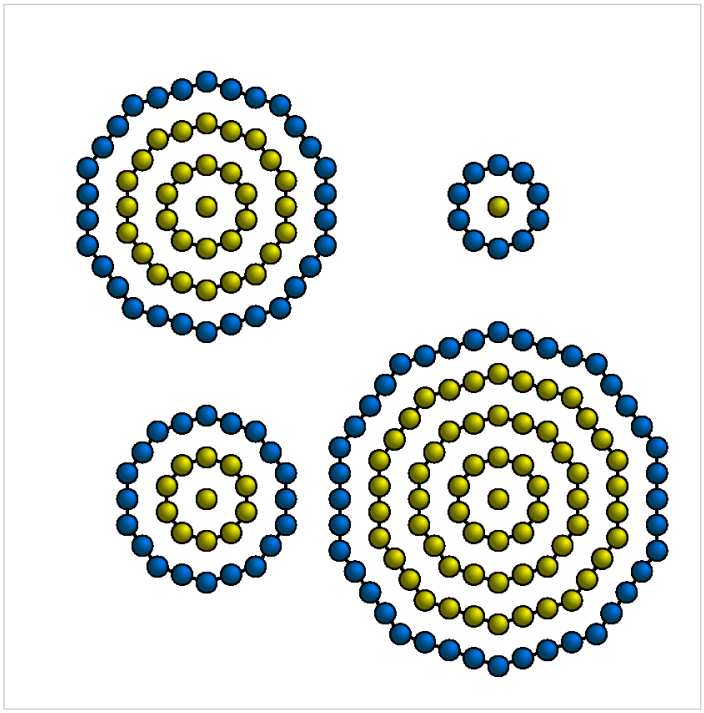
References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa093112
[2] Cletus Emmanuel (http://primes.utm.edu/bios/page.php?id=374) at Prime Pages
[3] Message to Yahoo primenumbers group (http://tech.groups.yahoo.com/group/primenumbers/message/14584) from Cletus Emmanuel
[4] http://en.wikipedia.org/wiki/Oeis%3Aa091516
[5] Entry for 253987th Carol number (http://primes.utm.edu/primes/page.php?id=80384) at Prime Pages
[6] Carol Primes and Kynea Primes (http://harvey563.tripod.com/Carol_Kynea.txt) by Steven Harvey
[7] Prime Curios 16127 (http://primes.utm.edu/curios/page.php/16127.html) at Prime Pages
[8] Prime Curios 16769023 (http://primes.utm.edu/curios/page.php/16769023.html) at Prime Pages

External links

- Weisstein, Eric W., " Near-Square Prime (http://mathworld.wolfram.com/Near-SquarePrime.html)" from MathWorld.
- Prime Database entry for Carol(226749) (http://primes.utm.edu/primes/page.php?id=73109)
- Prime Database entry for Carol(248949) (http://primes.utm.edu/primes/page.php?id=77385)

Centered decagonal number



A **centered decagonal number** is a centered figurate number that represents a decagon with a dot in the center and all other dots surrounding the center dot in successive decagonal layers. The centered decagonal number for *n* is given by the formula

$$5(n^2 - n) + 1$$

Thus, the first few centered decagonal numbers are

1, 11, 31, 61, 101, 151, 211, 281, 361, 451, 551, 661, 781, 911, 1051, ... (sequence A062786 [1] in OEIS)

Like any other centered *k*-gonal number, the *n*th centered decagonal number can reckoned by multiplying the (*n* - 1)th triangular number by *k*, 10 in this case, then adding 1. As a consequence of performing the calculation in base 10, the centered decagonal numbers can be obtained by simply adding a 1 to the right of each triangular number. Therefore, all centered decagonal numbers are odd and in base 10 always end in 1.

Another consequence of this relation to triangular numbers is the simple recurrence relation for centered decagonal numbers

$$CD_n = CD_{n-1} + 10(n - 1)$$

where CD_1 is 1.

Centered decagonal prime

A **centered decagonal prime** is a centered decagonal number that is prime. The first few centered decagonal primes are

11, 31, 61, 101, 151, 211, 281, 661, 911, 1051, 1201, 1361, 1531, 1901, 2311, 2531, 3001, 3251, 3511, 4651, 5281, ...

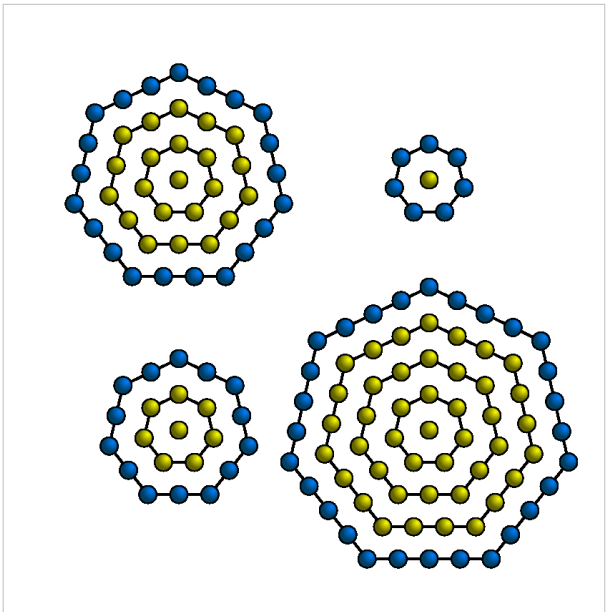
See also regular decagonal number.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa062786

Centered heptagonal number

A **centered heptagonal number** is a centered figurate number that represents a heptagon with a dot in the center and all other dots surrounding the center dot in successive heptagonal layers. The centered heptagonal number for *n* is given by the formula



$$\frac{7n^2 - 7n + 2}{2}.$$

This can also be calculated by multiplying the triangular number for (*n* - 1) by 7, then adding 1.

The first few centered heptagonal numbers are

1, 8, 22, 43, 71, 106, 148, 197, 253, 316, 386, 463, 547, 638, 736, 841, 953 (sequence A069099 [1] in OEIS)

Centered heptagonal numbers alternate parity in the pattern odd-even-even-odd.

Centered heptagonal prime

A **centered heptagonal prime** is a centered heptagonal number that is prime. The first few centered heptagonal primes are

43, 71, 197, 463, 547, 953, 1471, 1933, 2647, 2843, 3697, ... (sequence A144974 [2] in OEIS)

and centered heptagonal twin prime numbers are

43, 71, 197, 463, 1933, 5741, 8233, 9283, 11173, 14561, 34651, ... (A144975 [3]).

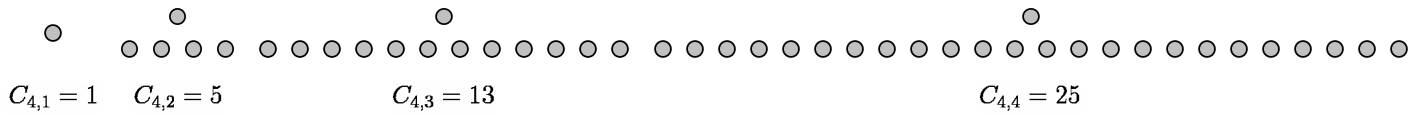
References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa069099
[2] http://en.wikipedia.org/wiki/Oeis%3Aa144974
[3] http://en.wikipedia.org/wiki/Oeis%3Aa144975

Centered square number

In elementary number theory, a **centered square number** is a centered figurate number that gives the number of dots in a square with a dot in the center and all other dots surrounding the center dot in successive square layers. That is, each centered square number equals the number of dots within a given city block distance of the center dot on a regular square lattice. While centered square numbers, like figurate numbers in general, have few if any direct practical applications, they are sometimes studied in recreational mathematics for their elegant geometric and arithmetic properties.

The figures for the first four centered square numbers are shown below:



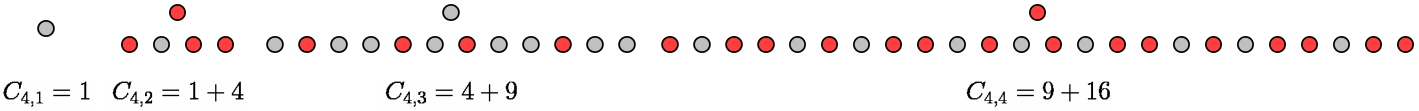
$C_{4,1} = 1$ $C_{4,2} = 5$ $C_{4,3} = 13$ $C_{4,4} = 25$

Relationships with other figurate numbers

The *n*th centered square number is given by the formula

$$C_{4,n} = n^2 + (n-1)^2.$$

In other words, a centered square number is the sum of two consecutive square numbers. The following pattern demonstrates this formula:

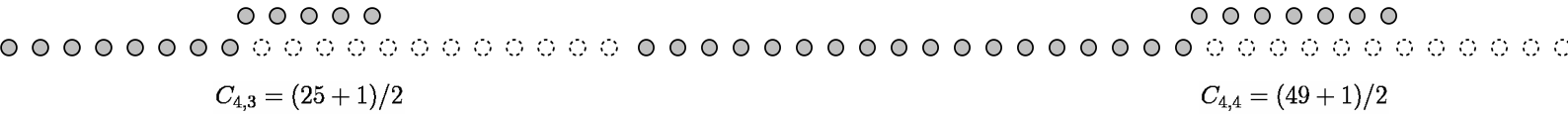


$C_{4,1} = 1$ $C_{4,2} = 1 + 4$ $C_{4,3} = 4 + 9$ $C_{4,4} = 9 + 16$

The formula can also be expressed as

$$C_{4,n} = \frac{(2n-1)^2 + 1}{2};$$

that is, *n* th centered square number is half of *n* th odd square number plus one, as illustrated below:



$C_{4,3} = (25+1)/2$ $C_{4,4} = (49+1)/2$

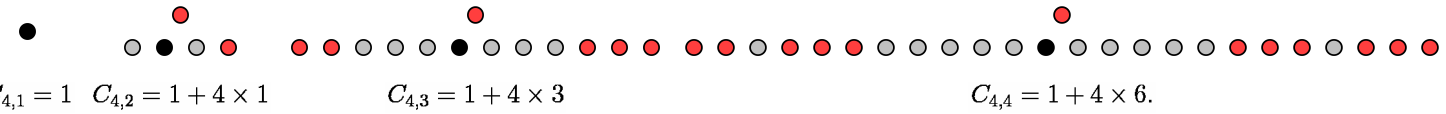
Like all centered polygonal numbers, centered square numbers can also be expressed in terms of triangular numbers:

$$C_{4,n} = 1 + 4\,T_{n-1},$$

where

$$T_n = \frac{n(n+1)}{2} = \frac{n^2+n}{2} = \binom{n+1}{2}$$

is the *n*th triangular number. This can be easily seen by removing the center dot and dividing the rest of the figure into four triangles, as below:



$C_{4,1} = 1$ $C_{4,2} = 1 + 4 \times 1$ $C_{4,3} = 1 + 4 \times 3$ $C_{4,4} = 1 + 4 \times 6.$

Properties

The first few centered square numbers are:

> 1, 5, 13, 25, 41, 61, 85, 113, 145, 181, 221, 265, 313, 365, 421, 481, 545, 613, 685, 761, 841, 925, 1013, 1105, 1201, 1301, 1405, 1513, 1625, 1741, 1861, 1985, 2113, 2245, 2381, 2521, 2665, 2813, 2965, 3121, 3281, 3445, 3613, 3785, 3961, 4141, 4325, … (sequence A001844 [1] in OEIS).

All centered square numbers are odd, and in base 10 one can notice the one's digits follows the pattern 1-5-3-5-1.

All centered square numbers and their divisors have a remainder of one when divided by four. Hence all centered square numbers and their divisors end with digits 1 or 5 in base 6, 8 or 12.

All centered square numbers except 1 are the third term of a Leg-Hypotenuse Pythagorean triple (for example, 3-4-5, 5-12-13).

Centered square prime

A **centered square prime** is a centered square number that is prime. Unlike regular square numbers, which are never prime, quite a few of the centered square numbers are prime. The first few centered square primes are:

> 5, 13, 41, 61, 113, 181, 313, 421, 613, 761, 1013, 1201, 1301, 1741, 1861, 2113, 2381, 2521, 3121, 3613, … (sequence A027862 [2] in OEIS).

References

- U. Alfred, "*n* and *n* + 1 consecutive integers with equal sums of squares", *Math. Mag.*, **35** (1962): 155–164.
- Apostol, Tom M. (1976), *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, New York-Heidelberg: Springer-Verlag, MR0434929, ISBN 978-0-387-90163-3
- A. H. Beiler, *Recreations in the Theory of Numbers*. New York: Dover (1964): 125
- Conway, J. H. and Guy, R. K. *The Book of Numbers*. New York: Springer-Verlag, pp. 41–42, 1996. ISBN 0-387-97993-X

External links

- (n^2 + 1) / 2 as a special case of M(i,j) = (i^2 + j) / 2 [3]

References

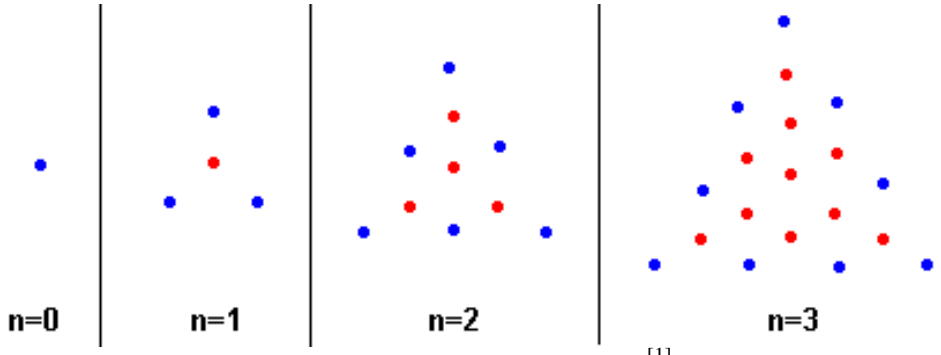
[1] http://en.wikipedia.org/wiki/Oeis%3Aa001844
[2] http://en.wikipedia.org/wiki/Oeis%3Aa027862
[3] http://www.muljadi.org/Median.htm

Centered triangular number

A **centered triangular number** is a centered figurate number that represents a triangle with a dot in the center and all other dots surrounding the center in successive triangular layers. The centered triangular number for *n* is given by the formula

$$\frac{3n^2+3n+2}{2}.$$

The following image shows the building of the centered triangular numbers using the associated figures: at each step the previous figure, shown in red, is surrounded by a triangle of new points, in blue.



The first few centered triangular numbers (sequence A005448 [1] in OEIS) are

1, 4, 10, 19, 31, 46, 64, 85, 109, 136, 166, 199, 235, 274, 316, 361, 409, 460, 514, 571, 631, 694, 760, 829, 901, 976, 1054, 1135, 1219, 1306, 1396, 1489, 1585, 1684, 1786, 1891, 1999, 2110, 2224, 2341, 2461, 2584, 2710, 2839, 2971

Each centered triangular number from 10 onwards is the sum of three consecutive regular triangular numbers. Also each centred triangular number has a remainder of 1 when divided by three and the quotient (if positive) is the previous regular triangular number.

The sum of the first *n* centered triangular numbers is the magic constant for an *n* by *n* normal magic square for $n > 2$.

Centered triangular prime

A **centered triangular prime** is a centered triangular number that is prime. The first few centered triangular primes are (sequence A125602 [2] in OEIS)

19, 31, 109, 199, 409, ...

(corresponding to n: 3, 4, 8, 11, 16, ...)

References

- Lancelot Hogben: *Mathematics for the Million*.(1936), republished by W. W. Norton & Company (September 1993), ISBN 978-0393310719
- Weisstein, Eric W., "Centered Triangular Number [3]" from MathWorld.
- On-Line Encyclopedia of Integer Sequences, sequence A005448 [1] and A125602 [2].

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa005448
[2] http://en.wikipedia.org/wiki/Oeis%3Aa125602
[3] http://mathworld.wolfram.com/CenteredTriangularNumber.html

Chen prime

Publication year	1973[Note 1]
Author of publication	Yuan, W.
Number of known cases	?
OEIS index and link	A109611 [1]

A prime number p is called a **Chen prime** if $p + 2$ is either a prime or a product of two primes. The even number $2p + 2$ therefore satisfies Chen's theorem.

In 1966, Chen Jingrun proved that there are infinitely many such primes. This result would also follow from the truth of the twin prime conjecture.

The first few Chen primes are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, 53, 59, 67, 71, 83, 89, 101, … (sequence A109611 [1] in OEIS).

The first few Chen primes that are not the lower member of a pair of twin primes are

2, 7, 13, 19, 23, 31, 37, 47, 53, 67, 83, 89, 109, 113, 127, ... A063637 [2].

The first few non-Chen primes are

43, 61, 73, 79, 97, 103, 151, 163, 173, 193, 223, 229, 241, … A102540 [3].

All of the supersingular primes are Chen primes.

Rudolf Ondrejka discovered the following 3x3 magic square of nine Chen primes:[4]

17	89	71
113	59	5
47	29	101

The lower member of a pair of twin primes is a Chen prime, by definition. In August 2009 Twin Prime Search and Primegrid found the largest known Chen prime, $65516468355 \cdot 2^{333333} - 1$ with 100355 digits.

Further results

Chen also proved the following generalization: For any even integer h, there exist infinitely many primes p such that $p + h$ is either a prime or a semiprime.

Terence Tao and Ben Green proved in 2005 that there are infinitely many three-term arithmetic progressions of Chen primes. Recently, Binbin Zhou proved that the Chen primes contain arbitrarily long arithmetic progressions.

Notes

1.^ Chen primes were first described by Yuan, W. On the Representation of Large Even Integers as a Sum of a Product of at Most 3 Primes and a Product of at Most 4 Primes [5], Scienca Sinica **16**, 157-176, 1973.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa109611

[2] http://en.wikipedia.org/wiki/Oeis%3Aa063637

[3] http://en.wikipedia.org/wiki/Oeis%3Aa102540

[4] Prime Curios! page on 59 (http://primes.utm.edu/curios/page.php/59.html)

[5] http://www.google.de/url?sa=t&source=web&cd=1&ved=0CBoQFjAA&url=http%3A%2F%2Fwww.worldscibooks.com%2Fetextbook%2F5774%2F5774_chap1.pdf&rct=j&q=On%20the%20Representation%20of%20a%20Large%20Even%20Integer%20as%20the%20Sum%20of%20a%20Prime%20and%20the%20Product%20of%20ei=EIvvTJqtLYTNswamjJ35Cg&usg=AFQjCNFQdqpZ4ig24WuhCrc10tdPCXOo0w&cad=rja

External links

- The Prime Pages (http://primes.utm.edu/)
- Green, Ben; Tao, Terence (2006). "Restriction theory of the Selberg sieve, with applications" (http://www.emis.de/journals/JTNB/2006-1/jtnb18-1_english.html). *Journal de théorie des nombres de Bordeaux* **18** (1): 147–182. arXiv:math.NT/0405581.
- Weisstein, Eric W., " Chen Prime (http://mathworld.wolfram.com/ChenPrime.html)" from MathWorld.
- The Chen primes contain arbitrarily long arithmetic progressions, Binbin Zhou, Acta Arith. 138 (2009), 301-315 (http://journals.impan.gov.pl/aa/Inf/138-4-1.html)

Circular prime

A **circular prime** is a prime number that remains prime on any cyclic rotation of its (base 10) digits.[1] [2] For example 1193 is a circular prime, since 1931, 9311 and 3119 all are also prime.[3] A circular prime with at least two digits can only consist of combinations of the digits 1, 3, 7 or 9, because having 0, 2, 4, 6 or 8 as the last digit makes the number divisible by 2, and having 0 or 5 as the last digit makes it divisible by 5.[1] The known circular primes are 2, 3, 5, 7, R_2, 13, 17, 37, 79, 113, 197, 199, 337, 1193, 3779, 11939, 19937, 193939, 199933, R_{19}, R_{23}, R_{317} and R_{1031}, where R_n is a repunit prime with n digits, and there are no other circular primes up to 10^{23}.[3] Note that this list contains only the smallest prime of each "circle", thus omitting for example 31, as it belongs to the same circle as 13. Another type of primes related to the circular primes are the permutable primes, which are a subset of the circular primes (every permutable prime is also a circular prime, but not necessarily vice versa).

References

[1] *The Universal Book of Mathematics* (http://books.google.de/books?id=nnpChqstvg0C&pg=PA70&dq=circular+prime&hl=de&ei=4TVMTLTOMYSD4Qag-MSaDA&sa=X&oi=book_result&ct=result&resnum=4&ved=0CDcQ6AEwAw#v=onepage&q=circular prime&f=false), Darling, David J., , retrieved 25 July 2010 (see page 70)

[2] *Prime Numbers - The Most Mysterious Figures in Math* (http://wenku.baidu.com/view/8d95d909581b6bd97f19ea85.html), Wells, D., , retrieved 27 July 2010 (see page 47 (page 28 of the book))

[3] *Circular Primes* (http://www.worldofnumbers.com/circular.htm), Patrick De Geest, , retrieved 25 July 2010

External links

- A016114 (http://oeis.org/classic/A016114) at OEIS
- Circular, Permutable, Truncatable and Deletable primes (http://web.archive.org/web/20041204160717/www.wschnei.de/digit-related-numbers/circular-primes.html)

Cousin prime

In mathematics, **cousin primes** are prime numbers that differ by four; compare this with twin primes, pairs of prime numbers that differ by two, and sexy primes, pairs of prime numbers that differ by six. The cousin primes (sequences A023200 [1] and A046132 [2] in OEIS) below 1000 are:

(3, 7), (7, 11), (13, 17), (19, 23), (37, 41), (43, 47), (67, 71), (79, 83), (97, 101), (103, 107), (109, 113), (127, 131), (163, 167), (193, 197), (223, 227), (229, 233), (277, 281), (307, 311), (313, 317), (349, 353), (379, 383), (397, 401), (439, 443), (457, 461), (463,467), (487, 491), (499, 503), (613, 617), (643, 647), (673, 677), (739, 743), (757, 761), (769, 773), (823, 827), (853, 857), (859, 863), (877, 881), (883, 887), (907, 911), (937, 941), (967, 971)

As of May 2009 the largest known cousin prime was (p, p+4) for

p = (311778476·587502·9001#·(587502·9001#+1)+210)·(587502·9001#−1)/35+1

where 9001# is a primorial. It was found by Ken Davis and has 11594 digits.[3]

The largest known cousin probable prime is

$474435381 \cdot 2^{98394} - 1$

$474435381 \cdot 2^{98394} - 5$.

It has 29629 digits and was found by Angel, Jobling and Augustin.[4] While the first of these numbers has been proven prime, there is no known primality test to easily determine whether the second number is prime.

It follows from the first Hardy–Littlewood conjecture that cousin primes have the same asymptotic density as twin primes. An analogy of Brun's constant for twin primes can be defined for cousin primes, with the initial term (3, 7) omitted:

$$B_4 = \left(\frac{1}{7} + \frac{1}{11}\right) + \left(\frac{1}{13} + \frac{1}{17}\right) + \left(\frac{1}{19} + \frac{1}{23}\right) + \cdots.$$

Using cousin primes up to 2^{42}, the value of B_4 was estimated by Marek Wolf in 1996 as

$B_4 \approx 1.1970449$.[5]

This constant should not be confused with Brun's constant for prime quadruplets, which is also denoted B_4.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa023200

[2] http://en.wikipedia.org/wiki/Oeis%3Aa046132

[3] Davis, Ken (2009-05-08). "11594 digit cousin prime pair" (http://tech.groups.yahoo.com/group/primenumbers/message/20235). *primenumbers mailing list*. . Retrieved 2009-05-09.

[4] http://primes.utm.edu/primes/page.php?id=60270

[5] Marek Wolf, *On the Twin and Cousin Primes* (http://www.ift.uni.wroc.pl/~mwolf/twins_ps.ps) (PostScript file).

- Weisstein, Eric W., " Cousin Primes (http://mathworld.wolfram.com/CousinPrimes.html)" from MathWorld.

Cuban prime

A **cuban prime** is a prime number that is a solution to one of two different specific equations involving third powers of *x* and *y*. The first of these equations is:

$$p = \frac{x^3 - y^3}{x - y},\ x = y + 1,\ y > 0$$

and the first few cuban primes from this equation are (sequence A002407 [1] in OEIS):

7, 19, 37, 61, 127, 271, 331, 397, 547, 631, 919, 1657, 1801, 1951, 2269, 2437, 2791, 3169, 3571, 4219, 4447, 5167, 5419, 6211, 7057, 7351, 8269, 9241, 10267, 11719, 12097, 13267, 13669, 16651, 19441, 19927, 22447, 23497, 24571, 25117, 26227

The general cuban prime of this kind can be rewritten as $\frac{(y+1)^3-y^3}{y+1-y}$, which simplifies to $3y^2 + 3y + 1$. This is exactly the general form of a centered hexagonal number; that is, all of these cuban primes are centered hexagonal. This kind of cuban primes has been researched by A. J. C. Cunningham, in a paper entitled *On quasi-Mersennian numbers*.

As of January 2006 the largest known has 65537 digits with $y = 100000845^{4096}$[2], found by Jens Kruse Andersen.
The second of these equations is:

$$p = \frac{x^3 - y^3}{x - y},\ x = y + 2.$$

It simplifies to $3y^2 + 6y + 4$. The first few cuban primes on this form are (sequence A002648 [3] in OEIS):

13, 109, 193, 433, 769, 1201, 1453, 2029, 3469, 3889, 4801, 10093, 12289, 13873, 18253, 20173, 21169, 22189, 28813, 37633, 43201, 47629, 60493, 63949, 65713, 69313

This kind of cuban primes have also been researched by Cunningham, in his book *Binomial Factorisations*.

The name "cuban prime" has to do with the role cubes (third powers) play in the equations, and has nothing to do with Cuba.

See also

- Cubic function
- List of prime numbers
- Prime number

References

- Phil Carmody, Eric W. Weisstein and Ed Pegg, Jr., "Cuban Prime [4]" from MathWorld.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa002407
[2] http://primes.utm.edu/primes/page.php?id=76705#comments
[3] http://en.wikipedia.org/wiki/Oeis%3Aa002648
[4] http://mathworld.wolfram.com/CubanPrime.html

Cullen number

In mathematics, a **Cullen number** is a natural number of the form $n \cdot 2^n + 1$ (written C_n). Cullen numbers were first studied by Fr. James Cullen in 1905. Cullen numbers are special cases of Proth numbers.

In 1976 Christopher Hooley showed that the natural density of positive integers $n \leq x$ for which C_n is a prime is of the order *o(x)* for $x \to \infty$. In that sense, almost all Cullen numbers are composite. Hooley's proof was reworked by Hiromi Suyama to show that it works for any sequence of numbers $n \cdot 2^{n+a} + b$ where *a* and *b* are integers, and in particular also for Woodall numbers. The only known **Cullen primes** are those for *n* equal:

> 1, 141, 4713, 5795, 6611, 18496, 32292, 32469, 59656, 90825, 262419, 361275, 481899, 1354828, 6328548, 6679881 (sequence A005849 [1] in OEIS).

Still, it is conjectured that there are infinitely many Cullen primes.

As of August 2009, the largest known Cullen prime is $6679881 \times 2^{6679881} + 1$. It is a megaprime with 2,010,852 digits and was discovered by a PrimeGrid participant from Japan.[2]

A Cullen number C_n is divisible by $p = 2n - 1$ if *p* is a prime number of the form 8*k* - 3; furthermore, it follows from Fermat's little theorem that if *p* is an odd prime, then p divides $C_{m(k)}$ for each $m(k) = (2^k - k) \quad (p - 1) - k$ (for $k > 0$). It has also been shown that the prime number *p* divides $C_{(p+1)/2}$ when the Jacobi symbol $(2 \mid p)$ is −1, and that *p* divides $C_{(3p-1)/2}$ when the Jacobi symbol $(2 \mid p)$ is +1.

It is unknown whether there exists a prime number *p* such that C_p is also prime.

Sometimes, a **generalized Cullen number** is defined to be a number of the form $n \cdot b^n + 1$, where $n + 2 > b$; if a prime can be written in this form, it is then called a **generalized Cullen prime**. Woodall numbers are sometimes called **Cullen numbers of the second kind**.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa005849

[2] "The Prime Database: 6679881*2^6679881+1" (http://primes.utm.edu/primes/page.php?id=89536), *Chris Caldwell's The Largest Known Primes Database*, , retrieved December 22, 2009

Further reading

- Cullen, James (December 1905), "Question 15897", *Educ. Times*: 534.
- Guy, Richard K. (2004), *Unsolved Problems in Number Theory* (3rd ed.), New York: Springer Verlag, pp. section B20, ISBN 0387208607.
- Hooley, Christopher (1976), *Applications of sieve methods*, New York: Cambridge University Press, pp. 115–119, ISBN 0521209153.
- Keller, Wilfrid (1995), "New Cullen Primes" (http://www.ams.org/mcom/1995-64-212/S0025-5718-1995-1308456-3/S0025-5718-1995-1308456-3.pdf), *Mathematics of Computation* **64** (212): 1733–1741.

External links

- Chris Caldwell, The Top Twenty: Cullen primes (http://primes.utm.edu/top20/page.php?id=6) at The Prime Pages.
- The Prime Glossary: Cullen number (http://primes.utm.edu/glossary/page.php?sort=Cullens) at The Prime Pages.
- Weisstein, Eric W., " Cullen number (http://mathworld.wolfram.com/CullenNumber.html)" from MathWorld.
- Cullen prime: definition and status (http://www.prothsearch.net/cullen.html) (outdated), Cullen Prime Search is now hosted at PrimeGrid

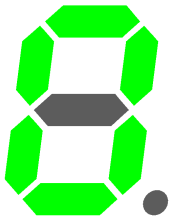
Dihedral prime

A **dihedral prime** or **dihedral calculator prime** is a prime number that still reads like itself or another prime number when read in a seven-segment display, regardless of orientation (normally or upside down), and surface (actual display or reflection on a mirror). The first few decimal dihedral primes are

> 2, 5, 11, 101, 181, 1181, 1811, 18181, 108881, 110881, 118081, 120121, 121021, 121151, 150151, 151051, 151121, 180181, 180811, 181081 (sequence A038136 [1] in OEIS).[2]

The smallest dihedral prime that reads differently with each orientation and surface combination is 120121 which becomes 121021 (upside down), 151051 (mirrored), and 150151 (both upside down and mirrored).

The digits 0, 1 and 8 remain the same regardless of orientation or surface (the fact that 1 moves from the right to the left of the seven-segment cell when reversed is ignored). 2 and 5 remain the same when viewed upside down, and turn into each other when reflected in a mirror. In the display of a calculator that can handle hexadecimal, 3 would become E reflected, but E being an even digit, the 3 can't be used as the first digit because the reflected number will be even. Though 6 and 9 become each other upside down, they are not valid digits when reflected, at least not in any of the numeral systems pocket calculators usually operate in.



LED-based 7-segment display showing the 16 hex digits.

Strobogrammatic primes that don't use 6 or 9 are dihedral primes. This includes repunit primes and all other palindromic primes which only contain digits 0, 1 and 8 (in binary, all palindromic primes are dihedral). It appears to be unknown whether there exist infinitely many dihedral primes, but this would follow from the conjecture that there are infinitely many repunit primes.

The palindromic prime $10^{180054} + 8\times(10^{58567}-1)/9\times10^{60744} + 1$, discovered in 2009 by Darren Bedwell, is 180055 digits long and may be the largest known dihedral prime as of 2009.[3]

Notes

[1] http://en.wikipedia.org/wiki/Oeis%3Aa038136

[2] A038136 (http://en.wikipedia.org/wiki/Oeis:a038136) misses the dihedral prime 5. Retrieved on 2008-10-05.

[3] Chris Caldwell, *The Top Twenty: Palindrome* (http://primes.utm.edu/top20/page.php?id=53). Retrieved on 2009-09-16

References

- Mike Keith. "Puzzle 39.- The Mirrorable Numbers" (http://www.primepuzzles.net/puzzles/puzz_039.htm). *The prime puzzles & problems connection*.
- Eric W. Weisstein. "Dihedral Prime" (http://mathworld.wolfram.com/DihedralPrime.html). *MathWorld − A Wolfram Web Resource*.

Dirichlet's theorem on arithmetic progressions

In number theory, **Dirichlet's theorem**, also called the Dirichlet prime number theorem, states that for any two positive coprime integers a and d, there are infinitely many primes of the form $a + nd$, where $n \geq 0$. In other words, there are infinitely many primes which are congruent to a modulo d. The numbers of the form $a + nd$ form an arithmetic progression

$$a,\ a+d,\ a+2d,\ a+3d,\ \ldots,$$

and Dirichlet's theorem states that this sequence contains infinitely many prime numbers. The theorem extends Euclid's theorem that there are infinitely many prime numbers. Stronger forms of Dirichlet's theorem state that, for any arithmetic progression, the sum of the reciprocals of the prime numbers in the progression diverges, and that different arithmetic progressions with the same modulus have approximately the same proportions of primes.

Note that Dirichlet's theorem does **not** require the prime numbers in an arithmetic sequence to be consecutive. It is also known that there exist arbitrarily long finite arithmetic progressions consisting only of primes, but this is a different result, known as the Green–Tao theorem.

Examples

An integer is a prime for the Gaussian integers if it is a prime number (in the normal sense) that is congruent to 3 modulo 4. The primes of the type $4n + 3$ are

3, 7, 11, 19, 23, 31, 43, 47, 59, 67, ….

They correspond to the following values of n:

0, 1, 2, 4, 5, 7, 10, 11, 14, 16, 17, 19, 20, 25, 26, 31, 32, 34, 37, 40, 41, 44, 47, 49, 52, 55, 56, 59, 62, 65, 67, 70, 76, 77, 82, 86, 89, 91, 94, 95, ….

The strong form of Dirichlet's theorem implies that

$$\frac{1}{3}+\frac{1}{7}+\frac{1}{11}+\frac{1}{19}+\frac{1}{23}+\frac{1}{31}+\frac{1}{43}+\frac{1}{47}+\frac{1}{59}+\frac{1}{67}+\cdots$$

is a divergent series.

The following table lists several arithmetic progressions and the first few prime numbers in each of them.

Arithmetic progression	First 10 of infinitely many primes	OEIS id
$2n + 1$	3, 5, 7, 11, 13, 17, 19, 23, 29, 31, …	A065091 [1]
$4n + 1$	5, 13, 17, 29, 37, 41, 53, 61, 73, 89, …	A002144 [2]
$4n + 3$	3, 7, 11, 19, 23, 31, 43, 47, 59, 67, …	A002145 [3]
$6n + 1$	7, 13, 19, 31, 37, 43, 61, 67, 73, 79, …	A002476 [4]
$6n + 5$	5, 11, 17, 23, 29, 41, 47, 53, 59, 71, …	A007528 [5]
$8n + 1$	17, 41, 73, 89, 97, 113, 137, 193, 233, 241, …	A007519 [6]
$8n + 3$	3, 11, 19, 43, 59, 67, 83, 107, 131, 139, …	A007520 [7]
$8n + 5$	5, 13, 29, 37, 53, 61, 101, 109, 149, 157, …	A007521 [8]
$8n + 7$	7, 23, 31, 47, 71, 79, 103, 127, 151, 167, …	A007522 [9]
$10n + 1$	11, 31, 41, 61, 71, 101, 131, 151, 181, 191, …	A030430 [10]
$10n + 3$	3, 13, 23, 43, 53, 73, 83, 103, 113, 163, …	A030431 [11]
$10n + 7$	7, 17, 37, 47, 67, 97, 107, 127, 137, 157, …	A030432 [12]
$10n + 9$	19, 29, 59, 79, 89, 109, 139, 149, 179, 199, …	A030433 [13]

Distribution

Since the primes thin out, on average, in accordance with the prime number theorem, the same must be true for the primes in arithmetic progressions. One naturally then asks about the way the primes are shared between the various arithmetic progressions for a given value of d (there are d of those, essentially, if we don't distinguish two progressions sharing almost all their terms). The answer is given in this form: the number of feasible progressions *modulo* d — those where a and d do not have a common factor > 1 — is given by Euler's totient function

$$\varphi(d).$$

Further, the proportion of primes in each of those is

$$\frac{1}{\varphi(d)}.$$

For example if d is a prime number q, each of the $q - 1$ progressions, other than

$$q, 2q, 3q, \ldots$$

contains a proportion $1/(q - 1)$ of the primes.

History

Euler stated that every arithmetic progression beginning with 1 contains an infinite number of primes. The theorem in the above form was first conjectured by Legendre in his attempted unsuccessful proofs of quadratic reciprocity and proved by Dirichlet in (Dirichlet 1837) with Dirichlet L-series. The proof is modeled on Euler's earlier work relating the Riemann zeta function to the distribution of primes. The theorem represents the beginning of rigorous analytic number theory.

In algebraic number theory, Dirichlet's theorem generalizes to Chebotarev's density theorem.

Atle Selberg (1949) gave an elementary proof.

References

- Apostol, Tom M. (1976), *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, New York-Heidelberg: Springer-Verlag, MR0434929, ISBN 978-0-387-90163-3
- Weisstein, Eric W., "Dirichlet's Theorem [14]" from MathWorld.
- Chris Caldwell, "Dirichlet's Theorem on Primes in Arithmetic Progressions" [15] at the Prime Pages.
- Dirichlet, P. G. L. (1837), "Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält", *Abhand. Ak. Wiss. Berlin* **48**
- Selberg, Atle (1949), "An elementary proof of Dirichlet's theorem about primes in an arithmetic progression" [16], *Annals of Mathematics* **50** (2): 297–304, doi:10.2307/1969454.

External links

- Scans of the original paper in German [17]
- Dirichlet: *There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime* [18] English translation of the original paper at the arXiv
- Dirichlet's Theorem [19] by Jay Warendorff, Wolfram Demonstrations Project.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa065091
[2] http://en.wikipedia.org/wiki/Oeis%3Aa002144
[3] http://en.wikipedia.org/wiki/Oeis%3Aa002145
[4] http://en.wikipedia.org/wiki/Oeis%3Aa002476
[5] http://en.wikipedia.org/wiki/Oeis%3Aa007528
[6] http://en.wikipedia.org/wiki/Oeis%3Aa007519
[7] http://en.wikipedia.org/wiki/Oeis%3Aa007520
[8] http://en.wikipedia.org/wiki/Oeis%3Aa007521
[9] http://en.wikipedia.org/wiki/Oeis%3Aa007522
[10] http://en.wikipedia.org/wiki/Oeis%3Aa030430
[11] http://en.wikipedia.org/wiki/Oeis%3Aa030431
[12] http://en.wikipedia.org/wiki/Oeis%3Aa030432
[13] http://en.wikipedia.org/wiki/Oeis%3Aa030433
[14] http://mathworld.wolfram.com/DirichletsTheorem.html
[15] http://primes.utm.edu/notes/Dirichlet.html
[16] http://jstor.org/stable/1969454
[17] http://bibliothek.bbaw.de/bibliothek-digital/digitalequellen/schriften/anzeige?band=07-abh/1837&seite:int=00000286
[18] http://arxiv.org/abs/0808.1408
[19] http://demonstrations.wolfram.com/DirichletsTheorem/

Double factorial

n	$n!$
0	1
1	1
2	2
3	6
4	24
5	120
6	720
7	5040
8	40320
9	362880
10	3628800
15	1307674368000
20	2432902008176640000
25	$1.5511210043 \times 10^{25}$
50	$3.0414093202 \times 10^{64}$
70	$1.1978571670 \times 10^{100}$
100	$9.3326215444 \times 10^{157}$
171	$1.2410180702 \times 10^{309}$
450	$1.7333687331 \times 10^{1000}$
1000	$4.0238726008 \times 10^{2567}$
3249	$6.4123376883 \times 10^{10000}$
10000	$2.8462596809 \times 10^{35659}$
25206	$1.2057034382 \times 10^{100000}$
100000	$2.8242294080 \times 10^{456573}$
205023	$2.5038989317 \times 10^{1000004}$
1000000	$8.2639316883 \times 10^{5565708}$
$1.0248383838 \times 10^{98}$	$10^{1.0000000000 \times 10}100$
$1.0000000000 \times 10^{100}$	$10^{9.9565705518 \times 10}101$
$1.7976931349 \times 10^{308}$	$10^{5.5336665775 \times 10}310$

The first few and selected larger members of the sequence of factorials (sequence A000142 [1] in OEIS). The values specified in scientific notation are rounded to the displayed precision.

In mathematics, the **factorial** of a positive integer n,[2] denoted by $n!$, is the product of all positive integers less than or equal to n. For example,

$$5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$$

0! is a special case that is explicitly defined to be 1.[2]

The factorial operation is encountered in many different areas of mathematics, notably in combinatorics, algebra and mathematical analysis. Its most basic occurrence is the fact that there are $n!$ ways to arrange n distinct objects into a sequence (i.e., permutations of the set of objects). This fact was known at least as early as the 12th century, to Hindu scholars.[3] The notation $n!$ was introduced by Christian Kramp in 1808.[4]

The definition of the factorial function can also be extended to non-integer arguments, while retaining its most important properties; this involves more advanced mathematics, notably techniques from mathematical analysis.

Definition

The factorial function is formally defined by

$$n! = \prod_{k=1}^{n} k$$

or recursively defined by

$$n! = \begin{cases} 1 & \text{if } n = 0, \\ (n-1)! \times n & \text{if } n > 0. \end{cases}$$

Both of the above definitions incorporate the instance

$$0! = 1,$$

in the first case by the convention that the product of no numbers at all is 1. This is useful because:

- There is exactly one permutation of zero objects (with nothing to permute, "everything" is left in place).
- The recurrence relation $(n + 1)! = n! \times (n + 1)$, valid for $n > 0$, extends to $n = 0$.
- It allows for the expression of many formulas, like the exponential function as a power series:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

- It makes many identities in combinatorics valid for all applicable sizes. The number of ways to choose 0 elements from the empty set is $\binom{0}{0} = \frac{0!}{0!0!} = 1$. More generally, the number of ways to choose (all) n elements among a set of n is $\binom{n}{n} = \frac{n!}{n!0!} = 1$.

The factorial function can also be defined for non-integer values using more advanced mathematics, detailed in the section below. This more generalized definition is used by advanced calculators and mathematical software such as Maple or Mathematica.

Applications

Although the factorial function has its roots in combinatorics, formulas involving factorials occur in many areas of mathematics.

- There are $n!$ different ways of arranging n distinct objects into a sequence, the permutations of those objects.
- Often factorials appear in the denominator of a formula to account for the fact that ordering is to be ignored. A classical example is counting k-combinations (subsets of k elements) from a set with n elements. One can obtain such a combination by choosing a k-permutation: successively selecting and removing an element of the set, k times, for a total of

$$n^{\underline{k}} = n(n-1)(n-2)\cdots(n-k+1)$$

possibilities. This however produces the *k*-combinations in a particular order that one wishes to ignore; since each *k*-combination is obtained in *k*! different ways, the correct number of *k*-combinations is

$$\frac{n^{\underline{k}}}{k!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)(k-2)\cdots 1}.$$

This number is known as the binomial coefficient $\binom{n}{k}$, because it is also the coefficient of X^k in $(1 + X)^n$.

- Factorials occur in algebra for various reasons, such as via the already mentioned coefficients of the binomial formula, or through averaging over permutations for symmetrization of certain operations.
- Factorials also turn up in calculus; for example they occur in the denominators of the terms of Taylor's formula, basically to compensate for the fact that the n^{th} derivative of x^n is $n!$.
- Factorials are also used extensively in probability theory.
- Factorials can be useful to facilitate expression manipulation. For instance the number of *k*-permutations of *n* can be written as

$$n^{\underline{k}} = \frac{n!}{(n-k)!};$$

while this is inefficient as a means to compute that number, it may serve to prove a symmetry property of binomial coefficients:

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{(n-k)!k!} = \frac{n^{\underline{n-k}}}{(n-k)!} = \binom{n}{n-k}.$$

Number theory

Factorials have many applications in number theory. In particular, *n*! is necessarily divisible by all prime numbers up to and including *n*. As a consequence, $n > 5$ is a composite number if and only if

$$(n-1)! \equiv 0 \pmod{n}.$$

A stronger result is Wilson's theorem, which states that

$$(p-1)! \equiv -1 \pmod{p}$$

if and only if *p* is prime.

Adrien-Marie Legendre found that the multiplicity of the prime *p* occurring in the prime factorization of *n*! can be expressed exactly as

$$\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

This fact is based on counting the number of factors *p* of the integers from 1 to *n*. The number of multiples of *p* in the numbers 1 to *n* are given by $\left\lfloor \frac{n}{p} \right\rfloor$; however, this formula counts those numbers with two factors of *p* only once. Hence another $\left\lfloor \frac{n}{p^2} \right\rfloor$ factors of *p* must be counted too. Similarly for three, four, five factors, to infinity. The sum is finite since p^i can only be less than or equal to *n* for finitely many values of *i*, and the floor function results in 0 when applied for $p^i > n$.

The only factorial that is also a prime number is 2, but there are many primes of the form $n! \pm 1$, called factorial primes.

All factorials greater than 0! and 1! are even, as they are all multiples of 2. Also, all factorials greater than 5! are multiples of 10 (and hence have a zero as their final digit), because they are multiples of 5 and 2.

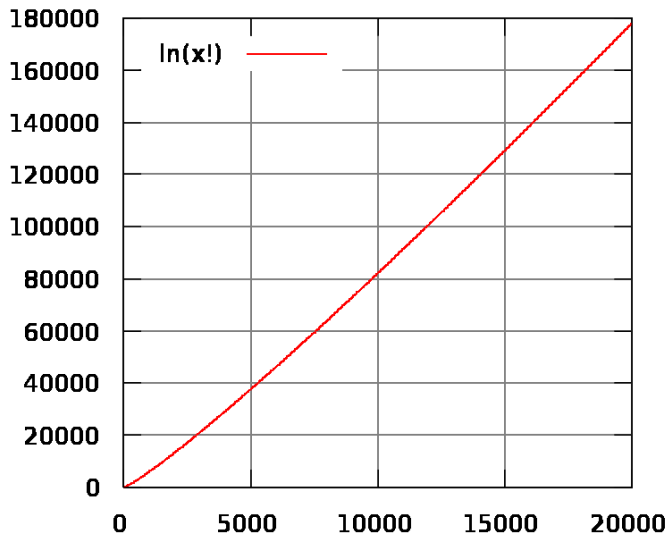
Also note that the reciprocals of factorials produce a convergent series: (see *e*)

$$\sum_{n=0}^{\infty} \frac{1}{n!} = \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120} + \ldots = e.$$

Rate of growth

As n grows, the factorial $n!$ becomes larger than all polynomials and exponential functions (but slower than double exponential functions) in n.

Most approximations for $n!$ are based on approximating its natural logarithm



Plot of the natural logarithm of the factorial

$$\log n! = \sum_{x=1}^{n} \log x.$$

The graph of the function $f(n)$=log $n!$ is shown in the figure on the right. It looks approximately linear for all reasonable values of n, but this intuition is false. We get one of the simplest approximations for log $n!$ by bounding the sum with an integral from above and below as follows:

$$\int_1^n \log x\,dx \leq \sum_{x=1}^{n} \log x \leq \int_0^n \log(x+1)\,dx$$

which gives us the estimate

$$n\log\left(\frac{n}{e}\right)+1 \leq \log n! \leq (n+1)\log\left(\frac{n+1}{e}\right)+1.$$

Hence log $n!$ is $\Theta(n \log n)$. This result plays a key role in the analysis of the computational complexity of sorting algorithms (see comparison sort).

From the bounds on log $n!$ deduced above we get that

$$e\left(\frac{n}{e}\right)^n \leq n! \leq e\left(\frac{n+1}{e}\right)^{n+1}.$$

It is sometimes practical to use weaker but simpler estimates. Using the above formula it is easily shown that for all n we have $(n/3)^n < n!$, and for all $n \geq 6$ we have $n! < (n/2)^n$.

For large n we get a better estimate for the number $n!$ using Stirling's approximation:

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

In fact, it can be proved that for all n we have

$$n! > \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

A much better approximation for log $n!$ was given by Srinivasa Ramanujan (Ramanujan 1988)

$$\log n! \approx n\log n - n + \frac{\log(n(1+4n(1+2n)))}{6} + \frac{\log(\pi)}{2}.$$

Computation

Computing factorials is trivial from an algorithmic point of view: successively multiplying a variable initialized to 1 by the integers 2 up to n (if any) will compute $n!$, provided the result fits in the variable. Interestingly, the factorial is often used as an example to illustrate recursive functions, while it is not intrinsically any more or less recursive (from a mathematical or computational point of view) than for instance a function computing the sum of the first n terms of a given sequence of numbers.

The main difficulty in computing factorials is the size of the result. To assure that the result will fit for all legal values of even the smallest commonly used integral type (8-bit signed integers) would require more than 700 bits, so no reasonable specification of a factorial function using fixed-size types can avoid questions of overflow. The values 12! and 20! are the largest factorials that can be stored in, respectively, the 32 bit and 64 bit integers commonly used in personal computers. Although floating point representation of the result allows going a bit further, it remains quite limited by possible overflow. The largest factorial that most calculators can handle is 69!, because $69! < 10^{100} < 70!$. Calculators that use 3-digit exponents can compute larger factorials, up to, for example, $253! \approx 5.2\times10^{499}$ on HP calculators and $449! \approx 3.9\times10^{997}$ on the TI-86. The calculator seen in Mac OS X, Microsoft Excel and Google Calculator, as well as the freeware Fox Calculator, can handle factorials up to 170!, which is the largest factorial that can be represented as a 64-bit IEEE 754 floating-point value. The scientific calculator in Windows XP is able to calculate factorials up to at least 100000!. Most software applications will compute small factorials by direct multiplication or table lookup. Larger factorial values can be approximated using Stirling's formula.

Wolfram Alpha can calculate exact results for the ceiling function and floor function applied to the binary, natural and common logarithm of $n!$ for values of n up to 249999, and up to 20,000,000! for the Integers.

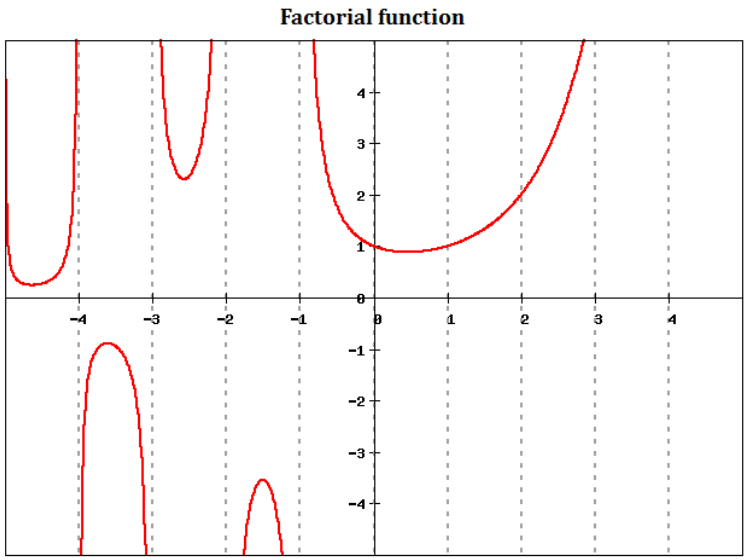
If very large exact factorials are needed, they can be computed using bignum arithmetic. In such computations speed may be gained by not sequentially multiplying the numbers up to (or down from) n into a single accumulator, but by partitioning the sequence so that the products for each of the two parts are approximately of the same size, compute those products recursively and then multiply.

The asymptotically-best efficiency is obtained by computing $n!$ from its prime factorization. As documented by Peter Borwein, prime factorization allows $n!$ to be computed in time $O(n(\log n \log\log n)^2)$, provided that a fast multiplication algorithm is used (for example, the Schönhage–Strassen algorithm).[5] Peter Luschny presents source code and benchmarks for several efficient factorial algorithms, with or without the use of a prime sieve.[6]

Extension of factorial to non-integer values of argument

The Gamma and Pi functions

Besides nonnegative integers, the factorial function can also be defined for non-integer values, but this requires more advanced tools from mathematical analysis. One function that "fills in" the values of the factorial (but with a shift of 1 in the argument) is called the Gamma function, denoted $\Gamma(z)$, defined for all complex numbers z except the non-positive integers, and given when the real part of z is positive by



The factorial function, generalized to all complex numbers except negative integers. For example, 0! = 1! = 1, (−0.5)! = $\sqrt{\pi}$, (0.5)! = $\sqrt{\pi}/2$.

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t}\,\mathrm{d}t.$$

Its relation to the factorials is that for any natural number n

$$n! = \Gamma(n+1).$$

Euler's original formula for the Gamma function was

$$\Gamma(z) = \lim_{n\to\infty} \frac{n^z n!}{\prod_{k=0}^{n}(z+k)}.$$

It is worth mentioning that there is an alternative notation that was originally introduced by Gauss which is sometimes used. The **Pi function**, denoted $\Pi(z)$ for real numbers z no less than 0, is defined by

$$\Pi(z) = \int_0^\infty t^z e^{-t}\,\mathrm{d}t\,.$$

In terms of the Gamma function it is

$$\Pi(z) = \Gamma(z+1)\,.$$

It truly extends the factorial in that

$$\Pi(n) = n! \text{ for } n \in \mathbf{N}\,.$$

In addition to this, the Pi function satisfies the same recurrence as factorials do, but at every complex value z where it is defined

$$\Pi(z) = z\Pi(z-1)\,.$$

In fact, this is no longer a recurrence relation but a functional equation. Expressed in terms of the Gamma function this functional equation takes the form

$$\Gamma(n+1) = n\Gamma(n)\,.$$

Since the factorial is extended by the Pi function, for every complex value z where it is defined, we can write:

$$z! = \Pi(z)$$

The values of these functions at half-integer values is therefore determined by a single one of them; one has

$$\Gamma\left(\frac{1}{2}\right) = \left(-\frac{1}{2}\right)! = \Pi\left(-\frac{1}{2}\right) = \sqrt{\pi},$$

from which it follows that for $n \in \mathbf{N}$,

$$\Gamma\left(\frac{1}{2}+n\right) = \left(-\frac{1}{2}+n\right)! = \Pi\left(-\frac{1}{2}+n\right) = \sqrt{\pi}\prod_{k=1}^{n}\frac{2k-1}{2} = \frac{(2n-1)!}{2^{2n-1}(n-1)!}\sqrt{\pi} = \frac{(2n)!}{4^n n!}\sqrt{\pi}.$$

For example,

$$\Gamma(4.5) = 3.5! = \Pi(3.5) = \frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2}\cdot\frac{7}{2}\sqrt{\pi} = \frac{8!}{4^4 4!}\sqrt{\pi} = \frac{105}{16}\sqrt{\pi} \approx 11.63.$$

It also follows that for $n \in \mathbf{N}$,

$$\Gamma\left(\frac{1}{2}-n\right) = \left(-\frac{1}{2}-n\right)! = \Pi\left(-\frac{1}{2}-n\right) = \sqrt{\pi}\prod_{k=1}^{n}\left(-\frac{2}{2k-1}\right) = \frac{(-4)^n n!}{(2n)!}\sqrt{\pi}.$$

For example,

$$\Gamma(-2.5) = (-3.5)! = \Pi(-3.5) = \left(-\frac{2}{1}\right)\left(-\frac{2}{3}\right)\left(-\frac{2}{5}\right)\sqrt{\pi} = \frac{(-4)^3 3!}{6!}\sqrt{\pi} = -\frac{8}{15}\sqrt{\pi} \approx -0.9453.$$

The Pi function is certainly not the only way to extend factorials to a function defined at almost all complex values, and not even the only one that is analytic wherever it is defined. Nonetheless it is usually considered the most natural way to extend the values of the factorials to a complex function. For instance, the Bohr–Mollerup theorem states that the Gamma function is the only function that takes the value 1 at 1, satisfies the functional equation $\Gamma(n+1) = n\Gamma(n)$, is meromorphic on the complex numbers, and is log-convex on the positive real axis. A similar statement holds for the Pi function as well, using the $\Pi(n) = n\Pi(n-1)$ functional equation.

However, there exist complex functions that are probably simpler in the sense of analytic function theory and which interpolate the factorial values. For example, Hadamard's 'Gamma'-function (Hadamard 1894) which, unlike the Gamma function, is an entire function.[7]

Euler also developed a convergent product approximation for the non-integer factorials, which can be seen to be equivalent to the formula for the Gamma function above:

$$\begin{aligned} n! = \Pi(n) &= \prod_{k=1}^{\infty}\left(\frac{k+1}{k}\right)^n \frac{k}{n+k} \\ &= \left[\left(\frac{2}{1}\right)^n \frac{1}{n+1}\right]\left[\left(\frac{3}{2}\right)^n \frac{2}{n+2}\right]\left[\left(\frac{4}{3}\right)^n \frac{3}{n+3}\right]\cdots. \end{aligned}$$

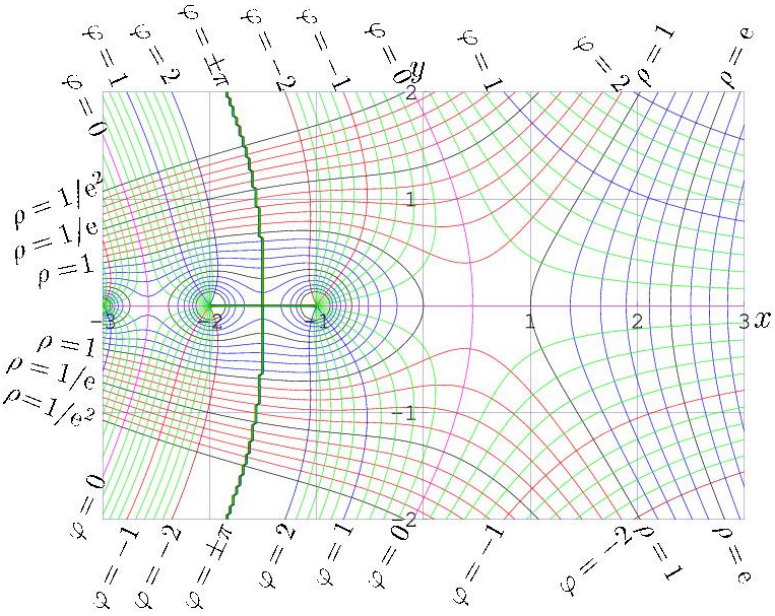
However, this formula does not provide a practical means of computing the Pi or Gamma function, as its rate of convergence is slow.

Applications of the gamma function

The volume of an *n*-dimensional hypersphere of radius *R* is

$$V_n = \frac{\pi^{n/2}}{\Gamma((n/2)+1)} R^n.$$

Factorial at the complex plane



Amplitude and phase of factorial of complex argument.

Representation through the Gamma-function allows evaluation of factorial of complex argument. Equilines of amplitude and phase of factorial are shown in figure. Let $f = \rho \exp(\mathrm{i}\varphi) = (x + \mathrm{i}y)! = \Gamma(x + \mathrm{i}y + 1)$. Several levels of constant modulus (amplitude) $\rho = \mathrm{const}$ and constant phase $\varphi = \mathrm{const}$ are shown. The grid covers range $-3 \le x \le 3,\ -2 \le y \le 2$ with unit step. The scratched line shows the level $\varphi = \pm\pi$. Thin lines show intermediate levels of constant modulus and constant phase. At poles $x + \mathrm{i}y \in (\text{negative integers})$, phase and amplitude are not defined. Equilines are dense in vicinity of singularities along negative integer values of the argument.

For $|z| < 1$, the Taylor expansions can be used:

$$z! = \sum_{n=0}^{\infty} g_n z^n.$$

The first coefficients of this expansion are

n	g_n	approximation
0	1	1
1	$-\gamma$	-0.5772156649
2	$\frac{\pi^2}{12}+\frac{\gamma^2}{2}$	0.9890559955
3	$-\frac{\zeta(3)}{3}-\frac{\pi^2\gamma}{12}-\frac{\gamma^3}{6}$	-0.9074790760

where γ is the Euler constant and ζ is the Riemann zeta function. Computer algebra systems such as Sage (mathematics software) can generate many terms of this expansion.

Approximations of factorial

For the large values of the argument, factorial can be approximated through the integral of the digamma function, using the continued fraction representation. This approach is due to T. J. Stieltjes (1894). Writing $z!$ = exp(P(z)) where P(z) is

$$P(z) = p(z) + \log(2\pi)/2 - z + \left(z + \frac{1}{2}\right)\log(z),$$

Stieltjes gave a continued fraction for p(z)

$$p(z) = \cfrac{a_0}{z + \cfrac{a_1}{z + \cfrac{a_2}{z + \cfrac{a_3}{z + \ddots}}}}$$

The first few coefficients a_n are [8]

n	a_n
0	1 / 12
1	1 / 30
2	53 / 210
3	195 / 371
4	22999 / 22737
5	29944523 / 19773142
6	109535241009 / 48264275462

There is common misconception, that $\log(z!) = P(z)$ or $\log(\Gamma(z+1)) = P(z)$ for any complex $z \neq 0$. Indeed, the relation through the logarithm is valid only for specific range of values of z in vicinity of the real axis, while $|\Im(\Gamma(z+1))| < \pi$. The larger is the real part of the argument, the smaller should be the imaginary part. However, the inverse relation, $z!$ = exp($P(z)$), is valid for the whole complex plane apart from zero. The convergence is poor in vicinity of the negative part of the real axis. (It is difficult to have good convergence of any approximation in vicinity of the singularities). While $|\Im(z)| > 2$ or $\Re(z) > 2$, the 6 coefficients above are sufficient for the evaluation of the factorial with the complex<double> precision. For higher precision more coefficients can be computed by a rational QD-scheme (H. Rutishauser's QD algorithm).[9]

Non-extendability to negative integers

The relation $n\,! = (n-1)! \times n$ allows one to compute the factorial for an integer given the factorial for a *smaller* integer. The relation can be inverted so that one can compute the factorial for an integer given the factorial for a *larger* integer:

$$n! = \frac{(n+1)!}{n+1}.$$

Note, however, that this recursion does not permit us to compute the factorial of a negative integer; use of the formula to compute (−1)! would require a division by zero, and thus blocks us from computing a factorial value for every negative integer. (Similarly, the Gamma function is not defined for non-positive integers, though it is defined for all other complex numbers.)

Factorial-like products and functions

There are several other integer sequences similar to the factorial that are used in mathematics:

Primorial

The primorial (sequence A002110 [10] in OEIS) is similar to the factorial, but with the product taken only over the prime numbers.

Double factorial

A function related to the factorial is the product of all *odd* values up to some odd positive integer *n*. It is often called **double factorial** (even though it only involves about half the factors of the ordinary factorial, and its value is therefore closer to the square root of the factorial), and denoted by *n*!!.

For an odd positive integer $n = 2k - 1$, $k \geq 1$, it is

$$(2k-1)!! = \prod_{i=1}^{k}(2i-1).$$

For example, 9!! = 1 × 3 × 5 × 7 × 9 = 945. This notation creates a notational ambiguity with the composition of the factorial function with itself (which for $n > 2$ gives much larger numbers than the double factorial); this may be justified by the fact that composition arises very seldom in practice, and could be denoted by (*n*!)! to circumvent the ambiguity. The double factorial notation is not essential; it can be expressed in terms of the ordinary factorial by

$$(2k-1)!! = \frac{(2k)!}{k!2^k},$$

since the denominator equals $\prod_{i=1}^{k} 2i$ and cancels the unwanted even factors from the numerator. The introduction of the double factorial is motivated by the fact that it occurs rather frequently in combinatorial and other settings, for instance

- (2*n* − 1)!! is the number of permutations of 2*n* whose cycle type consists of *n* parts equal to 2; these are the involutions without fixed points.
- (2*n* − 1)!! is the number of perfect matchings in a complete graph *K*(2*n*).
- (2*n* − 5)!! is the number of unrooted binary trees with *n* labeled leaves.
- The value $\Gamma\left(n+\frac{1}{2}\right)$ is equal to $\frac{(2n-1)!!}{2^n}\sqrt{\pi}$ (see above)

Sometimes *n*!! is defined for non-negative even numbers as well. One choice is a definition similar to the one for odd values

$$(2k)!! = \prod_{i=1}^{k}(2i) = k!2^k$$

For example, with this definition, 8!! = 2 × 4 × 6 × 8 = 384. However, note that this definition does not match the expression above, of the double factorial in terms of the ordinary factorial, and is also inconsistent with the extension of the definition of $n!!$ to complex numbers n that is achieved via the Gamma function as indicated below. Also, for even numbers, the double factorial notation is hardly shorter than expressing the same value using ordinary factorials. For combinatorial interpretations (the value gives, for instance, the size of the hyperoctahedral group), the latter expression can be more informative (because the factor 2^n is the order of the kernel of a projection to the symmetric group). Even though the formulas for the odd and even double factorials can be easily combined into

$$n!! = \prod_{i;\ 0 \le 2i < n} (n - 2i),$$

the only known interpretation for the sequence of all these numbers (sequence A006882 [11] in OEIS) is somewhat artificial: the number of down-up permutations of a set of *n* + 1 elements for which the entries in the even positions are increasing.

The sequence of double factorials for *n* = 1, 3, 5, 7, ... (sequence A001147 [12] in OEIS) starts as

1, 3, 15, 105, 945, 10395, 135135, ...

Some identities involving double factorials are:

$$(2n+1)!! = \frac{(2n+1)!}{2^n n!} = 2^n n! \binom{n+\frac{1}{2}}{n} = (-2)^{n+1}(n+1)! \binom{-\frac{1}{2}}{n+1}.$$
$$(2n-1)!! = \frac{(2n)!}{2^n n!} = 2^n n! \binom{n-\frac{1}{2}}{n} = (-2)^n n! \binom{-\frac{1}{2}}{n}.$$

Alternative extension of the double factorial

Disregarding the above definition of *n*!! for even values of *n*, the double factorial for odd integers can be extended to most real and complex numbers *z* by noting that when *z* is a positive odd integer then

$$z!! = z(z-2)\cdots(3) = 2^{(z-1)/2}\left(\frac{z}{2}\right)\left(\frac{z-2}{2}\right)\cdots\left(\frac{3}{2}\right) = 2^{(z-1)/2}\frac{\Gamma\left(\frac{z}{2}+1\right)}{\Gamma\left(\frac{1}{2}+1\right)} = \sqrt{\frac{2^{z+1}}{\pi}}\Gamma\left(\frac{z}{2}+1\right).$$

The expressions obtained by taking one of the above formulas for $(2n+1)!!$ and $(2n-1)!!$ and expressing the occurring factorials in terms of the gamma function can both be seen (using the multiplication theorem) to be equivalent to the one given here.

The expression found for *z*!! is defined for all complex numbers except the negative even numbers. Using it as the definition, the volume of an *n*-dimensional hypersphere of radius *R* can be expressed as

$$V_n = \frac{2(2\pi)^{(n-1)/2}}{n!!}R^n.$$

Multifactorials

A common related notation is to use multiple exclamation points to denote a **multifactorial**, the product of integers in steps of two ($n!!$), three ($n!!!$), or more. The double factorial is the most commonly used variant, but one can similarly define the triple factorial ($n!!!$) and so on. One can define the k^{th} factorial, denoted by $n!^{(k)}$, recursively for non-negative integers as

$$n!^{(k)} = \begin{cases} 1, & \text{if } 0 \le n < k, \\ n((n-k)!^{(k)}), & \text{if } n \ge k\,, \end{cases}$$

though see the alternative definition below.

Some mathematicians have suggested an alternative notation of $n!_2$ for the double factorial and similarly $n!_k$ for other multifactorials, but this has not come into general use.

With the above definition, $(kn)!^{(k)} = k^n n!$.

In the same way that $n!$ is not defined for negative integers, and $n!!$ is not defined for negative even integers, $n!^{(k)}$ is not defined for negative integers evenly divisible by k.

Alternative extension of the multifactorial

Alternatively, the multifactorial $z!^{(k)}$ can be extended to most real and complex numbers z by noting that when z is one more than a positive multiple of k then

$$z!^{(k)} = z(z-k)\cdots(k+1) = k^{(z-1)/k}\left(\frac{z}{k}\right)\left(\frac{z-k}{k}\right)\cdots\left(\frac{k+1}{k}\right) = k^{(z-1)/k}\frac{\Gamma\left(\frac{z}{k}+1\right)}{\Gamma\left(\frac{1}{k}+1\right)}.$$

This last expression is defined much more broadly than the original; with this definition, $z!^{(k)}$ is defined for all complex numbers except the negative real numbers evenly divisible by k. This definition is consistent with the earlier definition only for those integers z satisfying $z \equiv 1 \bmod k$.

In addition to extending $z!^{(k)}$ to most complex numbers z, this definition has the feature of working for all positive real values of k. Furthermore, when $k = 1$, this definition is mathematically equivalent to the $\Pi(z)$ function, described above. Also, when $k = 2$, this definition is mathematically equivalent to the alternative extension of the double factorial, described above.

Quadruple factorial

The so-called quadruple factorial, however, is not the multifactorial $n!^{(4)}$; it is a much larger number given by $(2n)!/n!$, starting as

1, 2, 12, 120, 1680, 30240, 665280, ... (sequence A001813 [13] in OEIS).

It is also equal to

$$2^n\frac{(2n)!}{n!2^n} = 2^n\frac{(2\cdot 4\cdots 2n)(1\cdot 3\cdots(2n-1))}{2\cdot 4\cdots 2n}$$
$$= (1\cdot 2)\cdot(3\cdot 2)\cdots((2n-1)\cdot 2) = (4n-2)!^{(4)}.$$

Superfactorial

Neil Sloane and Simon Plouffe defined the **superfactorial** in 1995 as the product of the first n factorials. So the superfactorial of 4 is

$$\mathrm{sf}(4) = 1!\times 2!\times 3!\times 4! = 288.$$

In general

$$\mathrm{sf}(n) = \prod_{k=1}^{n} k! = \prod_{k=1}^{n} k^{n-k+1} = 1^n\cdot 2^{n-1}\cdot 3^{n-2}\cdots(n-1)^2\cdot n^1.$$

Equivalently, the superfactorial is given by the formula

$$\mathrm{sf}(n) = \prod_{0\le i<j\le n}(j-i)$$

which is the determinant of a Vandermonde matrix.

The sequence of superfactorials starts (from $n = 0$) as

1, 1, 2, 12, 288, 34560, 24883200, ... (sequence A000178 [14] in OEIS)

Alternative definition

Clifford Pickover in his 1995 book *Keys to Infinity* used a new notation, *n$*, to define the superfactorial

$$n\$ \equiv \underbrace{n!^{n!^{\cdot^{\cdot^{\cdot^{n!}}}}}}_{n!},$$

or as,

$$n\$ = n!^{(4)} n!$$

where the $^{(4)}$ notation denotes the hyper4 operator, or using Knuth's up-arrow notation,

$$n\$ = (n!) \uparrow\uparrow (n!).$$

This sequence of superfactorials starts:

$$1\$ = 1$$

$$2\$ = 2^2 = 4$$

$$3\$ = 6 \uparrow\uparrow 6 = {}^6 6 = 6^{6^{6^{6^{6^{6}}}}}.$$

Here, as is usual for compound exponentiation, the grouping is understood to be from right to left:

$$a^{b^c} = a^{(b^c)}.$$

Hyperfactorial

Occasionally the **hyperfactorial** of *n* is considered. It is written as *H*(*n*) and defined by

$$H(n) = \prod_{k=1}^{n} k^k = 1^1 \cdot 2^2 \cdot 3^3 \cdots (n-1)^{n-1} \cdot n^n.$$

For *n* = 1, 2, 3, 4, ... the values *H*(*n*) are 1, 4, 108, 27648,... (sequence A002109 [15] in OEIS).

The asymptotic growth rate is

$$H(n) \sim An^{(6n^2+6n+1)/12} e^{-n^2/4}$$

where *A* = 1.2824... is the Glaisher–Kinkelin constant.[16] *H*(14) = 1.8474...×10^{99} is already almost equal to a googol, and *H*(15) = 8.0896...×10^{116} is almost of the same magnitude as the Shannon number, the theoretical number of possible chess games. Compared to the Pickover definition of the superfactorial, the hyperfactorial grows relatively slowly.

The hyperfactorial function can be generalized to complex numbers in a similar way as the factorial function. The resulting function is called the K-function.

Notes

[1] http://en.wikipedia.org/wiki/Oeis%3Aa000142

[2] Weisstein, Eric W., " Factorial (http://mathworld.wolfram.com/Factorial.html)" from MathWorld.

[3] N. L. Biggs, *The roots of combinatorics*, Historia Math. 6 (1979) 109–136

[4] Higgins, Peter (2008), *Number Story: From Counting to Cryptography*, New York: Copernicus, p. 12, ISBN 978-1-84800-000-1 says Krempe though.

[5] Peter Borwein. "On the Complexity of Calculating Factorials". *Journal of Algorithms* 6, 376–380 (1985)

[6] Peter Luschny, *Fast-Factorial-Functions: The Homepage of Factorial Algorithms* (http://www.luschny.de/math/factorial/FastFactorialFunctions.htm).

[7] Peter Luschny, *Hadamard versus Euler - Who found the better Gamma function?* (http://www.luschny.de/math/factorial/hadamard/HadamardsGammaFunction.html).

[8] Digital Library of Mathematical Functions, http://dlmf.nist.gov/5.10

[9] Peter Luschny, *On Stieltjes' Continued Fraction for the Gamma Function.* (http://www.luschny.de/math/factorial/approx/continuedfraction.html).

[10] http://en.wikipedia.org/wiki/Oeis%3Aa002110

[11] http://en.wikipedia.org/wiki/Oeis%3Aa006882

[12] http://en.wikipedia.org/wiki/Oeis%3Aa001147
[13] http://en.wikipedia.org/wiki/Oeis%3Aa001813
[14] http://en.wikipedia.org/wiki/Oeis%3Aa000178
[15] http://en.wikipedia.org/wiki/Oeis%3Aa002109
[16] Weisstein, Eric W., " Glaisher–Kinkelin Constant (http://mathworld.wolfram.com/Glaisher-KinkelinConstant.html)" from MathWorld.

References

- Hadamard, M. J. (1894) (in French), *Sur L'Expression Du Produit 1·2·3· · · · ·(n−1) Par Une Fonction Entière* (http://www.luschny.de/math/factorial/hadamard/HadamardFactorial.pdf), *OEuvres de Jacques Hadamard*, Centre National de la Recherche Scientifiques, Paris, 1968
- Ramanujan, Srinivasa (1988), *The lost notebook and other unpublished papers*, Springer Berlin, p. 339, ISBN 354018726X

External links

- Approximation formulas (http://www.luschny.de/math/factorial/approx/SimpleCases.html)
- All about factorial notation n! (http://factorielle.free.fr/index_en.html)
- Weisstein, Eric W., " Factorial (http://mathworld.wolfram.com/Factorial.html)" from MathWorld.
  - Weisstein, Eric W., " Double factorial (http://mathworld.wolfram.com/DoubleFactorial.html)" from MathWorld.
- *Factorial* (http://planetmath.org/encyclopedia/Factorial.html) at PlanetMath.
- "Double Factorial Derivations" (http://www.docstoc.com/docs/5606124/Double-Factorials-Selected-Proofs-and-Notes)

Factorial calculators and algorithms

- Factorial Calculator (http://web.ics.purdue.edu/~chen165/Math.htm): instantly finds factorials up to 10^14!
- Animated Factorial Calculator (http://www.gfredericks.com/main/sandbox/arith/factorial): shows factorials calculated as if by hand using common elementary school aglorithms
- "Factorial" (http://demonstrations.wolfram.com/Factorial/) by Ed Pegg, Jr. and Rob Morris, Wolfram Demonstrations Project, 2007.
- Fast Factorial Functions (with source code in Java, C#, C++, Scala and Go) (http://www.luschny.de/math/factorial/FastFactorialFunctions.htm)

Double Mersenne prime

In mathematics, a **double Mersenne number** is a Mersenne number of the form

$$M_{M_p} = 2^{2^p-1} - 1$$

where *p* is a Mersenne prime exponent.

The smallest double Mersenne numbers

The sequence of double Mersenne numbers begins [1]

$$M_{M_2} = M_3 = 7$$
$$M_{M_3} = M_7 = 127$$
$$M_{M_5} = M_{31} = 2147483647$$
$$M_{M_7} = M_{127} = 170141183460469231731687303715884105727$$ (sequence A077586 [2] in OEIS).

Double Mersenne primes

A double Mersenne number that is prime is called a **double Mersenne prime**. Since a Mersenne number M_p can be prime only if *p* is prime, (see Mersenne prime for a proof), a double Mersenne number M_{M_p} can be prime only if M_p is itself a Mersenne prime. The first values of *p* for which M_p is prime are *p* = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89. Of these, M_{M_p} is known to be prime for *p* = 2, 3, 5, 7; for *p* = 13, 17, 19, and 31, explicit factors have been found showing that the corresponding double Mersenne numbers are not prime. Thus, the smallest candidate for the next double Mersenne prime is $M_{M_{61}}$, or $2^{2305843009213693951} - 1$. Being approximately $1.695\times10^{694127911065419641}$, this number is far too large for any currently known primality test. It has no prime factor below 4×10^{33}.[3]

Catalan-Mersenne number

Write $M(p)$ instead of M_p. A special case of the double Mersenne numbers, namely the recursively defined sequence

2, M(2), M(M(2)), M(M(M(2))), M(M(M(M(2)))), ... (sequence A007013 [4] in OEIS)

is called the **Catalan-Mersenne numbers**.[5] It is said[1] that Catalan came up with this sequence after the discovery of the primality of $M(127) = M(M(M(M(2))))$ by Lucas in 1876.

Although the first five terms (up to $M(127)$) are prime, no known methods can decide if any more of these numbers are prime (in any reasonable time) simply because the numbers in question are too huge, unless a factor of M(M(127)) is discovered.

In popular culture

In the Futurama movie *The Beast with a Billion Backs*, the double Mersenne number M_{M_7} is briefly seen in "an elementary proof of the Goldbach conjecture". In the movie, this number is known as a "martian prime".

References

[1] Chris Caldwell, *Mersenne Primes: History, Theorems and Lists* (http://primes.utm.edu/mersenne/index.html#unknown) at the Prime Pages.

[2] http://en.wikipedia.org/wiki/Oeis%3Aa077586

[3] Tony Forbes, A search for a factor of MM61. Progress: 9 October 2008 (http://anthony.d.forbes.googlepages.com/mm61prog.htm). This reports a high-water mark of 204204000000×(10019+1)×(2^{61}−1), above 4×10^{33}. Retrieved on 2008-10-22.

[4] http://en.wikipedia.org/wiki/Oeis%3Aa007013

[5] Weisstein, Eric W., " Catalan-Mersenne Number (http://mathworld.wolfram.com/Catalan-MersenneNumber.html)" from MathWorld.

Further reading

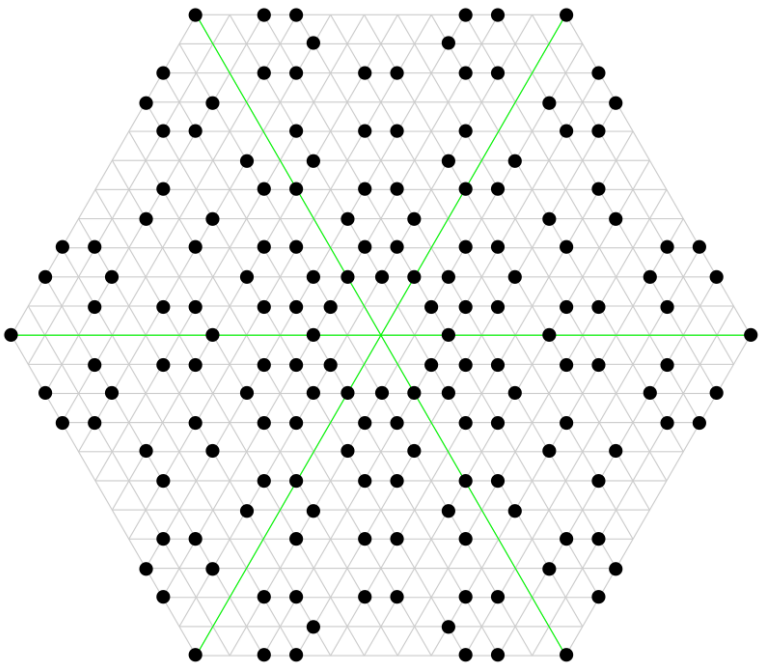
- Dickson, L. E. (1971) [1919], *History of the theory of numbers*, New York: Chelsea Publishing.

External links

- Weisstein, Eric W., " Double Mersenne Number (http://mathworld.wolfram.com/DoubleMersenneNumber.html)" from MathWorld.
- Tony Forbes, A search for a factor of MM61 (http://anthony.d.forbes.googlepages.com/mm61.htm).

Eisenstein prime

In mathematics, an **Eisenstein prime** is an Eisenstein integer



Small Eisenstein primes. Those on the green axes are associate to a natural prime of the form 3*n*−1. All others have an absolute value squared equal to a natural prime.

$$z = a + b\,\omega \qquad (\omega = e^{2\pi i/3})$$

that is irreducible (or equivalently prime) in the ring-theoretic sense: its only Eisenstein divisors are the units (±1, ±ω, $\pm\omega^2$), $a + b\omega$ itself and its associates.

The associates (unit multiples) and the complex conjugate of any Eisenstein prime are also prime.

An Eisenstein integer $z = a + b\omega$ is an Eisenstein prime if and only if either of the following (mutually exclusive) conditions hold:

1. z is equal to the product of a unit and a natural prime of the form $3n - 1$,
2. $|z|^2 = a^2 - ab + b^2$ is a natural prime (necessarily congruent to 0 or 1 modulo 3).

It follows that the absolute value squared of every Eisenstein prime is a natural prime or the square of a natural prime.

The first few Eisenstein primes that equal a natural prime $3n - 1$ are:

2, 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101 (sequence A003627 [1] in OEIS)

Natural primes that are congruent to 0 or 1 modulo 3 are *not* Eisenstein primes: they admit nontrivial factorizations in $\mathbf{Z}[\omega]$. For example:

$3 = -(1+2\omega)^2$

$7 = (3+\omega)(2-\omega)$.

Some non-real Eisenstein primes are

$2 + \omega$, $3 + \omega$, $4 + \omega$, $5 + 2\omega$, $6 + \omega$, $7 + \omega$, $7 + 3\omega$

Up to conjugacy and unit multiples, the primes listed above, together with 2 and 5, are all the Eisenstein primes of absolute value not exceeding 7.

As of March 2010, the largest known (real) Eisenstein prime is $19249 \times 2^{13018586} + 1$, which is the tenth largest known prime, discovered by Konstantin Agafonov.[2] All larger known primes are Mersenne primes, discovered by GIMPS. Real Eisenstein primes are congruent to 2 mod 3, and Mersenne primes (except the smallest, 3) are congruent to 1 mod 3; thus no Mersenne prime is an Eisenstein prime.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa003627

[2] Chris Caldwell, " The Top Twenty: Largest Known Primes (http://primes.utm.edu/top20/page.php?id=3)" from The Prime Pages. Retrieved 2010-03-12.

Emirp

An **emirp** (*prime* spelled backwards) is a prime number that results in a different prime when its digits are reversed.[1] This definition excludes the related palindromic primes. Emirps are also called ***reversible primes***.

The sequence of emirps begins 13, 17, 31, 37, 71, 73, 79, 97, 107, 113, 149, 157... (sequence A006567 [2] in OEIS).[1]

All non-palindromic permutable primes are emirps.

As of November 2009, the largest known emirp is $10^{10006}+941992101\times10^{4999}+1$, found by Jens Kruse Andersen in October 2007.[3]

References

[1] Weisstein, Eric W., " Emirp (http://mathworld.wolfram.com/Emirp.html)" from MathWorld.
[2] http://en.wikipedia.org/wiki/Oeis%3Aa006567
[3] Rivera, Carlos. " Problems & Puzzles: Puzzle 20.- Reversible Primes (http://www.primepuzzles.net/puzzles/puzz_020.htm)". Retrieved on December 17, 2007.

Euclid number

In mathematics, **Euclid numbers** are integers of the form $E_n = p_n\# + 1$, where $p_n\#$ is the primorial of p_n which is the nth prime. They are named after the ancient Greek mathematician Euclid.

It is sometimes falsely stated that Euclid's celebrated proof of the infinitude of prime numbers relied on these numbers. In fact, Euclid did not begin with the assumption that the set of all primes is finite. Rather, he said: consider any finite set of primes (he did not assume it contained just the first n primes, e.g. it could have been {3, 41, 53}) and reasoned from there to the conclusion that at least one prime exists that is not in that set.[1]

The first few Euclid numbers are 3, 7, 31, 211, 2311, 30031, 510511 (sequence A006862 [2] in OEIS).

It is not known whether or not there are an infinite number of prime Euclid numbers.

$E_6 = 13\# + 1 = 30031 = 59 \text{ x } 509$ is the first composite Euclid number, demonstrating that not all Euclid numbers are prime.

A Euclid number can not be a square. This is because Euclid numbers are always congruent to 3 mod 4.

For all $n \geq 3$ the last digit of E_n is 1, since $E_n - 1$ is divisible by 2 and 5.

References

[1] "Proposition 20" (http://aleph0.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html). .
[2] http://en.wikipedia.org/wiki/Oeis%3Aa006862

See also

- Euclid–Mullin sequence
- Proof of the infinitude of the primes (Euclid's theorem)
- Primorial prime

Even number

In mathematics, the **parity** of an object states whether it is even or odd.

This concept begins with integers. An **even number** is an integer that is "evenly divisible" by 2, i.e., divisible by 2 without remainder; an **odd number** is an integer that is not evenly divisible by 2. (The old-fashioned term "evenly divisible" is now almost always shortened to "divisible".) A formal definition of an odd number is that it is an integer of the form $n = 2k + 1$, where k is an integer. An even number has the form $n = 2k$ where k is an integer.

Examples of even numbers are −4, 8, and 1728. Examples of odd numbers are −5, 9, 3, and 71. This classification only applies to integers, i.e., a fractional number like 1/2 or 4.201 is neither even nor odd.

The sets of even and odd numbers can be defined as following:

- **Even** = $\{2k; \forall k \in \mathbb{Z}\}$
- **Odd** = $\{2k + 1; \forall k \in \mathbb{Z}\}$

A number (i.e., integer) expressed in the decimal numeral system is even or odd according to whether its last digit is even or odd. That is, if the last digit is 1, 3, 5, 7, or 9, then it's odd; otherwise it's even. The same idea will work using any even base. In particular, a number expressed in the binary numeral system is odd if its last digit is 1 and even if its last digit is 0. In an odd base, the number is even according to the sum of its digits – it is even if and only if the sum of its digits is even.

Arithmetic on even and odd numbers

The following laws can be verified using the properties of divisibility. They are a special case of rules in modular arithmetic, and are commonly used to check if an equality is likely to be correct by testing the parity of each side. As with ordinary arithmetic, multiplication and addition are commutative and associative, and multiplication is distibutive over addition. However, subtraction in parity is identical to addition, so subtraction also possesses these properties (which are absent from ordinary arithmetic).

Addition and subtraction

- even ± even = even;
- even ± odd = odd;
- odd ± odd = even;

Rules analogous to these for divisibility by 9 are used in the method of casting out nines.

Division

The division of two whole numbers does not necessarily result in a whole number. For example, 1 divided by 4 equals 1/4, which isn't even *or* odd, since the concepts even and odd apply only to integers. But when the quotient is an integer, it will be even if and only if the dividend has more factors of two than the divisor.

History

The ancient Greeks considered 1 to be neither fully odd nor fully even. Some of this sentiment survived into the 19th century: Friedrich Wilhelm August Fröbel's 1826 *The Education of Man* instructs the teacher to drill students with the claim that 1 is neither even nor odd, to which Fröbel attaches the philosophical afterthought,

> It is well to direct the pupil's attention here at once to a great far-reaching law of nature and of thought. It is this, that between two relatively different things or ideas there stands always a third, in a sort of balance, seeming to unite the two. Thus, there is here between odd and even numbers one number (one) which is neither of the two. Similarly, in form, the right angle stands between the acute and obtuse angles; and in language, the semi-vowels or aspirants between the mutes and vowels. A thoughtful teacher and a pupil taught to think for himself can scarcely help noticing this and other important laws.

Music theory

In wind instruments which are cylindrical and in effect closed at one end, such as the clarinet at the mouthpiece, the harmonics produced are odd multiples of the fundamental frequency. (With cylindrical pipes open at both ends, used for example in some organ stops such as the open diapason, the harmonics are even multiples of the same frequency, but this is the same as being all multiples of double the frequency and is usually perceived as such.) See harmonic series (music).

Higher mathematics

The even numbers form an ideal in the ring of integers, but the odd numbers do not — this is clear from the fact that the identity element for addition, zero, is an element of the even numbers only. An integer is even if it is congruent to 0 modulo this ideal, in other words if it is congruent to 0 modulo 2, and odd if it is congruent to 1 modulo 2.

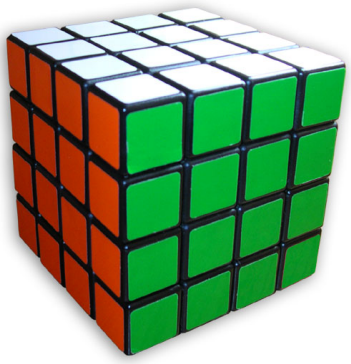
All prime numbers are odd, with one exception: the prime number 2. All known perfect numbers are even; it is unknown whether any odd perfect numbers exist.

The squares of all even numbers are even, and the squares of all odd numbers are odd. Since an even number can be expressed as 2x, $(2x)^2 = 4x^2$ which is even. Since an odd number can be expressed as 2x + 1, $(2x + 1)^2 = 4x^2 + 4x + 1$. $4x^2$ and 4x are even, which means that $4x^2 + 4x + 1$ is odd (since even + odd = odd).

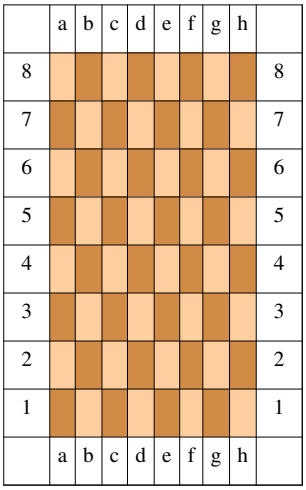
Goldbach's conjecture states that every even integer greater than 2 can be represented as a sum of two prime numbers. Modern computer calculations have shown this conjecture to be true for integers up to at least 4×10^{14}, but still no general proof has been found.

The Feit–Thompson theorem states that a finite group is always solvable if its order is an odd number. This is an example of odd numbers playing a role in an advanced mathematical theorem where the method of application of the simple hypothesis of "odd order" is far from obvious.

Parity for other objects



Rubik's Revenge in solved state



The two light bishops are confined to squares of opposite parity; the dark knight can only jump to squares of alternating parity.

Parity is also used to refer to a number of other properties.

- The parity of a permutation (as defined in abstract algebra) is the parity of the number of transpositions into which the permutation can be decomposed. For example (ABC) to (BCA) is even because it can be done by swapping A and B then C and A (two transpositions). It can be shown that no permutation can be decomposed both in an even and in an odd number of transpositions. Hence the above is a suitable definition. In Rubik's Revenge, Square-1, and other twisty puzzles, the moves of the puzzle allow only even permutations of the puzzle pieces, so parity is important in understanding the configuration space of these puzzles.
- The parity of a function describes how its values change when its arguments are exchanged with their negations. An even function, such as an even power of a variable, gives the same result for any argument as for its negation. An odd function, such as an odd power of a variable, gives for any argument the negation of its result when given the negation of that argument. It is possible for a function to be neither odd nor even, and for the case $f(x) = 0$, to be both odd and even.
- Integer coordinates of points in Euclidean spaces of two or more dimensions also have a parity, usually defined as the parity of the sum of the coordinates. For instance, the checkerboard lattice contains all integer points of even parity. This feature manifests itself in chess, as bishops are constrained to squares of the same parity; knights alternate parity between moves. This form of parity was famously used to solve the Mutilated chessboard problem.

Factorial prime

A **factorial prime** is a prime number that is one less or one more than a factorial (all factorials above 1 are even). The first few factorial primes are:

2 (0! + 1 or 1! + 1), 3 (2! + 1), 5 (3! − 1), 7 (3! + 1), 23 (4! − 1), 719 (6! − 1), 5039 (7! − 1), 39916801 (11! + 1), 479001599 (12! − 1), 87178291199 (14! − 1), ... (sequence A088054 [1] in OEIS)

$n! - 1$ is prime for (sequence A002982 [2] in OEIS):

n = 3, 4, 6, 7, 12, 14, 30, 32, 33, 38, 94, 166, 324, 379, 469, 546, 974, 1963, 3507, 3610, 6917, 21480, 34790, ... , 94550, 103040

$n! + 1$ is prime for (sequence A002981 [3] in OEIS):

n = 0, 1, 2, 3, 11, 27, 37, 41, 73, 77, 116, 154, 320, 340, 399, 427, 872, 1477, 6380, 26951, ...

No other factorial primes are known as of 2010.

Absence of primes to both sides of a factorial $n!$ implies a relatively lengthy run of consecutive composite numbers, since $n! \pm k$ is divisible by k for $2 \leq k \leq n$. For example, the next prime following 6227020777 = 13! − 23 is 6227020867 = 13! + 67 (a run of 89 consecutive composites); here the run is substantially longer than implied merely by the absence of factorial primes. Note that this is not the most efficient way to find large prime gaps. E.g., there are 95 consecutive composites between the primes 360653 and 360749.

External links

- Weisstein, Eric W., "Factorial Prime [4]" from MathWorld.
- List of largest known factorial primes [5] from the Prime Pages

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa088054
[2] http://en.wikipedia.org/wiki/Oeis%3Aa002982
[3] http://en.wikipedia.org/wiki/Oeis%3Aa002981
[4] http://mathworld.wolfram.com/FactorialPrime.html
[5] http://primes.utm.edu/top20/page.php?id=30

Fermat number

In mathematics, a **Fermat number**, named after Pierre de Fermat who first studied them, is a positive integer of the form

$$F_n = 2^{2^n} + 1$$

where n is a nonnegative integer. The first few Fermat numbers are:

3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, … (sequence A000215 [1] in OEIS).

If $2^n + 1$ is prime, and $n > 0$, it can be shown that n must be a power of two. (If $n = ab$ where $1 \le a, b \le n$ and b is odd, then $2^n + 1 = (2^a)^b + 1 \equiv (-1)^b + 1 = 0$ (**mod** $2^a + 1$). See below for complete proof.) In other words, every prime of the form $2^n + 1$ is a Fermat number, and such primes are called **Fermat primes**. The only known Fermat primes are F_0, F_1, F_2, F_3, and F_4.

Basic properties

The Fermat numbers satisfy the following recurrence relations

$$F_n = (F_{n-1} - 1)^2 + 1$$
$$F_n = F_{n-1} + 2^{2^{n-1}} F_0 \cdots F_{n-2}$$
$$F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$$
$$F_n = F_0 \cdots F_{n-1} + 2$$

for $n \ge 2$. Each of these relations can be proved by mathematical induction. From the last equation, we can deduce **Goldbach's theorem**: no two Fermat numbers share a common factor. To see this, suppose that $0 \le i < j$ and F_i and F_j have a common factor $a > 1$. Then a divides both

$$F_0 \cdots F_{j-1}$$

and F_j; hence a divides their difference, 2. Since $a > 1$, this forces $a = 2$. This is a contradiction, because each Fermat number is clearly odd. As a corollary, we obtain another proof of the infinitude of the prime numbers: for each F_n, choose a prime factor p_n; then the sequence $\{p_n\}$ is an infinite sequence of distinct primes.

Further properties:

- The number of digits $D(n,b)$ of F_n expressed in the base b is

  $$D(n, b) = \lfloor \log_b \left(2^{2^n} + 1\right) + 1 \rfloor \approx \lfloor 2^n \log_b 2 + 1 \rfloor$$ (See floor function).
- No Fermat number can be expressed as the sum of two primes, with the exception of $F_1 = 2 + 3$.
- No Fermat prime can be expressed as the difference of two pth powers, where p is an odd prime.
- With the exception of 3 and 5, the last digit of a Fermat number is 7.
- The sum of the reciprocals of all the Fermat numbers (sequence A051158 [2] in OEIS) is irrational. (Solomon W. Golomb, 1963)

Primality of Fermat numbers

Fermat numbers and Fermat primes were first studied by Pierre de Fermat, who conjectured (but admitted he could not prove) that all Fermat numbers are prime. Indeed, the first five Fermat numbers F_0,...,F_4 are easily shown to be prime. However, this conjecture was refuted by Leonhard Euler in 1732 when he showed that

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417.$$

Euler proved that every factor of F_n must have the form $k2^{n+1} + 1$.

It is widely believed that Fermat was aware of the form of the factors later proved by Euler, so it seems curious why he failed to follow through on the straightforward calculation to find the factor.[3] One common explanation is that Fermat made a computational mistake and was so convinced of the correctness of his claim that he failed to double-check his work.

There are no other known Fermat primes F_n with $n > 4$. However, little is known about Fermat numbers with large n.[4] In fact, each of the following is an open problem:

- Is F_n composite for all $n > 4$?
- Are there infinitely many Fermat primes? (Eisenstein 1844)[5]
- Are there infinitely many composite Fermat numbers?

The following heuristic argument suggests there are only finitely many Fermat primes: according to the prime number theorem, the "probability" that a number n is prime is at most $A/\ln(n)$, where A is a fixed constant. Therefore, the total expected number of Fermat primes is at most

$$A\sum_{n=0}^{\infty}\frac{1}{\ln F_n} = \frac{A}{\ln 2}\sum_{n=0}^{\infty}\frac{1}{\log_2(2^{2^n}+1)} < \frac{A}{\ln 2}\sum_{n=0}^{\infty}2^{-n} = \frac{2A}{\ln 2}.$$

It should be stressed that this argument is in no way a rigorous proof. For one thing, the argument assumes that Fermat numbers behave "randomly", yet we have already seen that the factors of Fermat numbers have special properties. If (more sophisticatedly) we regard the *conditional* probability that n is prime, given that we know all its prime factors exceed B, as at most $A\ln(B)/\ln(n)$, then using Euler's theorem that the least prime factor of F_n exceeds 2^{n+1}, we would find instead

$$A\sum_{n=0}^{\infty}\frac{\ln 2^{n+1}}{\ln F_n} = A\sum_{n=0}^{\infty}\frac{\log_2 2^{n+1}}{\log_2(2^{2^n}+1)} < A\sum_{n=0}^{\infty}(n+1)2^{-n} = 4A.$$

Although such arguments engender the belief that there are only finitely many Fermat primes, one can also produce arguments for the opposite conclusion. Suppose we regard the conditional probability that n is prime, given that we know all its prime factors are 1 modulo M, as at least $CM/\ln(n)$. Then using Euler's result that $M=2^{n+1}$ we would find that the expected total number of Fermat primes was at least

$$C\sum_{n=0}^{\infty}\frac{2^{n+1}}{\ln F_n} = \frac{C}{\ln 2}\sum_{n=0}^{\infty}\frac{2^{n+1}}{\log_2(2^{2^n}+1)} > \frac{C}{\ln 2}\sum_{n=0}^{\infty}1 = \infty,$$

and indeed this argument predicts that an asymptotically *constant fraction* of Fermat numbers are prime!

As of 2010 it is known that F_n is composite for $5 \le n \le 32$, although complete factorizations of F_n are known only for $0 \le n \le 11$, and there are no known factors for n in {20, 24}.[6] The largest Fermat number known to be composite is $F_{2478782}$, and its prime factor $3\times2^{2478785} + 1$ was discovered by John B. Cosgrave and his Proth-Gallot Group on October 10, 2003.

There are a number of conditions that are equivalent to the primality of F_n.

- **Proth's theorem** -- (1878) Let $N = k2^m + 1$ with odd $k < 2^m$. If there is an integer a such that

$$a^{(N-1)/2} \equiv -1 \mod N$$

then N is prime. Conversely, if the above congruence does not hold, and in addition

$$\left(\frac{a}{N}\right) = -1$$ (See Jacobi symbol)

then N is composite. If $N = F_n > 3$, then the above Jacobi symbol is always equal to -1 for $a = 3$, and this special case of Proth's theorem is known as Pépin's test. Although Pépin's test and Proth's theorem have been implemented on computers to prove the compositeness of many Fermat numbers, neither test gives a specific nontrivial factor. In fact, no specific prime factors are known for $n = 20$ and 24.

- Let $n \geq 3$ be a positive odd integer. Then n is a Fermat prime if and only if for every a co-prime to n, a is a primitive root **mod** n if and only if a is a quadratic nonresidue **mod** n.
- The Fermat number $F_n > 3$ is prime if and only if it can be written uniquely as a sum of two nonzero squares, namely

$$F_n = \left(2^{2^n-1}\right)^2 + 1^2.$$

When $F_n = x^2 + y^2$ not of the form shown above, a proper factor is:

$$\gcd(x + 2^{2^n-1}y, F_n).$$

Example 1: $F_5 = 62264^2 + 20449^2$, so a proper factor is

$$\gcd(62264 + 2^{2^4}\,20449,\, F_5) = 641.$$

Example 2: $F_6 = 4046803256^2 + 1438793759^2$, so a proper factor is

$$\gcd(4046803256 + 2^{2^5}\,1438793759,\, F_6) = 274177.$$

Factorization of Fermat numbers

Because of the size of Fermat numbers, it is difficult to factorize or to prove primality of those. Pépin's test gives a necessary and sufficient condition for primality of Fermat numbers, and can be implemented by modern computers. The elliptic curve method is a fast method for finding small prime divisors of numbers. Distributed computing project *Fermatsearch* has successfully found some factors of Fermat numbers. Yves Gallot's proth.exe has been used to find factors of large Fermat numbers. Edouard Lucas, improving the above mentioned result by Euler, proved in 1878 that every factor of Fermat number F_n, with n at least 2, is of the form $k \times 2^{n+2} + 1$ (see Proth number), where k is a positive integer; this is in itself almost sufficient to prove the primality of the known Fermat primes.

Factorizations of the first ten Fermat numbers are:

$F_0 = 2^1 + 1 = 3$ is prime

$F_1 = 2^2 + 1 = 5$ is prime

$F_2 = 2^4 + 1 = 17$ is prime

$F_3 = 2^8 + 1 = 257$ is prime

$F_4 = 2^{16} + 1 = 65{,}537$ is the largest known Fermat prime

$F_5 = 2^{32} + 1 = 4{,}294{,}967{,}297$

$= 641 \times 6{,}700{,}417$

$F_6 = 2^{64} + 1 = 18{,}446{,}744{,}073{,}709{,}551{,}617$

$= 274{,}177 \times 67{,}280{,}421{,}310{,}721$

$F_7 = 2^{128} + 1 = 340{,}282{,}366{,}920{,}938{,}463{,}463{,}374{,}607{,}431{,}768{,}211{,}457$

$= 59{,}649{,}589{,}127{,}497{,}217 \times 5{,}704{,}689{,}200{,}685{,}129{,}054{,}721$

$F_8 = 2^{256} + 1 = 115{,}792{,}089{,}237{,}316{,}195{,}423{,}570{,}985{,}008{,}687{,}907{,}853{,}269{,}984{,}665{,}640{,}564{,}039{,}457{,}584{,}007{,}913{,}129{,}639{,}937$

$= 1{,}238{,}926{,}361{,}552{,}897 \times 93{,}461{,}639{,}715{,}357{,}977{,}769{,}163{,}558{,}199{,}606{,}896{,}584{,}051{,}237{,}541{,}638{,}188{,}580{,}280{,}321$

$F_9 = 2^{512} + 1 = 13{,}407{,}807{,}929{,}942{,}597{,}099{,}574{,}024{,}998{,}205{,}846{,}127{,}479{,}365{,}820{,}592{,}393{,}377{,}723{,}561{,}443{,}721{,}764{,}030{,}073{,}546{,}976{,}801{,}874{,}298{,}166{,}903{,}427{,}690{,}031{,}858{,}186{,}486{,}050{,}853{,}753{,}882{,}811{,}946{,}569{,}946{,}433{,}649{,}006{,}084{,}097$

$= 2{,}424{,}833 \times 7{,}455{,}602{,}825{,}647{,}884{,}208{,}337{,}395{,}736{,}200{,}454{,}918{,}783{,}366{,}342{,}657 \times$
$741{,}640{,}062{,}627{,}530{,}801{,}524{,}787{,}141{,}901{,}937{,}474{,}059{,}940{,}781{,}097{,}519{,}023{,}905{,}821{,}316{,}144{,}415{,}759{,}504{,}705{,}008{,}092{,}818{,}711{,}693{,}940{,}737$

As of March 2010, only F_0 to F_{11} have been completely factored.[6] The distributed computing project Fermat Search is searching for new factors of Fermat numbers.[7] The set of all Fermat factors is A050922 (or, sorted, A023394) in OEIS.

Pseudoprimes and Fermat numbers

Like composite numbers of the form $2^p - 1$, every composite Fermat number is a strong pseudoprime to base 2. Because *all* strong pseudoprimes to base 2 are also Fermat pseudoprimes - i.e.

$$2^{F_n-1} \equiv 1 \pmod{F_n}$$

for all Fermat numbers.

Because it is generally believed that all but the first few Fermat numbers are composite, this makes it possible to generate infinitely many strong pseudoprimes to base 2 from the Fermat numbers.

In fact, Rotkiewicz showed in 1964 that the product of any number of prime *or* composite Fermat numbers will be a Fermat pseudoprime to base 2.

Other theorems about Fermat numbers

Lemma: If *n* is a positive integer,

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

proof:

$$\begin{aligned}
&(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} \\
&= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} \\
&= a^n + \sum_{k=1}^{n-1} a^k b^{n-k} - \sum_{k=1}^{n-1} a^k b^{n-k} - b^n \\
&= a^n - b^n.
\end{aligned}$$

Theorem: If $2^n + 1$ is an odd prime, then n is a power of 2.

proof:

If n is a positive integer but not a power of 2, then $n = rs$ where $1 \leq r < n$, $1 < s \leq n$ and s is odd.

By the preceding lemma, for positive integer m ,

$$(a-b) \mid (a^m - b^m)$$

where $\mid$ means "evenly divides". Substituting $a = 2^r$, $b = -1$, and $m = s$ and using that s is odd,

$$(2^r + 1) \mid (2^{rs} + 1),$$

and thus

$$(2^r + 1) \mid (2^n + 1).$$

Because $1 < 2^r + 1 < 2^n + 1$, it follows that $2^n + 1$ is not prime. Therefore, by contraposition n must be a power of 2.

Theorem: A Fermat prime cannot be a Wieferich prime.

Proof: We show if $p = 2^m + 1$ is a Fermat prime, then the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ does not satisfy. It is easy to show $2m|p-1$. Now write, $p - 1 = 2m\lambda$. If the given congruence satisfies, then $p^2|2^{2m\lambda} - 1$, therefore

$$0 \equiv (2^{2m\lambda}-1)/(2^m+1) = (2^m-1)(1+2^{2m}+2^{4m}+...+2^{2(\lambda-1)m}) \equiv -2\lambda \pmod{2^m+1}.$$

Hence $2^m + 1|2\lambda$,and therefore $2\lambda \geq 2^m + 1$. This leads to

$p - 1 \geq m(2^m + 1)$, which is impossible since $m \geq 2$.

A theorem of Édouard Lucas: Any prime divisor *p* of $F_n = 2^{2^n} + 1$ is of the form $k2^{n+2} + 1$ whenever n is greater than one.

Sketch of proof:

Let G_p denote the group of non-zero elements of the integers (mod *p*) under multiplication, which has order *p-1*. Notice that *2* (strictly speaking, its image (mod *p*)) has multiplicative order 2^{n+1} in G_p, so that, by Lagrange's theorem, *p-1* is divisible by 2^{n+1} and *p* has the form $k2^{n+1} + 1$ for some integer *k*, as Euler knew. Édouard Lucas went further. Since *n* is greater than *1*, the prime *p* above is congruent to 1 (mod *8*). Hence (as was known to Carl Friedrich Gauss), *2* is a quadratic residue (mod *p*), that is, there in integer *a* such that a^2 -2 is divisible by *p*. Then the image of *a* has order 2^{n+2} in the group G_p and (using Lagrange's theorem again), *p-1* is divisible by 2^{n+2} and *p* has the form $s2^{n+2} + 1$ for some integer *s*.

In fact, it can be seen directly that *2* is a quadratic residue (mod *p*), since $(1 + 2^{2^{n-1}})^2 \equiv 2^{1+2^{n-1}} \pmod{p}$. Since an odd power of *2* is a quadratic residue (mod *p*), so is *2* itself.

Relationship to constructible polygons

An *n*-sided regular polygon can be constructed with compass and straightedge if and only if *n* is the product of a power of 2 and distinct Fermat primes. In other words, if and only if *n* is of the form $n = 2^k p_1 p_2 \ldots p_s$, where *k* is a nonnegative integer and the p_i are distinct Fermat primes.

A positive integer *n* is of the above form if and only if its totient φ(*n*) is a power of 2.

Applications of Fermat numbers

Pseudorandom Number Generation

Fermat primes are particularly useful in generating pseudo-random sequences of numbers in the range 1 … *N*, where *N* is a power of 2. The most common method used is to take any seed value between 1 and *P* − 1, where *P* is a Fermat prime. Now multiply this by a number *A*, which is greater than the square root of *P* and is a primitive root modulo *P* (i.e., it is not a quadratic residue). Then take the result modulo *P*. The result is the new value for the RNG.

$$V_{j+1} = (A \times V_j) \bmod P$$ (see Linear congruential generator, RANDU)

This is useful in computer science since most data structures have members with 2^X possible values. For example, a byte has 256 (2^8) possible values (0–255). Therefore to fill a byte or bytes with random values a random number generator which produces values 1–256 can be used, the byte taking the output value − 1. Very large Fermat primes

are of particular interest in data encryption for this reason. This method produces only pseudorandom values as, after $P - 1$ repetitions, the sequence repeats. A poorly chosen multiplier can result in the sequence repeating sooner than $P - 1$.

Other interesting facts

A Fermat number cannot be a perfect number or part of a pair of amicable numbers.(Luca 2000)

The series of reciprocals of all prime divisors of Fermat numbers is convergent.(Krizek, Luca, Somer 2002)

If $n^n + 1$ is prime, there exists an integer m such that $n = 2^2m$. The equation $n^n + 1 = F_{(2^m+m)}$ holds at that time.[8]

Let the largest prime factor of Fermat number F_n be $P(F_n)$. Then,

$P(F_n) \geq 2^{n+2}(4n + 9) + 1$. (Grytczuk, Luca and Wojtowicz, 2001)

Generalized Fermat numbers

Numbers of the form $a^{2^n} + b^{2^n}$, where $a > 1$ are called **generalized Fermat numbers**. By analogy with the ordinary Fermat numbers, it is common to write generalized Fermat numbers of the form $a^{2^n} + 1$ as $F_n(a)$. In this notation, for instance, the number 100,000,001 would be written as $F_3(10)$.

An odd prime p is a generalized Fermat number if and only if p is congruent to 1 (mod 4) (with the exception of $3 = 2^{2^0} + 1$).

Generalized Fermat primes

Because of the ease of proving their primality, generalized Fermat primes have become in recent years a hot topic for research within the field of number theory. Many of the largest known primes today are generalized Fermat primes.

Generalized Fermat numbers can be prime only for even a, because if a is odd then every generalized Fermat number will be divisible by 2. By analogy with the heuristic argument for the finite number of primes among the base-2 Fermat numbers, it is to be expected that there will be only finitely many generalized Fermat primes for each even base. The smallest prime number $F_n(a)$ with $n > 4$ is $F_5(30)$, or $30^{32}+1$.

A more elaborate theory can be used to predict the number of bases for which $F_n(a)$ will be prime for a fixed n. The number of generalized Fermat primes can be roughly expected to halve as n is increased by 1.

Notes

[1] http://en.wikipedia.org/wiki/Oeis%3Aa000215
[2] http://en.wikipedia.org/wiki/Oeis%3Aa051158
[3] Křížek, Luca, Somer 2001, p. 38, Remark 4.15
[4] Chris Caldwell, "Prime Links++: special forms" (http://primes.utm.edu/links/theory/special_forms/) at The Prime Pages.
[5] Ribenboim, Paulo (1996), *The New Book of Prime Number Records*, New York: Springer, p. 88, ISBN 0387944575.
[6] Keller, Wilfrid (March 27, 2010), "Prime Factors of Fermat Numbers" (http://www.prothsearch.net/fermat.html#Summary), *ProthSearch.net*,
[7] FermatSearch.org (http://www.fermatsearch.org/)
[8] Jeppe Stig Nielsen, "S(n) = n^n + 1" (http://jeppesn.dk/nton.html).

References

- Golomb, S. W. (1963), "On the sum of the reciprocals of the Fermat numbers and related irrationalities", *Canad. J. Math.* **15**: 475–478
- Grytczuk, A.; Luca, F. & Wojtowicz, M. (2001), "Another note on the greatest prime factors of Fermat numbers", *Southeast Asian Bulletin of Mathematics* **25** (1): 111–115, doi:10.1007/s10012-001-0111-4
- Guy, Richard K. (2004), *Unsolved Problems in Number Theory* (3rd ed.), New York: Springer Verlag, pp. A3, A12, B21, ISBN 0387208607
- Křížek, Michal; Luca, Florian & Somer, Lawrence (2001), *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, CMS books in mathematics, **10**, New York: Springer, ISBN 0387953329 (This book contains an extensive list of references.)
- Křížek, Michal; Luca, Florian & Somer, Lawrence (2002), "On the convergence of series of reciprocals of primes related to the Fermat numbers", *Journal of Number Theory* **97** (1): 95–112, doi:10.1006/jnth.2002.2782
- Luca, Florian (2000), "The anti-social Fermat number", *American Mathematical Monthly* **107** (2): 171–173, doi:10.2307/2589441
- Robinson, Raphael M. (1954), "Mersenne and Fermat Numbers", *Proceedings of the American Mathematical Society* **5** (5): 842–846, doi:10.2307/2031878.

External links

- Chris Caldwell, The Prime Glossary: Fermat number (http://primes.utm.edu/glossary/page.php?sort=FermatNumber) at The Prime Pages.
- Luigi Morelli, History of Fermat Numbers (http://www.fermatsearch.org/history.html)
- John Cosgrave, Unification of Mersenne and Fermat Numbers (http://www.spd.dcu.ie/johnbcos/fermat6.htm)
- Wilfrid Keller, Prime Factors of Fermat Numbers (http://www.prothsearch.net/fermat.html)
- Weisstein, Eric W., " Fermat Number (http://mathworld.wolfram.com/FermatNumber.html)" from MathWorld.
- Yves Gallot, Generalized Fermat Prime Search (http://pagesperso-orange.fr/yves.gallot/primes/index.html)
- Mark S. Manasse, Complete factorization of the ninth Fermat number (http://www.google.com/groups?selm=1990Jun15.190100.8505@src.dec.com&oe=UTF-8&output=gplain) (original announcement)

Fibonacci prime

A **Fibonacci prime** is a Fibonacci number that is prime, a type of integer sequence prime.

The first Fibonacci primes are (sequence A005478 [1] in OEIS):

2, 3, 5, 13, 89, 233, 1597, 28657, 514229, 433494437, 2971215073, ...

Known Fibonacci primes

It is not known if there are infinitely many Fibonacci primes. The first 33 are F_n for the n values (sequence A001605 [2] in OEIS):

3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571, 2971, 4723, 5387, 9311, 9677, 14431, 25561, 30757, 35999, 37511, 50833, 81839.

In addition to these proven Fibonacci primes, there have been found probable primes for

n = 104911, 130021, 148091, 201107, 397379, 433781, 590041, 593689, 604711, 931517, 1049897, 1285607, 1636007, 1803059, 1968721.[3]

Except for the case $n = 4$, all Fibonacci primes have a prime index, but not all prime indexes are a Fibonacci prime.

F_p is prime for 8 out of the first 10 primes p; the exceptions are $F_2 = 1$ and $F_{19} = 4181 = 37 \times 113$. However, Fibonacci primes become rarer as the index increases. F_p is prime for only 25 of the 1,229 primes p below 10,000.[4]

As of November 2009, the largest known certain Fibonacci prime is F_{81839}, with 17103 digits. It was proved prime by David Broadhurst and Bouk de Water in 2001.[5] [6] The largest known probable Fibonacci prime is $F_{1968721}$. It has 411439 digits and was found by Henri Lifchitz in 2009.[3]

Divisibility of Fibonacci numbers

Fibonacci numbers that have a prime index p do not share any common divisors greater than 1 with the preceding Fibonacci numbers, due to the identity

$\mathrm{GCD}(F_n, F_m) = F_{\mathrm{GCD}(n,m)}$.[7]

For $n \geq 3$, F_n divides F_m iff n divides m.[8]

If we suppose that m, is a prime number p from the identity above, and n is less than p, then it is clear that F_p, cannot share any common divisors with the preceding Fibonacci numbers.

$\mathrm{GCD}(F_p, F_n) = F_{\mathrm{GCD}(p,n)} = F_1 = 1$

Carmichael's theorem states that every Fibonacci number (except for 1, 8 and 144) has at least one unique prime factor that has not been a factor of the preceding Fibonacci numbers.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa005478

[2] http://en.wikipedia.org/wiki/Oeis%3Aa001605

[3] PRP Top Records, Search for : F(n) (http://www.primenumbers.net/prptop/searchform.php?form=F(n)&action=Search). Retrieved 2009-11-21.

[4] Sloane's A005478 (http://en.wikipedia.org/wiki/Oeis:a005478), A001605 (http://en.wikipedia.org/wiki/Oeis:a001605)

[5] Number Theory Archives announcement by David Broadhurst and Bouk de Water (http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0104&L=nmbrthry&P=R1807&D=0)

[6] Chris Caldwell, The Top Twenty: Fibonacci Number (http://primes.utm.edu/top20/page.php?id=39) from the Prime Pages. Retrieved 2009-11-21.

[7] Paulo Ribenboim, *My Numbers, My Friends*, Springer-Verlag 2000

[8] Wells 1986, p.65

External links

- Weisstein, Eric W., " Fibonacci Prime (http://mathworld.wolfram.com/FibonacciPrime.html)" from MathWorld.
- R. Knott *Fibonacci primes* (http://www.mcs.surrey.ac.uk/Personal/R.Knott/Fibonacci/fibmaths.html#fibprimes)
- Caldwell, Chris. Fibonacci number (http://primes.utm.edu/glossary/page.php/FibonacciNumber.html), Fibonacci prime (http://primes.utm.edu/glossary/page.php?sort=FibonacciPrime), and Record Fibonacci primes (http://primes.utm.edu/top20/page.php?id=39) at the Prime Pages
- Small parallel Haskell program to find probable Fibonacci primes at haskell.org (http://www.haskell.org/haskellwiki/Fibonacci_primes_in_parallel)

Fortunate prime

A **Fortunate number**, named after Reo Fortune, for a given positive integer n is the smallest integer $m > 1$ such that $p_n\# + m$ is a prime number, where the primorial $p_n\#$ is the product of the first n prime numbers.

For example, to find the seventh Fortunate number, one would first calculate the product of the first seven primes (2, 3, 5, 7, 11, 13 and 17), which is 510510. Adding 2 to that gives another even number, while adding 3 would give another multiple of 3. One would similarly rule out the integers up to 18. Adding 19, however, gives 510529, which is prime. Hence 19 is a Fortunate number. The Fortunate number for $p_n\#$ is always above p_n. This is because $p_n\#$, and thus $p_n\# + m$, is divisible by the prime factors of m for $m = 2$ to p_n.

The Fortunate numbers for the first primorials are:

> 3, 5, 7, 13, 23, 17, 19, 23, 37, 61, 67, 61, 71, 47, 107, 59, 61, 109, etc. (sequence A005235 [1] in OEIS).

The Fortunate numbers sorted in numerical order with duplicates removed:

> 3, 5, 7, 13, 17, 19, 23, 37, 47, 59, 61, 67, 71, 79, 89, 101, 103, 107, 109, 127, 151, 157, 163, 167, 191, 197, 199 (A046066 [2]).

Reo Fortune conjectured that no Fortunate number is composite. A **Fortunate prime** is a Fortunate number which is also a prime number. As of 2009, all the known Fortunate numbers are also Fortunate primes.

References

- Chris Caldwell, "The Prime Glossary: Fortunate number" [3] at the Prime Pages.
- Weisstein, Eric W., "Fortunate Prime [4]" from MathWorld.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa005235
[2] http://en.wikipedia.org/wiki/Oeis%3Aa046066
[3] http://primes.utm.edu/glossary/page.php?sort=FortunateNumber
[4] http://mathworld.wolfram.com/FortunatePrime.html

Full reptend prime

In number theory, a **full reptend prime** or **long prime** in base *b* is a prime number *p* such that the formula

$$\frac{b^{p-1}-1}{p}$$

(where *p* does not divide *b*) gives a cyclic number. Therefore the digital expansion of $1/p$ in base *b* repeats the digits of the corresponding cyclic number infinitely. Base 10 may be assumed if no base is specified.
The first few values of *p* for which this formula produces cyclic numbers in decimal are (sequence A001913 [1] in OEIS)

> 7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, 223, 229, 233, 257, 263, 269, 313, 337, 367, 379, 383, 389, 419, 433, 461, 487, 491, 499, 503, 509, 541, 571, 577, 593, 619, 647, 659, 701, 709, 727, 743, 811, 821, 823, 857, 863, 887, 937, 941, 953, 971, 977, 983 …

For example, the case *b* = 10, *p* = 7 gives the cyclic number 142857, thus, 7 is a full reptend prime. Furthermore, 1 divided by 7 written out in base 10 is 0.142857142857142857142857...

Not all values of *p* will yield a cyclic number using this formula; for example *p* = 13 gives 076923076923. These failed cases will always contain a repetition of digits (possibly several).

The known pattern to this sequence comes from algebraic number theory, specifically, this sequence is the set of primes p such that 10 is a primitive root modulo p. Artin's conjecture on primitive roots is that this sequence contains 37.395..% of the primes.

The term "long prime" was used by John Conway and Richard Guy in their *Book of Numbers*. Confusingly, Sloane's OEIS refers to these primes as "cyclic numbers."

The corresponding cyclic number to prime *p* will possess *p* - 1 digits if and only if *p* is a full reptend prime.

Patterns of occurrence of full reptend primes

Advanced modular arithmetic can show that any prime of the following forms:

1. 40*k*+1
2. 40*k*+3
3. 40*k*+9
4. 40*k*+13
5. 40*k*+27
6. 40*k*+31
7. 40*k*+37
8. 40*k*+39

can *never* be a full reptend prime in base-10. The first primes of these forms, with their periods, are:

40*k*+1	**40*k*+3**	**40*k*+9**	**40*k*+13**	**40*k*+27**	**40*k*+31**	**40*k*+37**	**40*k*+39**
41 period 5	43 period 21	89 period 44	13 period 6	67 period 33	31 period 15	37 period 3	79 period 13
241 period 30	83 period 41	409 period 204	53 period 13	107 period 53	71 period 35	157 period 78	199 period 99
281 period 28	163 period 81	449 period 32	173 period 43	227 period 113	151 period 75	197 period 98	239 period 7
401 period 200	283 period 141	569 period 284	293 period 146	307 period 153	191 period 95	277 period 69	359 period 179

However, studies show that *two-thirds* of primes of the form 40*k*+*n*, where $n \neq \{1,3,9,13,27,31,37,39\}$ are full reptend primes. For some sequences, the preponderance of full reptend primes is much greater. For instance, 285 of the 295 primes of form 120*k*+23 below 100000 are full reptend primes, with 20903 being the first that is not full reptend.

References

- Weisstein, Eric W., "Artin's Constant [2]" from MathWorld.
- Weisstein, Eric W., "Full Reptend Prime [3]" from MathWorld.
- Conway, J. H. and Guy, R. K. The Book of Numbers. New York: Springer-Verlag, 1996.
- Francis, Richard L.; "Mathematical Haystacks: Another Look at Repunit Numbers"; in *The College Mathematics Journal*, Vol. 19, No. 3. (May, 1988), pp. 240-246.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa001913

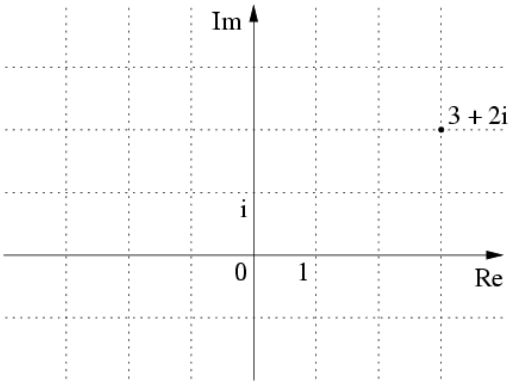
[2] http://mathworld.wolfram.com/ArtinsConstant.html

[3] http://mathworld.wolfram.com/FullReptendPrime.html

Gaussian integer

In number theory, a **Gaussian integer** is a complex number whose real and imaginary part are both integers. The Gaussian integers, with ordinary addition and multiplication of complex numbers, form an integral domain, usually written as **Z**[*i*]. The Gaussian integers are a special case of the quadratic integers. This domain does not have a total ordering that respects arithmetic.

Formally, Gaussian integers are the set



Gaussian integers as lattice points in the complex plane

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

The *norm* of a Gaussian integer is the natural number defined as

$$N(a + bi) = a^2 + b^2 = (a + bi)\overline{(a + bi)} = (a + bi)(a - bi).$$

(Where the overline over "a+bi" refers to the complex conjugate.)

The norm is multiplicative, i.e.

$$N(z \cdot w) = N(z) \cdot N(w).$$

The units of **Z**[*i*] are therefore precisely those elements with norm 1, i.e. the elements

1, −1, *i* and −*i*.

As a unique factorization domain

The Gaussian integers form a unique factorization domain with units 1, −1, *i*, and −*i*. If *x* is a Gaussian integer, the four numbers *x*, *ix*, −*x*, and −*ix* are called the associates of *x*.

The prime elements of **Z**[*i*] are also known as **Gaussian primes**. An associate of a Gaussian prime is also a Gaussian prime. The Gaussian primes are symmetric about the real and imaginary axes. The **positive integer** Gaussian primes are OEIS A002145. It is a common error to refer to only these positive integers as "the Gaussian primes" when in fact this term refers to **all** the Gaussian primes. [1]

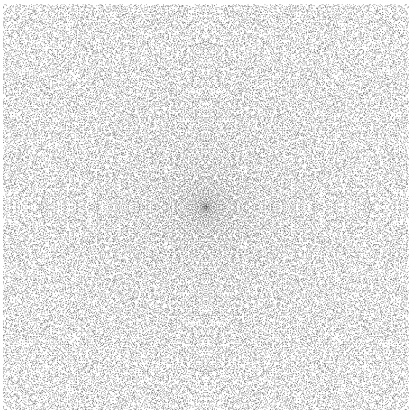
A Gaussian integer $a + bi$ is prime if and only if:

- one of *a*, *b* is zero and the other is a prime of the form $4n + 3$ or its negative $-(4n + 3)$ (where $n \geq 0$)
- or both are nonzero and $a^2 + b^2$ is prime.

The following elaborates on these conditions.

2 is a special case (in the language of algebraic number theory, 2 is the only ramified prime in **Z**[*i*]).

The integer 2 factors as $2 = i(1 - i)^2$ when considered as a Gaussian integer. It is the only prime integer divisible by the square of a Gaussian prime.



Some of the Gaussian primes

The necessary conditions can be stated as following: a Gaussian integer is prime only when its norm is prime, or its norm is a square of a prime. This is because for any Gaussian integer g, notice $g|g\bar{g} = N(g)$. Now $N(g)$ is an integer, and so can be factored as a product $p_1 p_2 \cdots p_n$ of rational primes, that is, as prime numbers in $\mathbb{Z}$ by the fundamental theorem of arithmetic. By definition of prime, if g is prime then it divides p_i for some i. Also, $\bar{g}$ divides $\overline{p_i} = p_i$, so $N(g) = g\bar{g}|p_i^2$. This gives only two options: either the norm of g is prime, or the square of a prime.

If in fact $N(g) = p^2$ for some rational prime p, then both g and $\overline{g}$ divide p^2. Neither can be a unit, and so $g = pu$ and $\overline{g} = p\overline{u}$ where u is a unit. This is to say that either $a = 0$ or $b = 0$, where $g = a + bi$

However, not every rational prime p is a Gaussian prime. 2 is not because $2 = (1 + i)(1 - i)$. Neither are primes of the form $4n + 1$ because Fermat's theorem on sums of two squares assures us they can be written $a^2 + b^2$ for integers a and b, and $a^2 + b^2 = (a + bi)(a - bi)$. The only type of primes remaining are of the form $4n + 3$.

Rational primes of the form $4n + 3$ are also Gaussian primes. For suppose $g = p + 0i$ for $p = 4n + 3$ a prime, and it can be factored $g = hk$. Then $p^2 = N(g) = N(h)N(k)$. If the factorization is non-trivial, then $N(h) = N(k) = p$. But no sum of squares—prime sum or not—can be written $4n + 3$. So the factorization must have been trivial and g is a Gaussian prime.

Likewise i times a rational prime of the form $4n + 3$ is a Gaussian prime, but i times a prime of the form $4n + 1$ is not.

If g is a Gaussian integer with prime norm, then g is a Gaussian prime. This is because if $g = hk$, then $N(g) = N(h)N(k)$ and being prime one of $N(h)$, or $N(k)$ must be 1, hence one of h, k must be a unit.

As an integral closure

The ring of Gaussian integers is the integral closure of **Z** in the field of Gaussian rationals **Q**(*i*) consisting of the complex numbers whose real and imaginary part are both rational.

As a Euclidean domain

It is easy to see graphically that every complex number is within $\frac{\sqrt{2}}{2}$ units of a Gaussian integer. Put another way, every complex number (and hence every Gaussian integer) has a maximal distance of $\frac{\sqrt{2}}{2}\sqrt{N(z)}$ units to some multiple of z, where z is any Gaussian integer; this turns **Z**[*i*] into a Euclidean domain, where $v(z) = N(z)$.

Historical background

The ring of Gaussian integers was introduced by Carl Friedrich Gauss in his second monograph on quartic reciprocity (1832) (see [2]). The theorem of quadratic reciprocity (which he had first succeeded in proving in 1796) relates the solvability of the congruence $x^2 \equiv q \pmod{p}$ to that of $x^2 \equiv p \pmod{q}$. Similarly, cubic reciprocity relates the solvability of $x^3 \equiv q \pmod{p}$ to that of $x^3 \equiv p \pmod{q}$, and biquadratic (or quartic) reciprocity is a relation between $x^4 \equiv q \pmod{p}$ and $x^4 \equiv p \pmod{q}$. Gauss discovered that the law of biquadratic reciprocity and its supplements were more easily stated and proved as statements about "whole complex numbers" (i.e. the Gaussian integers) than they are as statements about ordinary whole numbers (i.e. the integers).

In a footnote he notes that the Eisenstein integers are the natural domain for stating and proving results on cubic reciprocity and indicates that similar extensions of the integers are the appropriate domains for studying higher reciprocity laws.

This paper not only introduced the Gaussian integers and proved they are a unique factorization domain, it also introduced the terms norm, unit, primary, and associate, which are now standard in algebraic number theory.

Unsolved problems

Gauss's circle problem does not deal with the Gaussian integers *per se*, but instead asks for the number of lattice points inside a circle of a given radius centered at the origin. This is equivalent to determining the number of Gaussian integers with norm less than a given value.

There are also conjectures and unsolved problems about the Gaussian primes. Two of them are:

The real and imaginary axes have the infinite set of Gaussian primes 3, 7, 11, 19, ... and their associates. Are there any other lines that have infinitely many Gaussian primes on them? In particular, are there infinitely many Gaussian primes of the form $1+ki$?[3]

Is it possible to walk to infinity using the Gaussian primes as stepping stones and taking steps of bounded length?[4]

Notes

[1] (http://www.research.att.com/~njas/sequences/A002145#COMMENT), OEIS sequence A002145 "COMMENT" section

[2] http://www.ems-ph.org/journals/show_pdf.php?issn=0013-6018&vol=53&iss=1&rank=2

[3] Ribenboim, Ch.III.4.D Ch. 6.II, Ch. 6.IV (Hardy & Littlewood's conjecture E and F)

[4] See Moat-Crossing Problem in the external links

References

- C. F. Gauss, Theoria residuorum biquadraticorum. Commentatio secunda., Comm. Soc. Reg. Sci. Gottingen 7 (1832) 1-34; reprinted in Werke, Georg Olms Verlag, Hildesheim, 1973, pp. 93-148.
- From Numbers to Rings: The Early History of Ring Theory (http://www.ems-ph.org/journals/show_pdf.php?issn=0013-6018&vol=53&iss=1&rank=2), by Israel Kleiner (Elem. Math. 53 (1998) 18 – 35)
- Ribenboim, Paulo (1996). *The New Book of Prime Number Records*. New York: Springer. ISBN 0-387-94457-5.

External links

- www.alpertron.com.ar/GAUSSIAN.HTM (http://www.alpertron.com.ar/GAUSSIAN.HTM) is a Java applet that evaluates expressions containing Gaussian integers and factors them into Gaussian primes.
- www.alpertron.com.ar/GAUSSPR.HTM (http://www.alpertron.com.ar/GAUSSPR.HTM) is a Java applet that features a graphical view of Gaussian primes.
- Henry G. Baker (1993) Complex Gaussian Integers for 'Gaussian Graphics', ACM SIGPLAN Notices, Vol. 28, Issue 11. DOI 10.1145/165564.165571 (http://portal.acm.org/citation.cfm?doid=165564.165571) (html) (http://home.pipeline.com/~hbaker1/Gaussian.html)
- IMO Compendium (http://www.imocompendium.com/index.php?options=mbb|tekstkut&page=0&art=extensions_ddj|f&ttn=Dushan D;jukic1| Arithmetic in Quadratic Fields|N/A&knj=&p=3nbbw45001) text on quadratic extensions and Gaussian Integers in problem solving
- Weisstein, Eric W., " Moat-Crossing Problem (http://mathworld.wolfram.com/Moat-CrossingProblem.html)" from MathWorld.
- Gethner, Ellen; Wagon, Stan; Wick, Brian (April 1998). "A Stroll Through the Gaussian Primes" (http://www.joma.org/images/upload_library/22/Chauvenet/GethnerWagonWick.pdf). *American Mathematical Monthly* **105** (4): 327–337. doi:10.2307/2589708.
- Weisstein, Eric W., " Landau's Problems (http://mathworld.wolfram.com/LandausProblems.html)" from MathWorld.

Genocchi number

The **Genocchi numbers**, named after Angelo Genocchi, are a sequence of integers, G_n that satisfy the relation

$$\frac{2t}{e^t+1} = \sum_{n=1}^{\infty} G_n \frac{t^n}{n!}.$$

The first few Genocchi numbers are 1, −1, 0, 1, 0, −3, 0, 17 (sequence A001469 [1] in OEIS). G_n is 0 for odd $n > 1$.

It has been proven that −3 and 17 are the only prime Genocchi numbers.

They are related to Bernoulli numbers B_n by the formula

$$G_n = 2\left(1-2^n\right) B_n.$$

References

- Weisstein, Eric W., "Genocchi Number [2]" from MathWorld.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa001469

[2] http://mathworld.wolfram.com/GenocchiNumber.html

Goldbach's conjecture

Goldbach's conjecture is one of the oldest unsolved problems in number theory and in all of mathematics. It states:

> Every even integer greater than 2 can be expressed as the sum of two primes.[1]

Such a number is called a **Goldbach number**. Expressing a given even number as a sum of two primes is called a **Goldbach partition** of the number. For example,

4 = 2 + 2

6 = 3 + 3

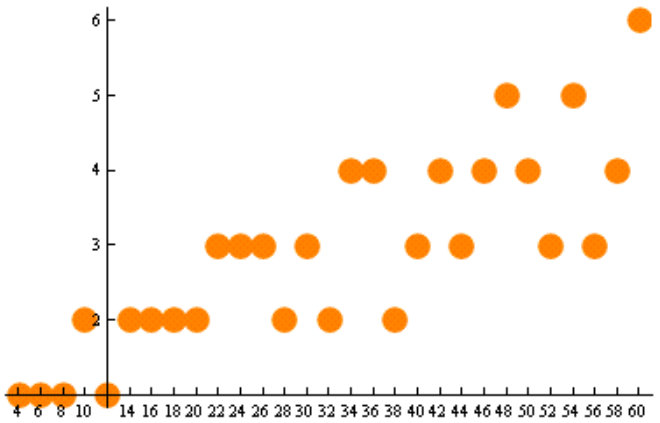
8 = 3 + 5

10 = 7 + 3 or 5 + 5

12 = 5 + 7

14 = 3 + 11 or 7 + 7

...
{52 = 5 + 47, 52 = 11 + 41, 52 = 23 + 29}
{54 = 7 + 47, 54 = 11 + 43, 54 = 13 + 41, 54 = 17 + 37, 54 = 23 + 31}
{56 = 3 + 53, 56 = 13 + 43, 56 = 19 + 37}
{58 = 5 + 53, 58 = 11 + 47, 58 = 17 + 41, 58 = 29 + 29}
{60 = 7 + 53, 60 = 13 + 47, 60 = 17 + 43, 60 = 19 + 41, 60 = 23 + 37,



The number of ways an even number can be represented as the sum of two primes[2]

Origins

On 7 June 1742, the German mathematician Christian Goldbach of originally Brandenburg-Prussia wrote a letter to Leonhard Euler (letter XLIII)[3] in which he proposed the following conjecture:

> Every integer which can be written as the sum of two primes, can also be written as the sum of as many primes as one wishes, until all terms are units.

He then proposed a second conjecture in the margin of his letter:

> Every integer greater than 2 can be written as the sum of three primes.

He considered 1 to be a prime number, a convention subsequently abandoned.[4] The two conjectures are now known to be equivalent, but this did not seem to be an issue at the time. A modern version of Goldbach's marginal conjecture is:

> **Every integer greater than 5 can be written as the sum of three primes**.

Euler replied in a letter dated 30 June 1742, and reminded Goldbach of an earlier conversation they had ("...so Ew vormals mit mir communicirt haben.."), in which Goldbach remarked his original (and not marginal) conjecture followed from the following statement

> **Every even integer greater than 2 can be written as the sum of two primes**,

which is thus also a conjecture of Goldbach. In the letter dated 30 June 1742, Euler stated:

> “Dass ... ein jeder numerus par eine summa duorum primorum sey, halte ich für ein ganz gewisses theorema, ungeachtet ich dasselbe necht demonstriren kann.” ("every even integer is a sum of two primes. I regard this as a completely certain theorem, although I cannot prove it.")[5] [6]

Goldbach's third version (equivalent to the two other versions) is the form in which the conjecture is usually expressed today. It is also known as the "strong", "even", or "binary" Goldbach conjecture, to distinguish it from a weaker corollary. The strong Goldbach conjecture implies the conjecture that **all odd numbers greater than 7 are the sum of three odd primes**, which is known today variously as the "weak" Goldbach conjecture, the "odd"

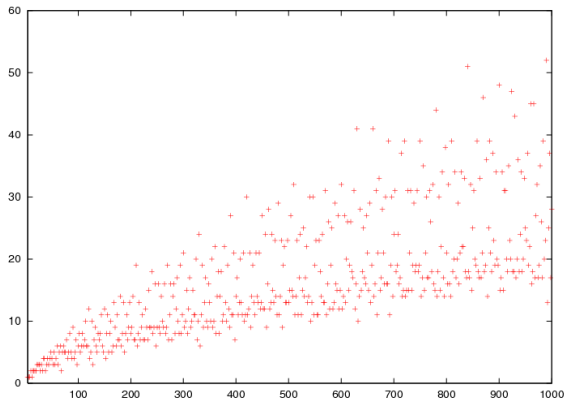
Goldbach conjecture, or the "ternary" Goldbach conjecture. Both questions have remained unsolved ever since, although the weak form of the conjecture appears to be much closer to resolution than the strong one. If the strong Goldbach conjecture is true, the weak Goldbach conjecture will be true by implication.[6]

Verified results

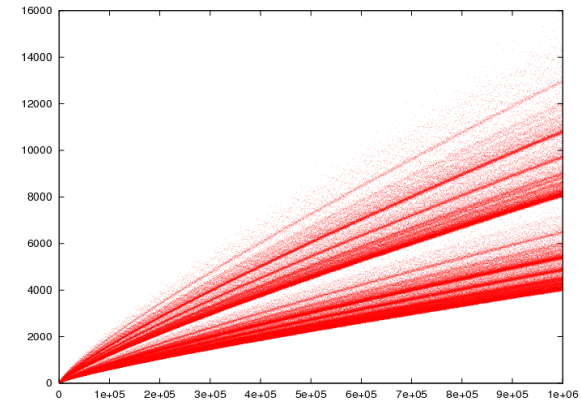
For small values of *n*, the strong Goldbach conjecture (and hence the weak Goldbach conjecture) can be verified directly. For instance, N. Pipping in 1938 laboriously verified the conjecture up to $n \leq 10^5$.[7] With the advent of computers, many more small values of *n* have been checked; T. Oliveira e Silva is running a distributed computer search that has verified the conjecture for $n \leq 1.609*10^{18}$ and some higher small ranges up to $4*10^{18}$ (double checked up to $1*10^{17}$).[8]

Heuristic justification

Statistical considerations which focus on the probabilistic distribution of prime numbers present informal evidence in favour of the conjecture (in both the weak and strong forms) for sufficiently large integers: the greater the integer, the more ways there are available for that number to be represented as the sum of two or three other numbers, and the more "likely" it becomes that at least one of these representations consists entirely of primes.



Number of ways to write an even number n as the sum of two primes (4 ≤ n ≤ 1,000)



Number of ways to write an even number n as the sum of two primes (4 ≤ n ≤ 1,000,000)

$$\sum_{m=3}^{n/2} \frac{1}{\ln m} \frac{1}{\ln(n-m)} \approx \frac{n}{2\ln^2 n}.$$

Since this quantity goes to infinity as *n* increases, we expect that every large even integer has not just one representation as the sum of two primes, but in fact has very many such representations.

The above heuristic argument is actually somewhat inaccurate, because it ignores some dependence between the events of *m* and $n-m$ being prime. For instance, if *m* is odd then $n-m$ is also odd, and if *m* is even, then $n-m$ is even, a non-trivial relation because (besides 2) only odd numbers can be prime. Similarly, if *n* is divisible by 3, and *m* was already a prime distinct from 3, then $n-m$ would also be coprime to 3 and thus be slightly more likely to be prime than a general number. Pursuing this type of analysis more carefully, Hardy and Littlewood in 1923 conjectured (as part of their famous *Hardy-Littlewood prime tuple conjecture*) that for any fixed $c \geq 2$, the number of representations of a large integer *n* as the sum of *c* primes $n = p_1 + \cdots + p_c$ with $p_1 \leq \cdots \leq p_c$ should be asymptotically equal to

$$\left(\prod_p \frac{p\gamma_{c,p}(n)}{(p-1)^c}\right) \int_{2\leq x_1\leq\cdots\leq x_c : x_1+\ldots+x_c=n} \frac{dx_1 \ldots dx_{c-1}}{\ln x_1 \ldots \ln x_c}$$

where the product is over all primes p, and $\gamma_{c,p}(n)$ is the number of solutions to the equation $n = q_1 + \ldots + q_c \mod p$ in modular arithmetic, subject to the constraints $q_1, \ldots, q_c \neq 0 \mod p$. This formula has been rigorously proven to be asymptotically valid for $c \geq 3$ from the work of Vinogradov, but is still only a conjecture when $c = 2$. In the latter case, the above formula simplifies to 0 when n is odd, and to

$$2\Pi_2 \left(\prod_{p|n;p\geq 3} \frac{p-1}{p-2} \right) \int_2^n \frac{dx}{\ln^2 x} \approx 2\Pi_2 \left(\prod_{p|n;p\geq 3} \frac{p-1}{p-2} \right) \frac{n}{\ln^2 n}$$

when n is even, where Π_2 is the twin prime constant

$$\Pi_2 := \prod_{p\geq 3} \left(1 - \frac{1}{(p-1)^2} \right) = 0.6601618158\ldots.$$

This asymptotic is sometimes known as the *extended Goldbach conjecture*. The strong Goldbach conjecture is in fact very similar to the twin prime conjecture, and the two conjectures are believed to be of roughly comparable difficulty.

The Goldbach partition functions shown here can be displayed as histograms which informatively illustrate the above equations. See Goldbach's comet.[9]

Rigorous results

Considerable work has been done on the weak Goldbach conjecture.

The strong Goldbach conjecture is much more difficult. Using the method of Vinogradov, Chudakov,[10] van der Corput,[11] and Estermann[12] showed that almost all even numbers can be written as the sum of two primes (in the sense that the fraction of even numbers which can be so written tends towards 1). In 1930, Lev Schnirelmann proved that every even number $n \geq 4$ can be written as the sum of at most 20 primes. This result was subsequently improved by many authors; currently, the best known result is due to Olivier Ramaré, who in 1995 showed that every even number $n \geq 4$ is in fact the sum of at most six primes. In fact, resolving the weak Goldbach conjecture will also directly imply that every even number $n \geq 4$ is the sum of at most four primes.[13]

Chen Jingrun showed in 1973 using the methods of sieve theory that every sufficiently large even number can be written as the sum of either two primes, or a prime and a semiprime (the product of two primes)[14] —e.g., 100 = 23 + 7·11.

In 1975, Hugh Montgomery and Robert Charles Vaughan showed that "most" even numbers were expressible as the sum of two primes. More precisely, they showed that there existed positive constants c and C such that for all sufficiently large numbers N, every even number less than N is the sum of two primes, with at most CN^{1-c} exceptions. In particular, the set of even integers which are not the sum of two primes has density zero.

Linnik proved in 1951 the existence of a constant K such that every sufficiently large even number is the sum of two primes and at most K powers of 2. Roger Heath-Brown and Jan-Christoph Schlage-Puchta in 2002 found that K=13 works.[15] This was improved to K=8 by Pintz and Ruzsa.[16]

One can pose similar questions when primes are replaced by other special sets of numbers, such as the squares. For instance, it was proven by Lagrange that every positive integer is the sum of four squares. See Waring's problem and the related Waring–Goldbach problem on sums of powers of primes.

Attempted proofs

As with many famous conjectures in mathematics, there are a number of purported proofs of the Goldbach conjecture, none accepted by the mathematical community.

Similar conjectures

- Lemoine's conjecture (also called *Levy's conjecture*) - states that all odd integers greater than 5 can be represented as the sum of an odd prime number and an even semiprime.
- Waring–Goldbach problem - asks whether large numbers can be expressed as a sum, with at most a constant number of terms, of like powers of primes.

In popular culture

- To generate publicity for the novel *Uncle Petros and Goldbach's Conjecture* by Apostolos Doxiadis, British publisher Tony Faber offered a $1,000,000 prize if a proof was submitted before April 2002. The prize was not claimed.
- The television drama *Lewis* featured a mathematics professor who had won the Fields medal for his work on Goldbach's conjecture.
- Isaac Asimov's short story "Sixty Million Trillion Combinations" featured a mathematician who suspected that his work on Goldbach's conjecture had been stolen.
- In the Spanish movie *La habitación de Fermat* (2007), a young mathematician claims to have proved the conjecture.
- A reference is made to the conjecture in the Futurama straight-to-DVD film *The Beast with a Billion Backs*, in which multiple elementary proofs are found in a Heaven-like scenario.
- Frederik Pohl's novella "The Gold at the Starbow's End" (1972) featured a crew on an interstellar flight that solved Goldbach's conjecture.
- Michelle Richmond's novel "No One You Know" (2008) features the murder of a mathematician who had been working on solving Goldbach's conjecture.

References

[1] Weisstein, Eric W., " Goldbach Number (http://mathworld.wolfram.com/GoldbachNumber.html)" from MathWorld.

[2] "Goldbach's Conjecture" (http://demonstrations.wolfram.com/GoldbachConjecture/) by Hector Zenil, Wolfram Demonstrations Project, 2007.

[3] (http://www.math.dartmouth.edu/~euler/correspondence/letters/OO0765.pdf)

[4] Weisstein, Eric W., " Goldbach Conjecture (http://mathworld.wolfram.com/GoldbachConjecture.html)" from MathWorld.

[5] Ingham, AE. "Popular Lectures" (http://www.claymath.org/Popular_Lectures/U_Texas/Riemann_1.pdf) (PDF). . Retrieved 2009-09-23.

[6] Caldwell, Chris (2008). "Goldbach's conjecture" (http://primes.utm.edu/glossary/page.php?sort=goldbachconjecture). . Retrieved 2008-08-13.

[7] Pipping, N. "Die Goldbachsche Vermutung und der Goldbach-Vinogradovsche Satz." Acta. Acad. Aboensis, Math. Phys. 11, 4-25, 1938.

[8] Tomás Oliveira e Silva, (http://www.ieeta.pt/~tos/goldbach.html). Retrieved 25 April 2008.

[9] Fliegel, Henry F.; Robertson, Douglas S.; "Goldbach's Comet: the numbers related to Goldbach's Conjecture"; Journal of Recreational Mathematics, v21(1) 1-7, 1989.

[10] Chudakov, Nikolai G. (1937), *Doklady Akademii Nauk SSSR* **17**: 335–338.

[11] Van der Corput, J. G, "Sur l'hypothèse de Goldbach." Proc. Akad. Wet. Amsterdam, **41** (1938), 76-80.

[12] Estermann, T. "On Goldbach's problem: proof that almost all even positive integers are sums of two primes." Proc. London Math. Soc., (2) **44** (1938), 307-314.

[13] Sinisalo, Matti K. (Oct., 1993), "Checking the Goldbach Conjecture up to 4 10^{11}", *Mathematics of Computation* **61** (204): 931–934

[14] J. R. Chen, On the representation of a larger even integer as the sum of a prime and the product of at most two primes. Sci. Sinica 16 (1973), 157--176.

[15] D. R. Heath-Brown, J. C. Puchta, Integers represented as a sum of primes and powers of two. (http://arxiv.org/abs/math.NT/0201299) The Asian Journal of Mathematics, **6** (2002), no. 3, pages 535-565.

[16] J. Pintz, I. Z. Ruzsa: On Linnik's approximation to Goldbach's problem, I, *Acta Arithmetica*, **109**(2003), 169–194.

Further reading

- Deshouillers, J.-M.; Effinger, G.; te Riele, H. & Zinoviev, D. (1997), "A complete Vinogradov 3-primes theorem under the Riemann hypothesis" (http://www.ams.org/era/1997-03-15/S1079-6762-97-00031-0/S1079-6762-97-00031-0.pdf), *Electron. Res. Announc. Amer. Math. Soc.* **3**: 99–104, doi:10.1090/S1079-6762-97-00031-0
- Doxiadis, Apostolos (2001), *Uncle Petros and Goldbach's Conjecture*, New York: Bloomsbury, ISBN 1582341281
- Montgomery, H. L. & Vaughan, R. C. (1975), "The exceptional set in Goldbach's problem. Collection of articles in memory of Jurii Vladimirovich Linnik", *Acta arithmetica* **27**: pp. 353–370

External links

- Goldbach's original letter to Euler - PDF format (in German and Latin) (http://www.math.dartmouth.edu/~euler/correspondence/letters/OO0765.pdf)
- *Goldbach's conjecture* (http://primes.utm.edu/glossary/page.php?sort=GoldbachConjecture), part of Chris Caldwell's Prime Pages.
- *Goldbach conjecture verification* (http://www.ieeta.pt/~tos/goldbach.html), Tomás Oliveira e Silva's distributed computer search.
- Online tool (http://wims.unice.fr/wims/wims.cgi?module=tool/number/goldbach.en) to test Goldbach's conjecture on submitted integers.
- Goldbach Weave (http://wardley.org/misc/goldbach.html) showing a graphical representation of Goldbach's conjecture.

Good prime

A **good prime** is a prime number whose square is greater than the product of any two primes at the same number of positions before and after it in the sequence of primes.

A good prime satisfies the inequality

$$p_n^2 > p_{(n-i)} \cdot p_{(n+i)}$$

for all $1 \le i \le n-1$. p_n is the nth prime.

There are infinitely many good primes.[1] The first good primes are

5, 11, 17, 29, 37, 41, 53, 59, 67, 71, 97, 101, 127, 149 (sequence A028388 [2] in OEIS).

References

[1] Weisstein, Eric W., " Good Prime (http://mathworld.wolfram.com/GoodPrime.html)" from MathWorld.

[2] http://en.wikipedia.org/wiki/Oeis%3Aa028388

Happy number

A **happy number** is defined by the following process. Starting with any positive integer, replace the number by the sum of the squares of its digits, and repeat the process until the number equals 1 (where it will stay), or it loops endlessly in a cycle which does not include 1. Those numbers for which this process ends in 1 are **happy numbers**, while those that do not end in 1 are **unhappy numbers** (or **sad numbers**[1]).

Overview

More formally, given a number $n = n_0$, define a sequence n_1, n_2, ... where $n_{i+1}$is the sum of the squares of the digits of n_i . Then *n* is happy if and only if there exists *i* such that $n_i = 1$.

If a number is happy, then all members of its sequence are happy; if a number is unhappy, all members of its sequence are unhappy.

For example, 7 is happy, as the associated sequence is:

$7^2 = 49$

$4^2 + 9^2 = 97$

$9^2 + 7^2 = 130$

$1^2 + 3^2 + 0^2 = 10$

$1^2 + 0^2 = 1.$

The happy numbers below 500 are

1, 7, 10, 13, 19, 23, 28, 31, 32, 44, 49, 68, 70, 79, 82, 86, 91, 94, 97, 100, 103, 109, 129, 130, 133, 139, 167, 176, 188, 190, 192, 193, 203, 208, 219, 226, 230, 236, 239, 262, 263, 280, 291, 293, 301, 302, 310, 313, 319, 320, 326, 329, 331, 338, 356, 362, 365, 367, 368, 376, 379, 383, 386, 391, 392, 397, 404, 409, 440, 446, 464, 469, 478, 487, 490, 496 (sequence A007770 [2] in OEIS).

The happiness of a number is preserved by rearranging the digits, and by inserting or removing any number of zeros anywhere in the number.

Sequence behavior

If *n* is not happy, then its sequence does not go to 1. What happens instead is that it ends up in the cycle

4, 16, 37, 58, 89, 145, 42, 20, 4, ...

To see this fact, first note that if *n* has *m* digits, then the sum of the squares of its digits is at most 9^2m , or $81m$.

For $m = 4$and above,

$$n \geq 10^{m-1} > 81m$$

so any number over 1000 gets smaller under this process and in particular becomes a number with strictly fewer digits. Once we are under 1000, the number for which the sum of squares of digits is largest is 999, and the result is 3 times 81, that is, 243.

- In the range 100 to 243, the number 199 produces the largest next value, of 163.
- In the range 100 to 163, the number 159 produces the largest next value, of 107.
- In the range 100 to 107, the number 107 produces the largest next value, of 50.

Considering more precisely the intervals [244,999], [164,243], [108,163] and [100,107], we see that every number above 99 gets strictly smaller under this process. Thus, no matter what number we start with, we eventually drop below 100. An exhaustive search then shows that every number in the interval [1,99] either is happy or goes to the above cycle.

The above work produces the interesting result that no positive integer other than 1 is the sum of the squares of its own digits.

There are infinitely many happy numbers and infinitely many unhappy numbers. For example, if you wonder if any number will produce 14308, say, the quick response is to write down the digit 1 14308 times and you have created such a number. In fact, you have created infinitely many such numbers since there is nothing to stop you slotting in as many zero digits as you fancy.

The first pair of consecutive happy numbers is 31, 32. The first set of triplets is 1880, 1881, and 1882.

An interesting question is to wonder about the density of happy numbers. In the interval [1,243] 15.6% (to 3 significant figures) are happy.

Happy primes

A **happy prime** is a number that is both happy and prime. The happy primes below 500 are

> 7, 13, 19, 23, 31, 79, 97, 103, 109, 139, 167, 193, 239, 263, 293, 313, 331, 367, 379, 383, 397, 409, 487 (sequence A035497 [3] in OEIS).

All numbers, and therefore all primes, of the form $10^n + 3$ and $10^n + 9$ for n greater than 0 are Happy (This of course does not mean that these are the only happy primes, as evidenced by the sequence above). To see this, note that

- All such numbers will have at least 2 digits;
- The first digit will always be *1* due to the 10^n
- The last digit will always be either *3* or *9*.
- Any other digits will always be *0* (and therefore will not contribute to the sum of squares of the digits).
  - The sequence for adding 3 is: $1^2 + 3^2 = 10 \rightarrow 1^2 = 1$
  - The sequence for adding 9 is: $1^2 + 9^2 = 82 \rightarrow 8^2 + 2^2 = 64 + 4 = 68 \rightarrow 6^2 + 8^2 = 36 + 64 = 100$ -> 1

The palindromic prime $10^{150006} + 7426247 \times 10^{75000} + 1$ is also a happy prime with 150,007 digits because the many 0's do not contribute to the sum of squared digits, and $1^2 + 7^2 + 4^2 + 2^2 + 6^2 + 2^2 + 4^2 + 7^2 + 1^2 = 176$, which is a happy number. Paul Jobling discovered the prime in 2005.[4]

As of 2010, the largest known happy prime is $2^{42643801} - 1$(Mersenne prime). Its decimal expansion has 12,837,064 digits.[5]

Special happy numbers

- 986543210 : Greatest happy number with no redundant digits
- 1234456789 : Smallest zeroless pandigital happy number
- 10234456789 : Smallest pandigital happy number
- 13456789298765431 : Smallest zeroless pandigital palindromic happy number
- 1034567892987654301 : Smallest pandigital palindromic happy number

Happy pythagorean triplets

- All Pythagorean triplets with all integers happy and less than 10000

(700, 3465, 3535)	(748, 8211, 8245)	(910, 8256, 8306)	(940, 2109, 2309)
(940, 4653, 4747)	(1092, 1881, 2175)	(1323, 4536, 4725)	(1527, 2036, 2545)
(1785, 3392, 3833)	(1900, 1995, 2755)	(1995, 4788, 5187)	(2715, 3620, 4525)
(2751, 8360, 8801)	(2784, 6440, 7016)	(3132, 7245, 7893)	(3135, 7524, 8151)
(3290, 7896, 8554)	(3367, 3456, 4825)	(3680, 5313, 6463)	(4284, 5313, 6825)
(4633, 5544, 7225)	(5178, 6904, 8630)	(5286, 7048, 8810)	(5445, 6308, 8333)
(5712, 7084, 9100)	(6528, 7480, 9928)		

Happy numbers in other bases

The definition of happy numbers depends on the decimal (i.e., base 10) representation of the numbers. The definition can be extended to other bases.

To represent numbers in other bases, we may use a subscript to the right to indicate the base. For instance, 100_2 represents the number 4, and

$$123_5 = 1 \cdot 5^2 + 2 \cdot 5 + 3 = 38.$$

Then, it is easy to see that there are happy numbers in every base. For instance, the numbers

$$1_b, 10_b, 100_b, 1000_b, \ldots$$

are all happy, for any base *b*.

By a similar argument to the one above for decimal happy numbers, unhappy numbers in base *b* lead to cycles of numbers less than 1000_b. If $n < 1000_b$, then the sum of the squares of the base-*b* digits of *n* is less than or equal to

$$3(b-1)^2$$

which can be shown to be less than b^3. This shows that once the sequence reaches a number less than 1000_b, it stays below 1000_b, and hence must cycle or reach 1.

In base 2, all numbers are happy. All binary numbers larger than 1000_2 decay into a value equal to or less than 1000_2, and all such values are happy: The following four sequences contain all numbers less than 1000_2:

$$111_2 \to 11_2 \to 10_2 \to 1$$
$$110_2 \to 10_2 \to 1$$
$$101_2 \to 10_2 \to 1$$
$$100_2 \to 1.$$

Since all sequences end in 1, we conclude that all numbers are happy in base 2. This makes base 2 a *happy base*.

The only known happy bases are 2 and 4. There are no others less than 500,000,000.[6]

Cubing the digits rather than squaring

An interesting extension to the Happy Numbers problem is to find the sum of the cubes of the digits rather than the sum of the squares of the digits. For example, working in base 10, 1579 is happy, since:

$1^3+5^3+7^3+9^3=1+125+343+729=1198$

$1^3+1^3+9^3+8^3=1+1+729+512=1243$

$1^3+2^3+4^3+3^3=1+8+64+27=100$

$1^3+0^3+0^3=1$

In the same way that when summing the squares of the digits (and working in base 10) each number above 243(=3*81) produces a number which is strictly smaller, when summing the cubes of the digits each number above 2916(=4*729) produces a number which is strictly smaller.

By conducting an exhaustive search of [1,2916] one finds that for summing the cubes of digits base 10 there are happy numbers and eight different types of unhappy number:

those that eventually reach 371 which perpetually produces itself.

those that eventually reach 153 which perpetually produces itself.

those that eventually reach the loop $133 \to 55 \to 250 \to 133 \to \ldots$

those that eventually reach 370 which perpetually produces itself.

those that eventually reach the loop $217 \to 352 \to 160 \to 217 \to \ldots$

those that eventually reach 407 which perpetually produces itself.

those that eventually reach the loop $1459 \to 919 \to 1459 \to \ldots$

those that eventually reach the loop $136 \to 244 \to 136 \to \ldots$

Starting with the happy numbers and then following with the unhappy numbers in the order given above, the density of each type of number in the interval [1,2916] is 1.54%, 28.4%, 34.7%, 5.73%, 17.4%, 4.60%, 3.60%, 2.67% and 1.34% (all to 3 significant figures).

Intriguingly, the second type of unhappy number includes all multiples of three . This fact can be proved by the exhaustive search up to 2916 and noting that a number is a multiple of three if and only if the sum of digits is a multiple of three if and only if the sum of its cubed digits are a multiple of three. By similar reasoning, all happy numbers of this type must have a remainder of 1 when dividing by 3.

One interesting result which comes from the above work is that the only positive whole numbers which are the sum of the cubes of their digits are 1, 153, 370, 371 and 407.

Origin

The origin of happy numbers is not clear. Happy numbers were brought to the attention of Reg Allenby (a British author and Senior Lecturer in pure mathematics at Leeds University) by his daughter, who had learned of them at school. However they "may have originated in Russia" (Guy 2004:§E34).

Popular culture

In the *Doctor Who* episode "42", a sequence of happy primes (313, 331, 367, 379) is used as a code for unlocking a sealed door on a spaceship about to collide with a sun.

Programming examples

- Simple test in Python to check if a number is happy.

```
def is_Happy(k):
  s=set()
  while k != 1:
    digs=[int(i) for i in str(k)]
    k=sum([i**2 for i in digs])
    if k in s: return False
    s.add(k)
  return True
```

References

[1] "Sad Number" (http://mathworld.wolfram.com/SadNumber.html). Wolfram Research, Inc.. . Retrieved 2009-09-16.
[2] http://en.wikipedia.org/wiki/Oeis%3Aa007770
[3] http://en.wikipedia.org/wiki/Oeis%3Aa035497
[4] The Prime Database: 10^150006+7426247*10^75000+1 (http://primes.utm.edu/primes/page.php?id=76550)
[5] Prime Pages entry for $2^{42643801}$ - 1 (http://primes.utm.edu/primes/page.php?id=88847)
[6] A161872 (http://en.wikipedia.org/wiki/Oeis:a161872)

Additional resources

- Walter Schneider, Mathews: Happy Numbers (http://web.archive.org/web/20060204094653/http://www.wschnei.de/digit-related-numbers/happy-numbers.html).
- Weisstein, Eric W., " Happy Number (http://mathworld.wolfram.com/HappyNumber.html)" from MathWorld.
- Happy Numbers (http://mathforum.org/library/drmath/view/55856.html) at The Math Forum.
- Guy, Richard (2004). *Unsolved Problems in Number Theory (third edition)*. Springer-Verlag. ISBN 0-387-20860-7.

External links

- Reg Allenby page (http://www.maths.leeds.ac.uk/pure/staff/allenby/allenby.html)

Higgs prime

A **Higgs prime** is a prime number with a totient (one less than the prime) that evenly divides the square of the product of the smaller Higgs primes. (This can be generalized to cubes, fourth powers, etc.) To put it algebraically, given an exponent *a*, a Higgs prime Hp_n satisfies

$$\phi(Hp_n) | \prod_{i=1}^{n-1} {Hp_i}^a \text{ and } Hp_n > Hp_{n-1}$$

where Φ(*x*) is Euler's totient function.

For squares, the first few Higgs primes are 2, 3, 5, 7, 11, 13, 19, 23, 29, 31, 37, 43, 47, ... (sequence A007459 [1] in OEIS). So, for example, 13 is a Higgs prime because the square of the product of the smaller Higgs primes is 5336100, and divided by 12 this is 444675. But 17 is not a Higgs prime because the square of the product of the smaller primes is 901800900, which leaves a remainder of 4 when divided by 16.

From observation of the first few Higgs primes for squares through seventh powers, it would seem more compact to list those primes that are not Higgs primes:

Exponent	75th Higgs prime	Not Higgs prime below 75th Higgs prime
2	827	17, 41, 73, 83, 89, 97, 103, 109, 113, 137, 163, 167, 179, 193, 227, 233, 239, 241, 251, 257, 271, 281, 293, 307, 313, 337, 353, 359, 379, 389, 401, 409, 433, 439, 443, 449, 457, 467, 479, 487, 499, 503, 521, 541, 563, 569, 577, 587, 593, 601, 613, 617, 619, 641, 647, 653, 673, 719, 739, 751, 757, 761, 769, 773, 809, 811, 821, 823
3	521	17, 97, 103, 113, 137, 163, 193, 227, 239, 241, 257, 307, 337, 353, 389, 401, 409, 433, 443, 449, 479, 487
4	419	97, 193, 257, 353, 389
5	397	193, 257
6	389	257
7	389	257

Observation further reveals that a Fermat prime $2^{2^n} + 1$ can't be a Higgs prime for the *a*th power if *a* is less than 2^n.

It's not known if there are infinitely many Higgs primes for any exponent *a* greater than 1. The situation is quite different for *a* = 1. There are only four of them: 2, 3, 7 and 43 (a sequence suspiciously similar to Sylvester's sequence). In 1993, Burris and Lee found that about a fifth of the primes below a million are Higgs prime, and they concluded that even if the sequence of Higgs primes for squares is finite, "a computer enumeration is not feasible."

References

- S. Burris & S. Lee, "Tarski's high school identities", *Amer. Math. Monthly* **100** (1993): 233
- N. Sloane & S. Plouffe, *The Encyclopedia of Integer Sequences*, New York: Academic Press (1995): M0660

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa007459

Highly cototient number

In number theory, a branch of mathematics, a **highly cototient number** is a positive integer k which is above one and has more solutions to the equation

$$x - \varphi(x) = k,$$

than any other integer below k and above one. Here, φ is Euler's totient function. There are infinitely many solutions to the equation for $k = 1$ so this value is excluded in the definition. The first few highly cototient numbers are:

2, 4, 8, 23, 35, 47, 59, 63, 83, 89, 113, 119, 167, 209, 269, 299, 329, 389, 419, 509, 629, 659, 779, 839, 1049, 1169, 1259, 1469, 1649, 1679, 1889 (sequence A100827 [1] in OEIS).

There are many odd highly cototient numbers. In fact, after 8, all the numbers listed above are odd, and after 167 all the numbers listed above are congruent to 9 modulo 10.

The concept is somewhat analogous to that of highly composite numbers. Just as there are infinitely many highly composite numbers, there are also infinitely many highly cototient numbers. Computations become harder, since integer factorization does, as the numbers get larger.

Primes

The first few highly cototient numbers which are primes (sequence A105440 [2] in OEIS) are

2, 23, 47, 59, 83, 89, 113, 167, 269, 389, 419, 509, 659, 839.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa100827
[2] http://en.wikipedia.org/wiki/Oeis%3Aa105440

Illegal prime

An **illegal prime** is a prime number that represents information forbidden to possess or distribute. One of the first illegal primes was discovered in 2001. When interpreted a particular way, it describes a computer program which bypasses the digital rights management scheme used on DVDs. Distribution of such a program in the United States is illegal under the Digital Millennium Copyright Act.[1] Illegal primes are a subset of illegal numbers.

Background

One of the earliest illegal prime numbers was generated in March 2001 by Phil Carmody. Its binary representation corresponds to a compressed version of the C source code of a computer program implementing the DeCSS decryption algorithm, which can be used by a computer to circumvent a DVD's copy protection.[1]

```
void CSSdescramble(unsigned char *sec,unsigned char *key) {
  unsigned int t1,t2,t3,t4,t5,t6;
  unsigned char *end=sec+0x800;
  t1=key[0]^sec[0x54]|0x100;
  t2=key[1]^sec[0x55];
  t3=(*((unsigned int *)(key+2)))^(*((unsigned int *)(sec+0x56)));
  t4=t3&7;
  t3=t3*2+8-t4;
  sec+=0x80;
  t5=0;
  while(sec!=end) {
    t4=CSSt2[t2]^CSSt3[t1];
    t2=t1>>1;
    t1=((t1&1)<<8)^t4;
    t4=CSSt5[t4];
    t6=(((((((t3>>3)^t3)>>1)^t3)>>8)^t3)>>5)&0xff;
    t3=(t3<<8)|t6;
    t6=CSSt4[t6];
    t5+=t6+t4;
    *sec++=CSSt1[*sec]^(t5&0xff);
    t5>>=8;
  }
}
```

The DeCSS code can be used by a computer to circumvent a DVD's copy protection.

Protests against the indictment of DeCSS author Jon Johansen and legislation prohibiting publication of DeCSS code took many forms. One of them was the representation of the illegal code in a form that had an *intrinsically archivable* quality. Since the bits making up a computer program also represent a number, the plan was for the number to have some special property that would make it archivable and publishable (one method was to print it on a t-shirt). The primality of a number is a fundamental property of number theory, and is therefore not dependent on legal definitions of any particular jurisdiction.

The large prime database of The Prime Pages website records the top 20 primes of various special forms; one of them is proof of primality using the elliptic curve primality proving (ECPP) algorithm. Thus, if the number were large enough, and proved prime using ECPP, it would be published.

Discovery

By exploitation of the fact that the gzip compression program ignores bytes after the end of a null terminated compressed file, a set of candidate primes was generated, each of which would result in the DeCSS C code when unzipped. Of these, several were identified as probable prime using the open source program OpenPFGW, and one of them was proved prime using the ECPP algorithm implemented by the Titanix software. Even at the time of discovery in 2001, this 1401 digit number was too small to be mentioned, so Carmody created a 1905-digit prime which was the tenth largest prime found using ECPP.

Following this, Carmody also discovered another prime, this one directly executable machine language for Linux i386, implementing the same functionality.

The first illegal prime number

The Register gives the 1401 digit number as:[2] [3]

4 85650 78965 73978 29309 84189 46942 86137 70744 20873 51357 92401 96520 73668 69851 34010 47237 44696 87974 39926 11751 09737 77701 02744 75280 49058 83138 40375 49709 98790 96539 55227 01171 21570 25974 66699 32402 26834 59661 96060 34851 74249 77358 46851 88556 74570 25712 54749 99648 21941 84655 71008 41190 86259 71694 79707 99152 00486 67099 75923 59606 13207 25973 79799 36188 60631 69144 73588 30024 53369 72781 81391 47979 55513 39994 93948 82899 84691 78361 00182 59789 01031 60196 18350 34344 89568 70538 45208 53804 58424 15654 82488 93338 04747 58711 28339 59896 85223 25446 08408 97111 97712 76941 20795 86244 05471 61321 00500 64598 20176 96177 18094 78113 62200 27234 48272 24932 32595 47234 68800 29277 76497 90614 81298 40428 34572 01463 48968 54716 90823 54737 83566 19721 86224 96943 16227 16663 93905 54302 41564 73292 48552 48991 22573 94665 48627 14048 21171 38124 38821 77176 02984 12552 44647 44505 58346 28144 88335 63190 27253 19590 43928 38737 64073 91689 12579 24055 01562 08897 87163 37599 91078 87084 90815 90975 48019 28576 84519 88596 30532 38234 90558 09203 29996 03234 47114 07760 19847 16353 11617 13078 57608 48622 36370 28357 01049 61259 56818 46785 96533 31007 70179 91614 67447 25492 72833 48691 60006 47585 91746 27812 12690 07351 83092 41530 10630 28932 95665 84366 20008 00476 77896 79843 82090 79761 98594 93646 30938 05863 36721 46969 59750 27968 77120 57249 96666 98056 14533 82074 12031 59337 70309 94915 27469 18356 59376 21022 20068 12679 82734 45760 93802 03044 79122 77498 09179 55938 38712 10005 88766 68925 84487 00470 77255 24970 60444 65212 71304 04321 18261 01035 91186 47666 29638 58495 08744 84973 73476 86142 08805 29443.

The first illegal executable prime number

The following 1811 digit prime number (discovered by Phil Carmody) can represent a non-compressed i386 ELF executable that reads CSS-encrypted data and outputs the decrypted data.[4]

49310 83597 02850 19002 75777 67239 07649 57284 90777 21502 08632 08075 01840 97926 27885 09765 88645 57802 01366 00732 86795 44734 11283 17353 67831 20155 75359 81978 54505 48115 71939 34587 73300 38009 93261 95058 76452 50238 20408 11018 98850 42615 17657 99417 04250 88903 70291 19015 87003 04794 32826 07382 14695 41570 33022 79875 57681 89560 16240 30064 11151 69008 72879 83819 42582 71674 56477 48166 84347 92846 45809 29131 53186 00700 10043 35318 93631 93439 12948 60445 03709 91980 04770 94629 21558 18071 11691 53031 87628 84778 78354 15759 32891 09329 54473 50881 88246 54950 60005 01900 62747 05305 38116 42782 94267 47485 34965 25745 36815 11706 55028 19055 52656 22135 31463 10421 00866 28679 71144 46706 36692 19825 86158 11125 15556 50481 34207 68673 23407 65505 48591 08269 56266 69306 62367 99702 10481 23965 62518 00681 83236 53959 34839 56753 57557 53246 19023 48106 47009 87753 02795 61868 92925 38069 33052 04238 14996 99454 56945 77413 83356 89906 00587 08321 81270 48611 33682 02651 59051 66351 87402 90181 97693 93767 78529 28722 10955 04129 25792 57381 86605 84501 50552 50274 99477 18831 29310 45769 80909 15304 61335 94190 30258 81320 59322 77444 38525 50466 77902 45186 97062 62778 88919 79580 42306 57506 15669 83469 56177 97879 65920 16440 51939 96071 69811 12615 19561 02762 83233 98257 91423 32172 69614 43744 38105 64855 29348 87634 92103 09887 02878 74532 33132 53212 26786 33283 70279 25099 74996 94887 75936 91591 76445 88032 71838 47402 35933 02037 48885 06755 70658 79194 61134 19323 07814 85443 64543 75113 20709 86063 90746 41756 41216 35042 38800 29678 08558 67037 03875 09410 76982 11837 65499 20520 43682 55854 64228 85024 29963 32268 53691 24648 55000 75591 66402 47292 40716 45072 53196 74499 95294 48434 74190 21077 29606 82055 81309 23626 83798 79519 66199 79828 55258 87161 09613 65617 80745 66159 24886 60889 81645 68541 72136 29208 46656 27913 14784 66791 55096 51543 10113 53858 62081 96875 83688 35955 77893 91454 53935 68199 60988 08540 47659 07358 97289 89834 25047 12891 84162 65878 96821 85380 87956 27903 99786 29449 39760 54675 34821 25675 01215 17082 73710 76462 70712 46753 21024 83678 15940 00875 05452 54353 7.

Using the numbers

Simply copying the decimal numbers from an electronic publication to a text file will typically result in a stream of bytes where each character (decimal digit or space) is encoded in one byte using the ASCII encoding. The particularity of these numbers is that when written in base 2, the resulting stream of bits can also be interpreted as the content of a gzip or executable file. Converting such big numbers to base 2 and writing the resulting stream of bits to a file is a nontrivial process. Below is the go source code of a program that takes a number on the command line and writes a binary representation to the standard output.

<syntaxhighlight lang=javascript> package main

import (. "os" . "strings" "fmt" "big")

func main() {

if len(Args) != 2 { fmt.Fprintf(Stderr, "Usage: %s <number>\n", Args[0]) Exit(1) }

number_str := Replace(Args[1], " ", "", -1) number, ok := big.NewInt(0).SetString(number_str, 0)

if !ok { fmt.Printf("Failed to convert \"%s\" to big int.\n", number_str) Exit(1) }

Stdout.Write(number.Bytes()) } </syntaxhighlight>

Given the appropriate numbers, this program will output the gzip and executable files described above.

References

[1] Prime glossary - Illegal prime (http://primes.utm.edu/glossary/page.php?sort=Illegal)

[2] DVD descrambler encoded in 'illegal' prime number (http://www.theregister.co.uk/2001/03/19/dvd_descrambler_encoded_in_illegal/) (Thomas C. Greene, *The Register*, Mon 19 March 2001)

[3] Prime Curios - first illegal prime (http://primes.utm.edu/curios/page.php?number_id=953)

[4] Prime Curios - first known non-trival executable prime (http://primes.utm.edu/curios/page.php?number_id=1214)

External links

- The first illegal prime (http://web.archive.org/web/20011212144451/fatphil.org/maths/illegal1.html)
- Phil Carmody's page discussing executable primes. (http://asdf.org/~fatphil/maths/illegal2.html)

Irregular prime

In number theory, a **regular prime** is a prime number $p > 2$ that does not divide the class number of the p-th cyclotomic field. Ernst Kummer (Kummer 1850) showed that an equivalent criterion for regularity is that p does not divide the numerator of any of the Bernoulli numbers B_k for $k = 2, 4, 6, \ldots, p - 3$. This is called **Kummer's criterion**. Kummer was able to prove that Fermat's last theorem holds true for regular prime exponents.

The first few regular primes are: 3, 5, 7, 11, 13, 17, 19, 23, 29, ... (sequence A007703 [1] in OEIS).

It has been conjectured that there are infinitely many regular primes. More precisely Siegel conjectured (1964) that $e^{-1/2}$, or about 61%, of all prime numbers are regular, in the asymptotic sense of natural density. Neither conjecture has been proven as of 2010.

An odd prime that is not regular is an **irregular prime**. The number of Bernoulli numbers B_k with a numerator divisible by p is called the **irregularity index** of p. K. L. Jensen has shown in 1915 that there are infinitely many irregular primes.

The first few irregular primes are: 37, 59, 67, 101, 103, 131, 149, ... (sequence A000928 [2] in OEIS)

References

- Kummer, E. E. (1850), "Allgemeiner Beweis des Fermat'schen Satzes, dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten (λ-3)/2 Bernoulli'schen Zahlen als Factoren nicht vorkommen" [3], *J. Reine Angew. Math.* **40**: 131–138.
- Keith Conrad, *Fermat's last theorem for regular primes* [4].
- Richard K. Guy, *Unsolved Problems in Number Theory* (3rd ed), Springer Verlag, 2004 ISBN 0-387-20860-7; section D2.
- Carl Ludwig Siegel, *Zu zwei Bemerkungen Kummers.* Nachr. Akad. d. Wiss. Goettingen, Math. Phys. K1., II, 1964, 51-62.

External links

- Chris Caldwell, The Prime Glossary: regular prime [5] at The Prime Pages.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa007703
[2] http://en.wikipedia.org/wiki/Oeis%3Aa000928
[3] http://www.digizeitschriften.de/resolveppn/GDZPPN002146738
[4] http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/fltreg.pdf
[5] http://primes.utm.edu/glossary/page.php?sort=Regular

Kynea number

A **Kynea number** is an integer of the form

$$4^n + 2^{n+1} - 1.$$

An equivalent formula is

$$(2^n + 1)^2 - 2.$$

This indicates that a Kynea number is the *n*th power of 4 plus the (*n* + 1)th Mersenne number. The first few Kynea numbers are

7, 23, 79, 287, 1087, 4223, 16639, 66047, 263167, 1050623, 4198399, 16785407 (sequence A093069 [1] in OEIS).

The binary representation of the *n*th Kynea number is a single leading one, followed by *n* - 1 consecutive zeroes, followed by *n* + 1 consecutive ones, or to put it algebraically:

$$4^n + \sum_{i=0}^{n} 2^i.$$

So, for example, 23 is 10111 in binary, 79 is 1001111, etc. The difference between the *n*th Kynea number and the *n*th Carol number is the (*n* + 2)th power of two.

Starting with 7, every third Kynea number is a multiple of 7. Thus, for a Kynea number to also be a prime number, its index *n* can not be of the form 3*x* + 1 for *x* > 0. The first few Kynea numbers that are also prime are 7, 23, 79, 1087, 66047, 263167, 16785407 (these are listed in Sloane's A091514 [2]). As of 2006, the largest known Kynea number that is also a prime is the Kynea number for *n* = 281621, approximately $5.455289117190661 \times 10^{169552}$. It was found by Cletus Emmanuel in November 2005, using k-Sieve from Phil Carmody and OpenPFGW. This is the 46th Kynea prime. Kynea numbers were studied by Cletus Emmanuel who named them after a baby girl.[3]

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa093069
[2] http://en.wikipedia.org/wiki/Oeis%3Aa091514
[3] (http://tech.groups.yahoo.com/group/primenumbers/message/14584)

External links

- Weisstein, Eric W., " Near-Square Prime (http://mathworld.wolfram.com/Near-SquarePrime.html)" from MathWorld.
- Prime Database entry for Kynea(281621) (http://primes.utm.edu/primes/page.php?id=75878)

Leyland number

In number theory, a **Leyland number** is a number of the form $x^y + y^x$, where x and y are integers greater than 1.[1] The first few Leyland numbers are

8, 17, 32, 54, 57, 100, 145, 177, 320, 368, 512, 593, 945, 1124 (sequence A076980 [2] in OEIS).

The requirement that x and y both be greater than 1 is important, since without it every positive integer would be a Leyland number of the form $x^1 + 1^x$. Also, because of the commutative property of addition, the condition $x \geq y$ is usually added to avoid double-covering the set of Leyland numbers (so we have $1 < y \leq x$).

The first prime Leyland numbers are

17, 593, 32993, 2097593, 8589935681, 59604644783353249, 523347633027360537213687137, 43143988327398957279342419750374600193 (A094133 [3])

corresponding to

3^2+2^3, 9^2+2^9, 15^2+2^{15}, 21^2+2^{21}, 33^2+2^{33}, 24^5+5^{24}, 56^3+3^{56}, $32^{15}+15^{32}$.[4]

As of June 2008, the largest Leyland number that has been proven to be prime is $2638^{4405} + 4405^{2638}$ with 15071 digits. From July 2004 to June 2006, it was the largest prime whose primality was proved by elliptic curve primality proving.[5] There are many larger known probable primes such as $91382^9 + 9^{91382}$,[6] but it is hard to prove primality of large Leyland numbers. Paul Leyland writes on his website: "More recently still, it was realized that numbers of this form are ideal test cases for general purpose primality proving programs. They have a simple algebraic description but no obvious cyclotomic properties which special purpose algorithms can exploit."

There is a project called XYYXF to factor composite Leyland numbers.[7]

References

[1] Richard Crandall and Carl Pomerance (2005), *Prime Numbers: A Computational Perspective*, Springer

[2] http://en.wikipedia.org/wiki/Oeis%3Aa076980

[3] http://en.wikipedia.org/wiki/Oeis%3Aa094133

[4] "Primes and Strong Pseudoprimes of the form $x^y + y^x$" (http://www.leyland.vispa.com/numth/primes/xyyx.htm). Paul Leyland. . Retrieved 2007-01-14.

[5] "Elliptic Curve Primality Proof" (http://primes.utm.edu/top20/page.php?id=27). Chris Caldwell. . Retrieved 2008-06-24.

[6] Henri Lifchitz & Renaud Lifchitz, PRP Top Records search (http://www.primenumbers.net/prptop/searchform.php?form=x^y+y^x&action=Search).

[7] "Factorizations of $x^y + y^x$ for $1 < y < x < 151$" (http://xyyxf.at.tut.by/default.html). Andrey Kulsha. . Retrieved 2008-06-24.

List of prime numbers

There are infinitely many prime numbers. Prime numbers may be generated with various formulas for primes. The first 500 primes are listed below, followed by lists of the first prime numbers of various types in alphabetical order.

The first 500 prime numbers

There are 20 consecutive primes in each of the 25 rows.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
1-20	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
21-40	73	79	83	89	97	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173
41-60	179	181	191	193	197	199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
61-80	283	293	307	311	313	317	331	337	347	349	353	359	367	373	379	383	389	397	401	409
81-100	419	421	431	433	439	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541
101-120	547	557	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
121-140	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	769	773	787	797	809
141-160	811	821	823	827	829	839	853	857	859	863	877	881	883	887	907	911	919	929	937	941
161-180	947	953	967	971	977	983	991	997	1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
181-200	1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
201-220	1229	1231	1237	1249	1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
221-240	1381	1399	1409	1423	1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
241-260	1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
261-280	1663	1667	1669	1693	1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
281-300	1823	1831	1847	1861	1867	1871	1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
301-320	1993	1997	1999	2003	2011	2017	2027	2029	2039	2053	2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
321-340	2131	2137	2141	2143	2153	2161	2179	2203	2207	2213	2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
341-360	2293	2297	2309	2311	2333	2339	2341	2347	2351	2357	2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
361-380	2437	2441	2447	2459	2467	2473	2477	2503	2521	2531	2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
381-400	2621	2633	2647	2657	2659	2663	2671	2677	2683	2687	2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
401-420	2749	2753	2767	2777	2789	2791	2797	2801	2803	2819	2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
421-440	2909	2917	2927	2939	2953	2957	2963	2969	2971	2999	3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
441-460	3083	3089	3109	3119	3121	3137	3163	3167	3169	3181	3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
461-480	3259	3271	3299	3301	3307	3313	3319	3323	3329	3331	3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
481-500	3433	3449	3457	3461	3463	3467	3469	3491	3499	3511	3517	3527	3529	3533	3539	3541	3547	3557	3559	3571

(sequence A000040 [1] in OEIS).

The Goldbach conjecture verification project reports that it has computed all primes below 10^{18}.[2] That means 24,739,954,287,740,860 primes, but they were not stored. There are known formulas to evaluate the prime-counting function (the number of primes below a given value) faster than computing the primes. This has been used to compute that there are 1,925,320,391,606,803,968,923 primes (roughly 2×10^{21}) below 10^{23}.

Lists of primes by type

Below are listed the first prime numbers of many named forms and types. More details are in the article for the name. *n* is a natural number (including 0) in the definitions. A prime number is a number that cannot be divided by a number other than 1 and itself.

Balanced primes

Primes which are the average of the previous prime and the following prime, meaning that the previous prime, the prime itself, and the following prime are in arithmetic progression.

5, 53, 157, 173, 211, 257, 263, 373, 563, 593, 607, 653, 733, 947, 977, 1103, 1123, 1187, 1223, 1367, 1511, 1747, 1753, 1907, 2287, 2417, 2677, 2903, 2963, 3307, 3313, 3637, 3733, 4013, 4409, 4457, 4597, 4657, 4691, 4993, 5107, 5113, 5303, 5387, 5393 (A006562 [1])

Bell number primes

Primes that are the number of partitions of a set with *n* members.

2, 5, 877, 27644437, 35742549198872617291353508656626642567, 359334085968622831041960188598043661065388726959079837. The next term has 6539 digits. (A051131 [3])

Carol primes

Of the form $(2^n - 1)^2 - 2$.

7, 47, 223, 3967, 16127, 1046527, 16769023, 1073676287, 68718952447, 274876858367, 4398042316799, 1125899839733759, 18014398241046527, 1298074214633706835075030044377087 (A091516 [4])

Centered decagonal primes

Of the form $5(n^2 - n) + 1$.

11, 31, 61, 101, 151, 211, 281, 661, 911, 1051, 1201, 1361, 1531, 1901, 2311, 2531, 3001, 3251, 3511, 4651, 5281, 6301, 6661, 7411, 9461, 9901, 12251, 13781, 14851, 15401, 18301, 18911, 19531, 20161, 22111, 24151, 24851, 25561, 27011, 27751 (A090562 [4])

Centered heptagonal primes

Of the form $(7n^2 - 7n + 2) / 2$.

43, 71, 197, 463, 547, 953, 1471, 1933, 2647, 2843, 3697, 4663, 5741, 8233, 9283, 10781, 11173, 12391, 14561, 18397, 20483, 29303, 29947, 34651, 37493, 41203, 46691, 50821, 54251, 56897, 57793, 65213, 68111, 72073, 76147, 84631, 89041, 93563 (primes in A069099 [1])

Centered square primes

Of the form $n^2 + (n+1)^2$.

5, 13, 41, 61, 113, 181, 313, 421, 613, 761, 1013, 1201, 1301, 1741, 1861, 2113, 2381, 2521, 3121, 3613, 4513, 5101, 7321, 8581, 9661, 9941, 10513, 12641, 13613, 14281, 14621, 15313, 16381, 19013, 19801, 20201, 21013, 21841, 23981, 24421, 26681 (A027862 [2])

Centered triangular primes

Of the form $(3n^2 + 3n + 2) / 2$.

19, 31, 109, 199, 409, 571, 631, 829, 1489, 1999, 2341, 2971, 3529, 4621, 4789, 7039, 7669, 8779, 9721, 10459, 10711, 13681, 14851, 16069, 16381, 17659, 20011, 20359, 23251, 25939, 27541, 29191, 29611, 31321, 34429, 36739, 40099, 40591, 42589 (A125602 [2])

Chen primes

p is prime and $p + 2$ is either a prime or semiprime.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, 53, 59, 67, 71, 83, 89, 101, 107, 109, 113, 127, 131, 137, 139, 149, 157, 167, 179, 181, 191, 197, 199, 211, 227, 233, 239, 251, 257, 263, 269, 281, 293, 307, 311, 317, 337, 347, 353, 359, 379, 389, 401, 409 (A109611 [1])

Circular primes

A circular prime number is a number that remains prime on any cyclic rotation of its digits (in base 10).

2, 3, 5, 7, 11, 13, 17, 31, 37, 71, 73, 79, 97, 113, 131, 197, 199, 311, 337, 373, 719, 733, 919, 971, 991, 1193, 1931, 3119, 3779, 7793, 7937, 9311, 9377, 11939, 19391, 19937, 37199, 39119, 71993, 91193, 93719, 93911, 99371, 193939, 199933, 319993, 331999, 391939, 393919, 919393, 933199, 939193, 939391, 993319, 999331 (A068652 [5])

Some sources only list the smallest prime in each cycle, for example listing 13 but omitting 31:

2, 3, 5, 7, 11, 13, 17, 37, 79, 113, 197, 199, 337, 1193, 3779, 11939, 19937, 193939, 199933, 1111111111111111, 11111111111111111111 (A016114 [6])

All repunit primes are circular.

Cousin primes

(p, $p + 4$) are both prime.

(3, 7), (7, 11), (13, 17), (19, 23), (37, 41), (43, 47), (67, 71), (79, 83), (97, 101), (103, 107), (109, 113), (127, 131), (163, 167), (193, 197), (223, 227), (229, 233), (277, 281) (A023200 [1], A046132 [2])

Cuban primes

Of the form $\frac{x^3-y^3}{x-y},\ x = y + 1$

7, 19, 37, 61, 127, 271, 331, 397, 547, 631, 919, 1657, 1801, 1951, 2269, 2437, 2791, 3169, 3571, 4219, 4447, 5167, 5419, 6211, 7057, 7351, 8269, 9241, 10267, 11719, 12097, 13267, 13669, 16651, 19441, 19927, 22447, 23497, 24571, 25117, 26227, 27361, 33391, 35317 (A002407 [1])

Of the form $\frac{x^3-y^3}{x-y},\ x = y + 2$

13, 109, 193, 433, 769, 1201, 1453, 2029, 3469, 3889, 4801, 10093, 12289, 13873, 18253, 20173, 21169, 22189, 28813, 37633, 43201, 47629, 60493, 63949, 65713, 69313, 73009, 76801, 84673, 106033, 108301, 112909, 115249 (A002648 [3])

Cullen primes

Of the form $n \cdot 2^n + 1$.

3, 393050634124102232869567034555427371542904833 (A050920 [7])

Dihedral primes

Primes that remain prime when read upside down or mirrored in a seven-segment display.

2, 5, 11, 101, 181, 1181, 1811, 18181, 108881, 110881, 118081, 120121, 121021, 121151, 150151, 151051, 151121, 180181, 180811, 181081 (A134996 [8])

Double factorial primes

Of the form $n!! + 1$. Values of *n*:

1, 2, 518, 33416, 37310, 52608 (A080778 [9])

Note that $n = 0$ and $n = 1$ produce the same prime, namely 2.

Of the form $n!! - 1$. Values of *n*:

3, 4, 6, 8, 16, 26, 64, 82, 90, 118, 194, 214, 728, 842, 888, 2328, 3326, 6404, 8670, 9682, 27056, 44318 (A007749 [10])

Double Mersenne primes

Of the form $2^{(2^p-1)} - 1$ for prime *p*.

7, 127, 2147483647, 170141183460469231731687303715884105727 (primes in A077586 [2])

As of January 2008, these are the only known double Mersenne primes (subset of Mersenne primes.)

Eisenstein primes without imaginary part

Eisenstein integers that are irreducible and real numbers (primes of form $3n - 1$).

2, 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101, 107, 113, 131, 137, 149, 167, 173, 179, 191, 197, 227, 233, 239, 251, 257, 263, 269, 281, 293, 311, 317, 347, 353, 359, 383, 389, 401 (A003627 [1])

Emirps

Primes which become a different prime when their decimal digits are reversed.

13, 17, 31, 37, 71, 73, 79, 97, 107, 113, 149, 157, 167, 179, 199, 311, 337, 347, 359, 389, 701, 709, 733, 739, 743, 751, 761, 769, 907, 937, 941, 953, 967, 971, 983, 991 (A006567 [2])

Euclid primes

Of the form $p_n\# + 1$ (a subset of primorial primes).

3, 7, 31, 211, 2311, 200560490131 (A018239 [11][12])

Even prime

Of the form $2n$; n = 1, 2, 3, 4, ...

2

The only even prime is 2.
2 is therefore sometimes called "the oddest prime" as a pun on the non-mathematical meaning of "odd".[13]

Factorial primes

Of the form $n! - 1$ or $n! + 1$.

2, 3, 5, 7,11, 23, 719, 5039, 39916801, 479001599, 87178291199, 10888869450418352160768000001, 265252859812191058636308479999999, 263130836933693530167218012159999999, 8683317618811886495518194401279999999 (A088054 [1])

Fermat primes

Of the form $2^{2^n} + 1$.

3, 5, 17, 257, 65537 (A019434 [14])

As of April 2009 these are the only known Fermat primes.

Fibonacci primes

Primes in the Fibonacci sequence $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$.

2, 3, 5, 13, 89, 233, 1597, 28657, 514229, 433494437, 2971215073, 99194853094755497, 106634041749171059581457216 9, 191347024000932780814494239 17 (A005478 [1])

Fortunate primes

Fortunate numbers that are prime (it has been conjectured they all are).

3, 5, 7, 13, 17, 19, 23, 37, 47, 59, 61, 67, 71, 79, 89, 101, 103, 107, 109, 127, 151, 157, 163, 167, 191, 197, 199, 223, 229, 233, 239, 271, 277, 283, 293, 307, 311, 313, 331, 353, 373, 379, 383, 397 (A046066 [2])

Gaussian primes

Prime elements of the Gaussian integers (primes of form $4n + 3$).

3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163, 167, 179, 191, 199, 211, 223, 227, 239, 251, 263, 271, 283, 307, 311, 331, 347, 359, 367, 379, 383, 419, 431, 439, 443, 463, 467, 479, 487, 491, 499, 503 (A002145 [3])

Genocchi number primes

17

The only positive prime Genocchi number is 17.[15]

Good primes

Primes p_n for which $p_n^2 > p_{n-i} \times p_{n+i}$ for all $1 \le i \le n-1$, where p_n is the nth prime.

5, 11, 17, 29, 37, 41, 53, 59, 67, 71, 97, 101, 127, 149, 179, 191, 223, 227, 251, 257, 269, 307 (A028388 [2])

Happy primes

Happy numbers that are prime.

7, 13, 19, 23, 31, 79, 97, 103, 109, 139, 167, 193, 239, 263, 293, 313, 331, 367, 379, 383, 397, 409, 487, 563, 617, 653, 673, 683, 709, 739, 761, 863, 881, 907, 937, 1009, 1033, 1039, 1093 (A035497 [3])

Higgs primes for squares

Primes p for which $p - 1$ divides the square of the product of all earlier terms.

2, 3, 5, 7, 11, 13, 19, 23, 29, 31, 37, 43, 47, 53, 59, 61, 67, 71, 79, 101, 107, 127, 131, 139, 149, 151, 157, 173, 181, 191, 197, 199, 211, 223, 229, 263, 269, 277, 283, 311, 317, 331, 347, 349 (A007459 [1])

Highly cototient number primes

Primes that are a cototient more often than any integer below it except 1.

2, 23, 47, 59, 83, 89, 113, 167, 269, 389, 419, 509, 659, 839, 1049, 1259, 1889 (A105440 [2])

Irregular primes

Odd primes p which divide the class number of the p-th cyclotomic field.

37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283, 293, 307, 311, 347, 353, 379, 389, 401, 409, 421, 433, 461, 463, 467, 491, 523, 541, 547, 557, 577, 587, 593, 607, 613, 617, 619 (A000928 [2])

Kynea primes

Of the form $(2^n + 1)^2 - 2$.

7, 23, 79, 1087, 66047, 263167, 16785407, 1073807359, 17180131327, 68720001023, 4398050705407, 70368760954879, 18014398777917439, 18446744082299486207 (A091514 [2])

Left-truncatable primes

Primes that remain prime when the leading decimal digit is successively removed.

2, 3, 5, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 113, 137, 167, 173, 197, 223, 283, 313, 317, 337, 347, 353, 367, 373, 383, 397, 443, 467, 523, 547, 613, 617, 643, 647, 653, 673, 683 (A024785 [16])

Leyland primes

Of the form $x^y + y^x$ with $1 < x \le y$.

17, 593, 32993, 2097593, 8589935681, 59604644783353249, 523347633027360537213687137, 43143988327398957279342419750374600193 (A094133 [3])

Long primes

Primes p for which, in a given base b, $\frac{b^{p-1}-1}{p}$ gives a cyclic number. They are also called full reptend primes.

Primes p for base 10:
7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, 223, 229, 233, 257, 263, 269, 313, 337, 367, 379, 383, 389, 419, 433, 461, 487, 491, 499, 503, 509, 541, 571, 577, 593 (A001913 [1])

Lucas primes

Primes in the Lucas number sequence $L_0 = 2$, $L_1 = 1$, $L_n = L_{n-1} + L_{n-2}$.
2,[17] 3, 7, 11, 29, 47, 199, 521, 2207, 3571, 9349, 3010349, 54018521, 370248451, 6643838879, 119218851371, 5600748293801, 688846502588399, 32361122672259149 (A005479 [18])

Lucky primes

Lucky numbers that are prime.

3, 7, 13, 31, 37, 43, 67, 73, 79, 127, 151, 163, 193, 211, 223, 241, 283, 307, 331, 349, 367, 409, 421, 433, 463, 487, 541, 577, 601, 613, 619, 631, 643, 673, 727, 739, 769, 787, 823, 883, 937, 991, 997 (A031157 [19])

Markov primes

Primes p for which there exist integers x and y such that $x^2 + y^2 + p^2 = 3xyp$.
2, 5, 13, 29, 89, 233, 433, 1597, 2897, 5741, 7561, 28657, 33461, 43261, 96557, 426389, 514229, 1686049, 2922509, 3276509, 94418953, 321534781, 433494437, 780291637, 1405695061, 2971215073, 19577194573, 25209506681 (primes in A002559 [20])

Mersenne primes

Of the form $2^n - 1$.

3, 7, 31, 127, 8191, 131071, 524287, 2147483647, 2305843009213693951, 618970019642690137449562111, 162259276829213363391578010288127, 170141183460469231731687303715884105727 (A000668 [21])

As of June 2009, there are 47 known Mersenne primes (The 47th discovered is actually the 46th in size). The 13th, 14th, and 47th (based upon size), respectively, have 157, 183, and 12,978,189 digits.

Mills primes

Of the form $\lfloor \theta^{3^n} \rfloor$, where θ is Mills' constant. This form is prime for all positive integers n.
2, 11, 1361, 2521008887, 16022236204009818131831320183 (A051254 [22])

Minimal primes

Primes for which there is no shorter sub-sequence of the decimal digits that form a prime. There are exactly 26 minimal primes:

2, 3, 5, 7, 11, 19, 41, 61, 89, 409, 449, 499, 881, 991, 6469, 6949, 9001, 9049, 9649, 9949, 60649, 666649, 946669, 60000049, 66000049, 66600049 (A071062 [23])

Motzkin primes

Primes that are the number of different ways of drawing non-intersecting chords on a circle between *n* points.

2, 127, 15511, 953467954114363 (A092832 [24])

Newman–Shanks–Williams primes

Newman–Shanks–Williams numbers that are prime.

7, 41, 239, 9369319, 63018038201, 489133282872437279, 1917500294268803292859 (A088165 [25])

Odd primes

Of the form 2*n* - 1.

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199... (A065091 [1])

All prime numbers except the prime 2 are odd.

Padovan primes

Primes in the Padovan sequence $P(0) = P(1) = P(2) = 1, P(n) = P(n-2) + P(n-3)$.

2, 3, 5, 7, 37, 151, 3329, 23833, 13091204281, 3093215881333057, 1363005552434666078217421284621279933627102780881053358473 (A100891 [26])

Palindromic primes

Primes that remain the same when their decimal digits are read backwards.

2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929, 10301, 10501, 10601, 11311, 11411, 12421, 12721, 12821, 13331, 13831, 13931, 14341, 14741 (A002385 [27])

Partition primes

Partition numbers that are prime.

2, 3, 5, 7, 11, 101, 17977, 10619863, 6620830889, 80630964769, 228204732751, 1171432692373, 1398341745571, 10963707205259, 15285151248481, 10657331232548839, 790738119649411319, 18987964267331664557 (A049575 [28])

Pell primes

Primes in the Pell number sequence $P_0 = 0$, $P_1 = 1$, $P_n = 2P_{n-1} + P_{n-2}$.

2, 5, 29, 5741, 33461, 44560482149, 1746860020068409, 68480406462161287469, 13558774610046711780701, 41256368885625488682215597974614 49 (A086383 [29])

Permutable primes

Any permutation of the decimal digits is a prime.

2, 3, 5, 7, 11, 13, 17, 31, 37, 71, 73, 79, 97, 113, 131, 199, 311, 337, 373, 733, 919, 991, 1111111111111111111, 11111111111111111111111 (A003459 [30])

It seems likely that all further permutable primes are repunits, i.e. contain only the digit 1.

Perrin primes

Primes in the Perrin number sequence $P(0) = 3$, $P(1) = 0$, $P(2) = 2$, $P(n) = P(n - 2) + P(n - 3)$.

2, 3, 5, 7, 17, 29, 277, 367, 853, 14197, 43721, 1442968193, 792606555396977, 18727865918041723432 1, 6624116048878014107157986479 7 (A074788 [31])

Pierpont primes

Of the form $2^u 3^v + 1$ for some integers $u,v \geq 0$.

These are also class 1- primes.

2, 3, 5, 7, 13, 17, 19, 37, 73, 97, 109, 163, 193, 257, 433, 487, 577, 769, 1153, 1297, 1459, 2593, 2917, 3457, 3889, 10369, 12289, 17497, 18433, 39367, 52489, 65537, 139969, 147457 (A005109 [32])

Pillai primes

Primes p for which there exist $n > 0$ such that p divides $n! + 1$ and n does not divide $p - 1$.

23, 29, 59, 61, 67, 71, 79, 83, 109, 137, 139, 149, 193, 227, 233, 239, 251, 257, 269, 271, 277, 293, 307, 311, 317, 359, 379, 383, 389, 397, 401, 419, 431, 449, 461, 463, 467, 479, 499 (A063980 [33])

Primeval primes

Primes for which there are more prime permutations of some or all the decimal digits than for any smaller number.

2, 13, 37, 107, 113, 137, 1013, 1237, 1367, 10079 (A119535 [34])

Primorial primes

Of the form $p_n\# - 1$ or $p_n\# + 1$.

3, 5, 7, 29, 31, 211, 2309, 2311, 30029, 200560490131, 304250263527209, 23768741896345550770650537601358309 (union of A057705 [35] and A018239 [11][12])

Proth primes

Of the form $k \cdot 2^n + 1$ with odd k and $k < 2^n$.

3, 5, 13, 17, 41, 97, 113, 193, 241, 257, 353, 449, 577, 641, 673, 769, 929, 1153, 1217, 1409, 1601, 2113, 2689, 2753, 3137, 3329, 3457, 4481, 4993, 6529, 7297, 7681, 7937, 9473, 9601, 9857 (A080076 [36])

Pythagorean primes

Of the form $4n + 1$.

5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197, 229, 233, 241, 257, 269, 277, 281, 293, 313, 317, 337, 349, 353, 373, 389, 397, 401, 409, 421, 433, 449 (A002144 [2])

Prime quadruplets

(p, p+2, p+6, p+8) are all prime.

(5, 7, 11, 13), (11, 13, 17, 19), (101, 103, 107, 109), (191, 193, 197, 199), (821, 823, 827, 829), (1481, 1483, 1487, 1489), (1871, 1873, 1877, 1879), (2081, 2083, 2087, 2089), (3251, 3253, 3257, 3259), (3461, 3463, 3467, 3469), (5651, 5653, 5657, 5659), (9431, 9433, 9437, 9439) (A007530 [37], A136720 [38], A136721 [39], A090258 [40])

Ramanujan primes

Integers R_n that are the smallest to give at least n primes from $x/2$ to x for all $x \geq R_n$ (all such integers are primes).

2, 11, 17, 29, 41, 47, 59, 67, 71, 97, 101, 107, 127, 149, 151, 167, 179, 181, 227, 229, 233, 239, 241, 263, 269, 281, 307, 311, 347, 349, 367, 373, 401, 409, 419, 431, 433, 439, 461, 487, 491 (A104272 [41])

Regular primes

Primes p which do not divide the class number of the p-th cyclotomic field.

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 43, 47, 53, 61, 71, 73, 79, 83, 89, 97, 107, 109, 113, 127, 137, 139, 151, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 239, 241, 251, 269, 277, 281 (A007703 [1])

Repunit primes

Primes containing only the decimal digit 1.

11, 1111111111111111111, 11111111111111111111111 (A004022 [42])

The next have 317 and 1031 digits.

Primes in residue classes

Of form $a \cdot n + d$ for fixed a and d. Also called primes congruent to d modulo a.

Three cases have their own entry: 2n+1 are the odd primes, 4n+1 are Pythagorean primes, 4n+3 are the integer Gaussian primes.

2n+1: 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53 (A065091 [1])
4n+1: 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137 (A002144 [2])
4n+3: 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107 (A002145 [3])
6n+1: 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109, 127, 139 (A002476 [4])
6n+5: 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101, 107, 113 (A007528 [5])
8n+1: 17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 257, 281, 313, 337, 353 (A007519 [6])
8n+3: 3, 11, 19, 43, 59, 67, 83, 107, 131, 139, 163, 179, 211, 227, 251 (A007520 [7])
8n+5: 5, 13, 29, 37, 53, 61, 101, 109, 149, 157, 173, 181, 197, 229, 269 (A007521 [8])
8n+7: 7, 23, 31, 47, 71, 79, 103, 127, 151, 167, 191, 199, 223, 239, 263 (A007522 [9])
10n+1: 11, 31, 41, 61, 71, 101, 131, 151, 181, 191, 211, 241, 251, 271, 281 (A030430 [10])
10n+3: 3, 13, 23, 43, 53, 73, 83, 103, 113, 163, 173, 193, 223, 233, 263 (A030431 [11])
10n+7: 7, 17, 37, 47, 67, 97, 107, 127, 137, 157, 167, 197, 227, 257, 277 (A030432 [12])
10n+9: 19, 29, 59, 79, 89, 109, 139, 149, 179, 199, 229, 239, 269, 349, 359 (A030433 [13])
...

10n+d (d = 1, 3, 7, 9) are primes ending in the decimal digit d.

Right-truncatable primes

Primes that remain prime when the last decimal digit is successively removed.

2, 3, 5, 7, 23, 29, 31, 37, 53, 59, 71, 73, 79, 233, 239, 293, 311, 313, 317, 373, 379, 593, 599, 719, 733, 739, 797, 2333, 2339, 2393, 2399, 2939, 3119, 3137, 3733, 3739, 3793, 3797 (A024770 [43])

Safe primes

p and $(p-1) / 2$ are both prime.

5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467, 479, 503, 563, 587, 719, 839, 863, 887, 983, 1019, 1187, 1283, 1307, 1319, 1367, 1439, 1487, 1523, 1619, 1823, 1907 (A005385 [44])

Self primes in base 10

Primes that cannot be generated by any integer added to the sum of its decimal digits.

3, 5, 7, 31, 53, 97, 211, 233, 277, 367, 389, 457, 479, 547, 569, 613, 659, 727, 839, 883, 929, 1021, 1087, 1109, 1223, 1289, 1447, 1559, 1627, 1693, 1783, 1873 (A006378 [45])

Sexy primes

$(p, p + 6)$ are both prime.

(5, 11), (7, 13), (11, 17), (13, 19), (17, 23), (23, 29), (31, 37), (37, 43), (41, 47), (47, 53), (53, 59), (61, 67), (67, 73), (73, 79), (83, 89), (97, 103), (101, 107), (103, 109), (107, 113), (131, 137), (151, 157), (157, 163), (167, 173), (173, 179), (191, 197), (193, 199) (A023201 [46], A046117 [47])

Smarandache–Wellin primes

Primes which are the concatenation of the first n primes written in decimal.

2, 23, 2357 (A069151 [48])

The fourth Smarandache-Wellin prime is the 355-digit concatenation of the first 128 primes which end with 719.

Solinas primes

Of the form $2^a \pm 2^b \pm 1$, where $0 < b < a$.

3, 5, 7, 11, 13 (A165255 [49])

Sophie Germain primes

p and $2p + 1$ are both prime.

2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359, 419, 431, 443, 454, 491, 509, 593, 641, 653, 659, 683, 719, 743, 761, 809, 911, 953 (A005384 [50])

Star primes

Of the form $6n(n - 1) + 1$.

13, 37, 73, 181, 337, 433, 541, 661, 937, 1093, 2053, 2281, 2521, 3037, 3313, 5581, 5953, 6337, 6733, 7561, 7993, 8893, 10333, 10837, 11353, 12421, 12973, 13537, 15913, 18481 (A083577 [51])

Stern primes

Primes that are not the sum of a smaller prime and twice the square of a nonzero integer.

2, 3, 17, 137, 227, 977, 1187, 1493 (A042978 [52])

As of January 2008, these are the only known Stern primes, and possibly the only existing.

Super-primes

Primes with a prime index in the sequence of prime numbers (the 2nd, 3rd, 5th, ... prime).

3, 5, 11, 17, 31, 41, 59, 67, 83, 109, 127, 157, 179, 191, 211, 241, 277, 283, 331, 353, 367, 401, 431, 461, 509, 547, 563, 587, 599, 617, 709, 739, 773, 797, 859, 877, 919, 967, 991 (A006450 [53])

Supersingular primes

There are exactly fifteen supersingular primes:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71 (A002267 [54])

Thabit number primes

Of the form $3 \cdot 2^n - 1$.

2, 5, 11, 23, 47, 191, 383, 6143, 786431, 51539607551, 824633720831, 26388279066623, 108086391056891903, 55340232221128654847, 226673591177742970257407 (A007505 [55])

Prime triplets

(p, p+2, p+6) or (p, p+4, p+6) are all prime.

(5, 7, 11), (7, 11, 13), (11, 13, 17), (13, 17, 19), (17, 19, 23), (37, 41, 43), (41, 43, 47), (67, 71, 73), (97, 101, 103), (101, 103, 107), (103, 107, 109), (107, 109, 113), (191, 193, 197), (193, 197, 199), (223, 227, 229), (227, 229, 233), (277, 281, 283), (307, 311, 313), (311, 313, 317), (347, 349, 353) (A007529 [56], A098414 [57], A098415 [58])

Twin primes

(p, p + 2) are both prime.

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), (227, 229), (239, 241), (269, 271), (281, 283), (311, 313), (347, 349), (419, 421), (431, 433), (461, 463) (A001359 [59], A006512 [60])

Two-sided primes

Primes which are both left-truncatable and right-truncatable. There are exactly fifteen two-sided primes:

2, 3, 5, 7, 23, 37, 53, 73, 313, 317, 373, 797, 3137, 3797, 739397 (A020994 [61])

Ulam number primes

Ulam numbers that are prime.

2, 3, 11, 13, 47, 53, 97, 131, 197, 241, 409, 431, 607, 673, 739, 751, 983, 991, 1103, 1433, 1489, 1531, 1553, 1709, 1721, 2371, 2393, 2447, 2633, 2789, 2833, 2897 (A068820 [62])

Unique primes

Primes p for which the period length of $1/p$ is unique (no other prime gives the same).

3, 11, 37, 101, 9091, 9901, 333667, 909091, 99990001, 999999000001, 9999999900000001, 909090909090909091, 1111111111111111, 11111111111111111111, 900900900900990990990991 (A040017 [63])

Wagstaff primes

Of the form $(2^n + 1) / 3$.

3, 11, 43, 683, 2731, 43691, 174763, 2796203, 715827883, 2932031007403, 768614336404564651, 201487636602438195784363, 845100400152152934331135470251, 56713727820156410577229101238628035243 (A000979 [64])

n values:

3, 5, 7, 11, 13, 17, 19, 23, 31, 43, 61, 79, 101, 127, 167, 191, 199, 313, 347, 701, 1709, 2617, 3539, 5807, 10501, 10691, 11279, 12391, 14479, 42737, 83339, 95369, 117239, 127031, 138937, 141079, 267017, 269987, 374321 (A000978 [65])

Wall-Sun-Sun primes

A prime $p > 5$ is called a Wall-Sun-Sun prime if p^2 divides the Fibonacci number $F_{p-\left(\frac{p}{5}\right)}$, where the Legendre symbol $\left(\frac{p}{5}\right)$ is defined as

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5 \\ -1 & \text{if } p \equiv \pm 2 \pmod 5 \end{cases}$$

As of February 2010, no Wall-Sun-Sun primes are known.

Wedderburn-Etherington number primes

Wedderburn-Etherington numbers that are prime.

2, 3, 11, 23, 983, 2179, 24631, 3626149, 253450711, 596572387 (primes in A001190 [66])

Wieferich primes

Primes p for which p^2 divides $2^{p-1} - 1$

1093, 3511 (A001220 [67])

As of January 2008, these are the only known Wieferich primes.

Wilson primes

Primes p for which p^2 divides $(p - 1)! + 1$

5, 13, 563 (A007540 [68])

As of January 2008, these are the only known Wilson primes.

Wolstenholme primes

Primes p for which the binomial coefficient $\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$.

16843, 2124679 (A088164 [69])

As of January 2008, these are the only known Wolstenholme primes.

Woodall primes

Of the form $n \cdot 2^n - 1$.

7, 23, 383, 32212254719, 2833419889721787128217599, 1958459827775699263024005 11, 47769131098520414182480566228824883 19 (A050918 [70])

See also

- Illegal prime
- Largest known prime
- List of numbers
- Prime gap
- Probable prime
- Pseudoprime
- Strobogrammatic prime
- Strong prime
- Wall-Sun-Sun prime
- Wieferich pair

Notes

[1] http://en.wikipedia.org/wiki/Oeis%3Aa000040
[2] Tomás Oliveira e Silva, Goldbach conjecture verification (http://www.ieeta.pt/~tos/goldbach.html).
[3] http://en.wikipedia.org/wiki/Oeis%3Aa051131
[4] http://en.wikipedia.org/wiki/Oeis%3Aa090562
[5] http://en.wikipedia.org/wiki/Oeis%3Aa068652
[6] http://en.wikipedia.org/wiki/Oeis%3Aa016114
[7] http://en.wikipedia.org/wiki/Oeis%3Aa050920
[8] http://en.wikipedia.org/wiki/Oeis%3Aa134996
[9] http://en.wikipedia.org/wiki/Oeis%3Aa080778
[10] http://en.wikipedia.org/wiki/Oeis%3Aa007749
[11] http://en.wikipedia.org/wiki/Oeis%3Aa018239
[12] A018239 (http://en.wikipedia.org/wiki/Oeis:a018239) includes 2 = empty product of first 0 primes plus 1, but 2 is excluded in this list.
[13] http://mathworld.wolfram.com/OddPrime.html
[14] http://en.wikipedia.org/wiki/Oeis%3Aa019434
[15] Weisstein, Eric W., " Genocchi Number (http://mathworld.wolfram.com/GenocchiNumber.html)" from MathWorld.
[16] http://en.wikipedia.org/wiki/Oeis%3Aa024785
[17] It varies whether $L_0 = 2$ is included in the Lucas numbers.
[18] http://en.wikipedia.org/wiki/Oeis%3Aa005479
[19] http://en.wikipedia.org/wiki/Oeis%3Aa031157
[20] http://en.wikipedia.org/wiki/Oeis%3Aa002559
[21] http://en.wikipedia.org/wiki/Oeis%3Aa000668
[22] http://en.wikipedia.org/wiki/Oeis%3Aa051254
[23] http://en.wikipedia.org/wiki/Oeis%3Aa071062
[24] http://en.wikipedia.org/wiki/Oeis%3Aa092832
[25] http://en.wikipedia.org/wiki/Oeis%3Aa088165
[26] http://en.wikipedia.org/wiki/Oeis%3Aa100891
[27] http://en.wikipedia.org/wiki/Oeis%3Aa002385
[28] http://en.wikipedia.org/wiki/Oeis%3Aa049575
[29] http://en.wikipedia.org/wiki/Oeis%3Aa086383
[30] http://en.wikipedia.org/wiki/Oeis%3Aa003459
[31] http://en.wikipedia.org/wiki/Oeis%3Aa074788
[32] http://en.wikipedia.org/wiki/Oeis%3Aa005109
[33] http://en.wikipedia.org/wiki/Oeis%3Aa063980
[34] http://en.wikipedia.org/wiki/Oeis%3Aa119535
[35] http://en.wikipedia.org/wiki/Oeis%3Aa057705

[36] http://en.wikipedia.org/wiki/Oeis%3Aa080076
[37] http://en.wikipedia.org/wiki/Oeis%3Aa007530
[38] http://en.wikipedia.org/wiki/Oeis%3Aa136720
[39] http://en.wikipedia.org/wiki/Oeis%3Aa136721
[40] http://en.wikipedia.org/wiki/Oeis%3Aa090258
[41] http://en.wikipedia.org/wiki/Oeis%3Aa104272
[42] http://en.wikipedia.org/wiki/Oeis%3Aa004022
[43] http://en.wikipedia.org/wiki/Oeis%3Aa024770
[44] http://en.wikipedia.org/wiki/Oeis%3Aa005385
[45] http://en.wikipedia.org/wiki/Oeis%3Aa006378
[46] http://en.wikipedia.org/wiki/Oeis%3Aa023201
[47] http://en.wikipedia.org/wiki/Oeis%3Aa046117
[48] http://en.wikipedia.org/wiki/Oeis%3Aa069151
[49] http://en.wikipedia.org/wiki/Oeis%3Aa165255
[50] http://en.wikipedia.org/wiki/Oeis%3Aa005384
[51] http://en.wikipedia.org/wiki/Oeis%3Aa083577
[52] http://en.wikipedia.org/wiki/Oeis%3Aa042978
[53] http://en.wikipedia.org/wiki/Oeis%3Aa006450
[54] http://en.wikipedia.org/wiki/Oeis%3Aa002267
[55] http://en.wikipedia.org/wiki/Oeis%3Aa007505
[56] http://en.wikipedia.org/wiki/Oeis%3Aa007529
[57] http://en.wikipedia.org/wiki/Oeis%3Aa098414
[58] http://en.wikipedia.org/wiki/Oeis%3Aa098415
[59] http://en.wikipedia.org/wiki/Oeis%3Aa001359
[60] http://en.wikipedia.org/wiki/Oeis%3Aa006512
[61] http://en.wikipedia.org/wiki/Oeis%3Aa020994
[62] http://en.wikipedia.org/wiki/Oeis%3Aa068820
[63] http://en.wikipedia.org/wiki/Oeis%3Aa040017
[64] http://en.wikipedia.org/wiki/Oeis%3Aa000979
[65] http://en.wikipedia.org/wiki/Oeis%3Aa000978
[66] http://en.wikipedia.org/wiki/Oeis%3Aa001190
[67] http://en.wikipedia.org/wiki/Oeis%3Aa001220
[68] http://en.wikipedia.org/wiki/Oeis%3Aa007540
[69] http://en.wikipedia.org/wiki/Oeis%3Aa088164
[70] http://en.wikipedia.org/wiki/Oeis%3Aa050918

External links

- Lists of Primes (http://primes.utm.edu/lists/) at the Prime Pages.
- Interface to a list of the first 98 million primes (http://www.rsok.com/~jrm/printprimes.html) (primes less than 2,000,000,000)
- Weisstein, Eric W., " Prime Number Sequences (http://mathworld.wolfram.com/topics/PrimeNumberSequences.html)" from MathWorld.
- Selected prime related sequences (http://www.research.att.com/~njas/sequences/Sindx_Pri.html) in OEIS.

Lucas number

The **Lucas numbers** are an integer sequence named after the mathematician François Édouard Anatole Lucas (1842–1891), who studied both that sequence and the closely related Fibonacci numbers. Lucas numbers and Fibonacci numbers form complementary instances of Lucas sequences.

Definition

Like the Fibonacci numbers, each Lucas number is defined to be the sum of its two immediate previous terms, i.e. it is *a* Fibonacci integer sequence. Consequently, the ratio between two consecutive Lucas numbers converges to the golden ratio. However, the first two Lucas numbers are $L_0 = 2$ and $L_1 = 1$ instead of 0 and 1, and the properties of Lucas numbers are therefore somewhat different from those of Fibonacci numbers.

A Lucas number may thus be defined as follows:

$$L_n := \begin{cases} 2 & \text{if } n = 0; \\ 1 & \text{if } n = 1; \\ L_{n-1} + L_{n-2} & \text{if } n > 1. \end{cases}$$

The sequence of Lucas numbers begins:

2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, ... (sequence A000032 [1] in OEIS)

Extension to negative integers

Using $L_{n-2} = L_n - L_{n-1}$, one can extend the Lucas numbers to negative integers to obtain a doubly infinite sequence :

..., -11, 7, -4, 3, -1, 2, 1, 3, 4, 7, 11, ... (terms L_n for $-5 \leq n \leq 5$ are shown).

The formula for terms with negative indices in this sequence is

$$L_{-n} = (-1)^n L_n.$$

Relationship to Fibonacci numbers

The Lucas numbers are related to the Fibonacci numbers by the identities

- $L_n = F_{n-1} + F_{n+1}$
- $L_n^2 = 5F_n^2 + 4(-1)^n$, and thus as n approaches +∞, the ratio $\frac{L_n}{F_n}$ approaches $\sqrt{5}$.
- $F_{2n} = L_n F_n$
- $F_n = \frac{L_{n-1} + L_{n+1}}{5}$

Their closed formula is given as:

$$L_n = \varphi^n + (1-\varphi)^n = \varphi^n + (-\varphi)^{-n} = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n,$$

where φ is the Golden ratio. Alternatively, L_n is the closest integer to φ^n.

Congruence relation

L_n is congruent to 1 mod n if n is prime, but some composite values of n also have this property.

Lucas primes

A **Lucas prime** is a Lucas number that is prime. The first few Lucas primes are

2, 3, 7, 11, 29, 47, 199, 521, 2207, 3571, 9349, ... (sequence A005479 [18] in OEIS)

If L_n is prime then n is either 0, prime, or a power of 2.[2] $L\ 2^m$ is prime for m = 1, 2, 3, and 4 and no other known values of m .

Lucas polynomials

The **Lucas polynomials** $L_n(x)$ are a polynomial sequence derived from the Lucas numbers in the same way as Fibonacci polynomials are derived from the Fibonacci numbers. Lucas polynomials are defined by the following recurrence relation:

$$L_n(x) = \begin{cases} 2, & \text{if } n = 0 \\ x, & \text{if } n = 1 \\ xL_{n-1}(x) + L_{n-2}(x), & \text{if } n \geq 2 \end{cases}$$

Lucas polynomials can be expressed in terms of Lucas sequences as

$$L_n(x) = V_n(x, -1).$$

The first few Lucas polynomials are:

$$L_0(x) = 2$$
$$L_1(x) = x$$
$$L_2(x) = x^2 + 2$$
$$L_3(x) = x^3 + 3x$$
$$L_4(x) = x^4 + 4x^2 + 2$$
$$L_5(x) = x^5 + 5x^3 + 5x$$
$$L_6(x) = x^6 + 6x^4 + 9x^2 + 2$$

The Lucas numbers are recovered by evaluating the polynomials at x = 1. The degree of $L_n(x)$ is n. The ordinary generating function for the sequence is

$$\sum_{n=0}^{\infty} L_n(x)t^n = \frac{2 - xt}{1 - t(x + t)}.$$

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa000032
[2] Chris Caldwell, " The Prime Glossary: Lucas prime (http://primes.utm.edu/glossary/page.php?sort=LucasPrime)" from The Prime Pages.

External links

- Weisstein, Eric W., " Lucas Number (http://mathworld.wolfram.com/LucasNumber.html)" from MathWorld.
- Weisstein, Eric W., " Lucas Polynomial (http://mathworld.wolfram.com/LucasPolynomial.html)" from MathWorld.
- Dr Ron Knott (http://www.mcs.surrey.ac.uk/Personal/R.Knott/Fibonacci/lucasNbs.html)
- Lucas numbers and the Golden Section (http://milan.milanovic.org/math/english/lucas/lucas.html)
- A Lucas Number Calculator can be found here. (http://www.plenilune.pwp.blueyonder.co.uk/fibonacci-calculator.asp)
- A Tutorial on Generalized Lucas Numbers (http://nakedprogrammer.com/LucasNumbers.aspx)

Lucky number

In number theory, a **lucky number** is a natural number in a set which is generated by a "sieve" similar to the Sieve of Eratosthenes that generates the primes.

Begin with a list of integers starting with 1:

```
1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,
```

Every second number (all even numbers) is eliminated, leaving only the odd integers:

```
1,    3,    5,    7,    9,   11,   13,   15,   17,   19,   21,   23,   25,
```

The second term in this sequence is 3. Every third number which remains in the list is eliminated:

```
1,    3,          7,    9,         13,   15,         19,   21,         25,
```

The third surviving number is now 7, so every seventh number that remains is eliminated:

```
1,    3,          7,    9,         13,   15,               21,         25,
```

As this procedure is repeated indefinitely, the survivors are the lucky numbers:

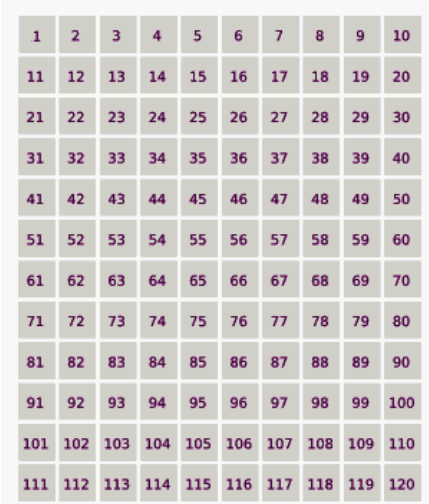
> 1, 3, 7, 9, 13, 15, 21, 25, 31, 33, 37, 43, 49, 51, 63, 67, 69, 73, 75, 79, 87, 93, 99, ... (sequence A000959 [1] in OEIS).

The term was introduced in 1955 in a paper by Gardiner, Lazarus, Metropolis and Ulam. They suggest also calling its defining sieve the sieve of Josephus Flavius.[2]

Lucky numbers share some properties with primes, such as asymptotic behaviour according to the prime number theorem; also Goldbach's conjecture has been extended to them. There are infinitely many lucky numbers. Because of these apparent connections with the prime numbers, some mathematicians have suggested that these properties may be found in a larger class of sets of numbers generated by sieves of a certain unknown form, although there is little theoretical basis for this conjecture. Twin lucky numbers and twin primes also appear to occur with similar frequency.

A **lucky prime** is a lucky number that is prime. It is not known whether there are infinitely many lucky primes. The first few are

> 3, 7, 13, 31, 37, 43, 67, 73, 79, 127, 151, 163, 193 (sequence A031157 [19] in OEIS).



An animation demonstrating the lucky number sieve. The numbers in red are lucky numbers.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa000959

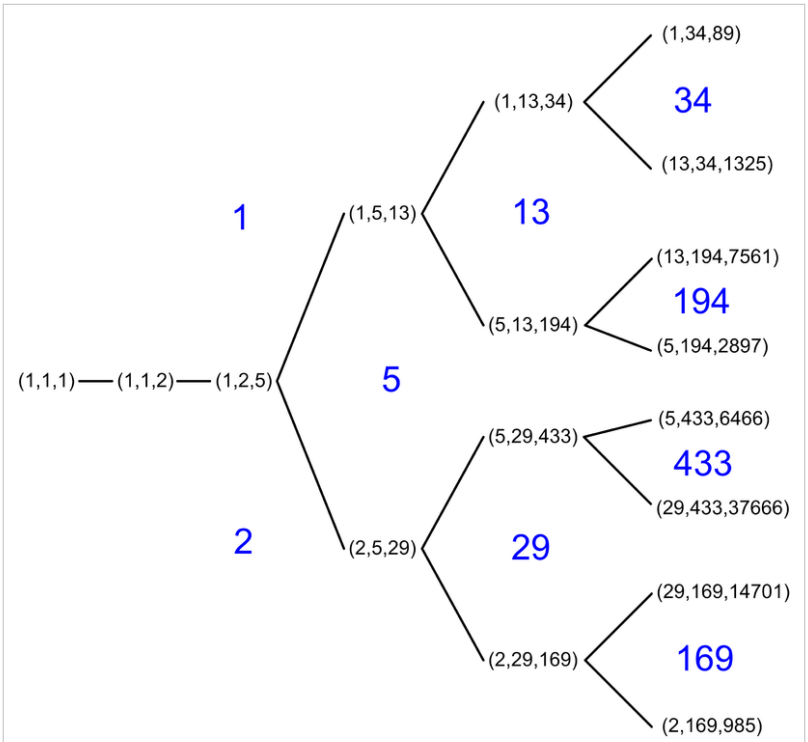
[2] V. Gardiner, R. Lazarus, N. Metropolis and S. Ulam, "On certain sequences of integers defined by sieves", *Mathematics Magazine* **29**:3 (1955), pp. 117–122.

External links

- Peterson, Ivars. MathTrek: Martin Gardner's Lucky Number (http://www.sciencenews.org/sn_arc97/9_6_97/mathland.htm)
- Weisstein, Eric W., " Lucky Number (http://mathworld.wolfram.com/LuckyNumber.html)" from MathWorld.
- Lucky Numbers (http://demonstrations.wolfram.com/LuckyNumbers/) by Enrique Zeleny, The Wolfram Demonstrations Project.

Markov number

A **Markov number** or **Markoff number** is a positive integer *x*, *y* or *z* that is part of a solution to the Markov Diophantine equation



The first levels of the Markov number tree

$$x^2 + y^2 + z^2 = 3xyz.$$

The first few Markov numbers are

1, 2, 5, 13, 29, 34, 89, 169, 194, 233, 433, 610, 985, 1325, ... (sequence A002559 [20] in OEIS)

appearing as coordinates of the Markov triples

(1, 1, 1), (1, 1, 2), (1, 2, 5), (1, 5, 13), (2, 5, 29), (1, 13, 34), (1, 34, 89), (2, 29, 169), (5, 13, 194), (1, 89, 233), (5, 29, 433), (89, 233, 610), etc.

There are infinitely many Markov numbers and Markov triples.

Properties

The symmetry of the Markov equation allows us to rearrange the order of the coordinates, so a Markov triple (a, b, c) may be normalized, as above, by assuming that $a \leq b \leq c$. Aside from the two smallest triples, every Markov triple (a, b, c) consists of three distinct integers. The unicity conjecture states that for a given Markov number c, there is exactly one normalized solution having c as its largest element.

The Markov numbers can also be arranged in a binary tree. The largest number at any level is always about a third from the bottom. All the Markov numbers on the regions adjacent to 2's region are odd-indexed Pell numbers (or numbers *n* such that $2n^2 - 1$ is a square, A001653 [1]), and all the Markov numbers on the regions adjacent to 1's region are odd-indexed Fibonacci numbers (A001519 [2]). Thus, there are infinitely many Markov triples of the form

$$(1, F_{2n-1}, F_{2n+1}),$$

where F_x is the *x*th Fibonacci number. Likewise, there are infinitely many Markov triples of the form

$$(2, P_{2n-1}, P_{2n+1}),$$

where P_x is the *x*th Pell number.[3]

Odd Markov numbers are 1 more than multiples of 4, while even Markov numbers are 2 more than multiples of 32.[4] Markov numbers are not always prime but members of a Markov triple are always coprime.

Knowing one Markov triple (*x*, *y*, *z*) one can find another Markov triple, of the form $(x, y, 3xy - z)$.[5] It's not necessary that $x < y < z$ in order for the $(x, y, 3xy - z)$ to yield another triple.

If we start, as an example, with (1, 5, 13) we get its three neighbors (5, 13, 194), (1, 13, 34) and (1, 2, 5) in the Markov tree if *x* is set to 1, 5 and 13, respectively. Applying $(x, y, z) \to (x, y, 3xy - z)$ twice returns the same triple one started with, therefore a reordering is necessary to obtain new triples. For instance, starting with (1, 1, 2) and trading *y* and *z* before each iteration of the transform lists Markov triples with Fibonacci numbers. Starting with that same triplet and trading *x* and *z* before each iteration gives the triples with Pell numbers.

In his 1982 paper, Don Zagier conjectured that the *n*th Markov number is asymptotically given by

$$m_n = \tfrac{1}{3}e^{C\sqrt{n}+o(1)} \quad \text{with } C = 2.3523418721\ldots.$$

Moreover he pointed out that $x^2 + y^2 + z^2 = 3xyz + 4/9$, an extremely good approximation of the original Diophantine equation, is equivalent to $f(x) + f(y) = f(z)$ with $f(t) = \operatorname{arcosh}(3t/2)$.[6]

The *n*th Lagrange number can be calculated from the *n*th Markov number with the formula

$$L_n = \sqrt{9 - \frac{4}{{m_n}^2}}.$$

Markov numbers are named after the Russian mathematician Andrey Markov. Due to different methods of transliterating Cyrillic, the term is written as "Markoff numbers" in some literature. But in this particular case, "Markov" might be preferable because "Markoff number" might be misunderstood as "mark-off number."

Notes

[1] http://en.wikipedia.org/wiki/Oeis%3Aa001653

[2] http://en.wikipedia.org/wiki/Oeis%3Aa001519

[3] A030452 (http://en.wikipedia.org/wiki/Oeis:a030452) lists Markov numbers that appear in solutions where one of the other two terms is 5.

[4] Zhang, Ying (2007). "Congruence and Uniqueness of Certain Markov Numbers" (http://journals.impan.gov.pl/aa/Inf/128-3-7.html). *Acta Arithmetica* **128** (3): 295–301. doi:10.4064/aa128-3-7. MR2313995. .

[5] Because $x^2+y^2+(3xy-z)^2 = x^2+y^2+z^2+9x^2y^2-6xyz = 9x^2y^2-3xyz = 3(3xy-z)xy$.

[6] Zagier, Don B. (1982). "On the Number of Markoff Numbers Below a Given Bound" (http://links.jstor.org/sici?sici=0025-5718(198210)39:160<709:OTNOMN>2.0.CO;2-U). *Mathematics of Computation* **160** (160): 709–723. doi:10.2307/2007348. MR0669663. .

References

- Thomas Cusick, Mari Flahive: *The Markoff and Lagrange spectra*, Math. Surveys and Monographs **30**, AMS, Providence 1989

Mersenne prime

Publication year	1536[Note 1]
Author of publication	Regius, H.
Number of known cases	47
OEIS index and link	A000668 [21]

In mathematics, a **Mersenne number**, named after Marin Mersenne, is a positive integer that is one less than a power of two:

$$M_p = 2^p - 1.$$

Some definitions of Mersenne numbers require that the exponent p be prime.

A **Mersenne prime** is a Mersenne number that is prime. It is known[1] that if $2^p - 1$ is prime then p is prime, so it makes no difference which Mersenne number definition is used. As of October 2009, only 47 Mersenne primes are known. The largest known prime number ($2^{43,112,609} - 1$) is a Mersenne prime.[2] Since 1997, all newly-found Mersenne primes have been discovered by the "Great Internet Mersenne Prime Search" (GIMPS), a distributed computing project on the Internet.

About Mersenne primes

Many fundamental questions about Mersenne primes remain unresolved. It is not even known whether the set of Mersenne primes is finite. The Lenstra–Pomerance–Wagstaff conjecture asserts that, on the contrary, there are infinitely many Mersenne primes and predicts their order of growth. It is also not known whether infinitely many Mersenne numbers with prime exponents are composite, although this would follow from widely believed conjectures about prime numbers, for example, the infinitude of Sophie Germain primes.

A basic theorem about Mersenne numbers states that in order for M_p to be a Mersenne prime, the exponent p itself must be a prime number. This rules out primality for numbers such as $M_4 = 2^4 - 1 = 15$: since the exponent $4 = 2\times2$ is composite, the theorem predicts that 15 is also composite; indeed, $15 = 3\times5$. The three smallest Mersenne primes are

$$M_2 = 3, M_3 = 7, M_5 = 31.$$

While it is true that only Mersenne numbers M_p, where $p = 2, 3, 5, \ldots$ *could* be prime, often M_p is not prime even for a prime exponent p. The smallest counterexample is the Mersenne number

$$M_{11} = 2^{11} - 1 = 2047 = 23 \times 89,$$

which is not prime, even though 11 is a prime number. The lack of an obvious rule to determine whether a given Mersenne number is prime makes the search for Mersenne primes an interesting task, which becomes difficult very quickly, since Mersenne numbers grow very rapidly. The Lucas–Lehmer primality test is an efficient primality test that greatly aids this task. The search for the largest known prime has somewhat of a cult following. Consequently, a lot of computer power has been expended searching for new Mersenne primes, much of which is now done using distributed computing.

Mersenne primes are used in pseudorandom number generators such as the Mersenne twister, Park–Miller random number generator, Generalized Shift Register and Fibonacci RNG.

Searching for Mersenne primes

The identity

$$2^{ab} - 1 = (2^a - 1) \cdot \left(1 + 2^a + 2^{2a} + 2^{3a} + \cdots + 2^{(b-1)a}\right)$$

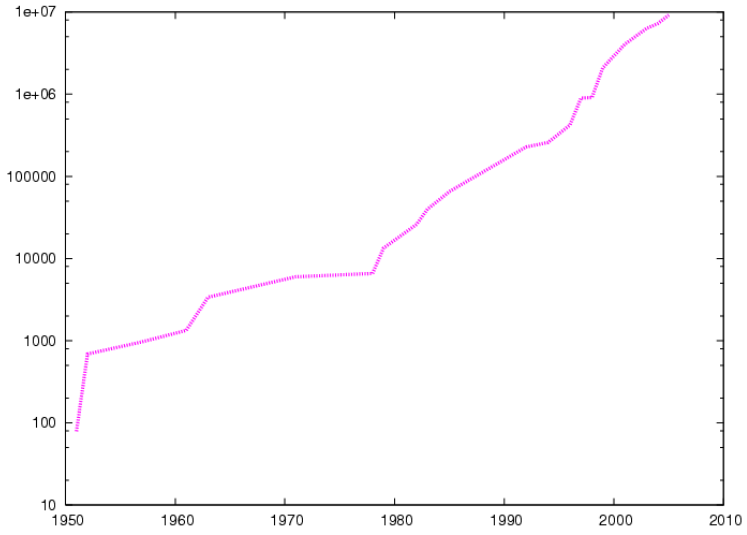
shows that M_p can be prime only if p itself is prime—that is, the primality of p is necessary but not sufficient for M_p to be prime—which simplifies the search for Mersenne primes considerably. The converse statement, namely that M_p is necessarily prime if p is prime, is false. The smallest counterexample is $2^{11} - 1 = 2{,}047 = 23 \times 89$, a composite number.

Fast algorithms for finding Mersenne primes are available, and the largest known prime numbers as of 2009 are Mersenne primes.

The first four Mersenne primes $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ and $M_7 = 127$ were known in antiquity. The fifth, $M_{13} = 8191$, was discovered anonymously before 1461; the next two (M_{17} and M_{19}) were found by Cataldi in 1588. After nearly two centuries, M_{31} was verified to be prime by Euler in 1772. The next (in historical, not numerical order) was M_{127}, found by Lucas in 1876, then M_{61} by Pervushin in 1883. Two more (M_{89} and M_{107}) were found early in the 20th century, by Powers in 1911 and 1914, respectively.

The best method presently known for testing the primality of Mersenne numbers is the Lucas–Lehmer primality test. Specifically, it can be shown that for prime $p > 2$, $M_p = 2^p - 1$ is prime if and only if M_p divides S_{p-2}, where $S_0 = 4$ and, for $k > 0$,

$$S_k = S_{k-1}^2 - 2.$$



Graph of number of digits in largest known Mersenne prime by year - electronic era. Note that the vertical scale, the number of digits, is a double logarithmic scale of the value of the prime.

The search for Mersenne primes was revolutionized by the introduction of the electronic digital computer. Alan Turing searched for them on the Manchester Mark 1 in 1949.[3] But the first successful identification of a Mersenne prime, M_{521}, by this means was achieved at 10:00 P.M. on January 30, 1952 using the U.S. National Bureau of Standards Western Automatic Computer (SWAC) at the Institute for Numerical Analysis at the University of California, Los Angeles, under the direction of Lehmer, with a computer search program written and run by Prof. R.M. Robinson. It was the first Mersenne prime to be identified in thirty-eight years; the next one, M_{607}, was found by the computer a little less than two hours later. Three more — M_{1279}, M_{2203}, M_{2281} — were found by the same program in the next several months. M_{4253} is the first Mersenne prime that is titanic, M_{44497} is the first gigantic, and $M_{6,972,593}$ was the first megaprime to be discovered, being a prime with at least 1,000,000 digits.[4] All three were the first known prime of any kind of that size.

In September 2008, mathematicians at UCLA participating in GIMPS won part of a $100,000 prize from the Electronic Frontier Foundation for their discovery of a very nearly 13-million-digit Mersenne prime. The prize, finally confirmed in October 2009, is for the first known prime with at least 10 million digits. The prime was found on a Dell OptiPlex 745 on August 23, 2008. This is the eighth Mersenne prime discovered at UCLA.[5]

On April 12, 2009, a GIMPS server log reported that a 47th Mersenne prime had possibly been found. This report was apparently overlooked until June 4, 2009. The find was verified on June 12, 2009. The prime is $2^{42,643,801} - 1$. Although it is chronologically the 47th Mersenne prime to be discovered, it is less than the largest known which was the 45th to be discovered.

Theorems about Mersenne numbers

1. If a and p are natural numbers such that $a^p - 1$ is prime, then $a = 2$ or $p = 1$.
   - **Proof**: $a \equiv 1 \pmod{a-1}$. Then $a^p \equiv 1 \pmod{a-1}$, so $a^p - 1 \equiv 0 \pmod{a-1}$. Thus $a - 1 \mid a^p - 1$. However, $a^p - 1$ is prime, so $a - 1 = a^p - 1$ or $a - 1 = \pm 1$. In the former case, $a = a^p$, hence $a = 0,1$ (which is a contradiction, as neither -1 nor 0 is prime) or $p = 1$. In the latter case, $a = 2$ or $a = 0$. If $a = 0$, however, $0^p - 1 = 0 - 1 = -1$ which is not prime. Therefore, $a = 2$.
2. If $2^p - 1$ is prime, then p is prime.
   - **Proof**: suppose that p is composite, hence can be written $p = a \cdot b$ with a and $b > 1$. Then $(2^a)^b - 1$ is prime, but $b > 1$ and $2^a > 2$, contradicting statement 1.
3. If p is an odd prime, then any prime q that divides $2^p - 1$ must be 1 plus a multiple of $2p$. This holds even when $2^p - 1$ is prime.
   - **Examples**: Example I: $2^5 - 1 = 31$ is prime, and 31 is 1 plus a multiple of 2×5. Example II: $2^{11} - 1 = 23 \times 89$, where $23 = 1 + 2 \times 11$, and $89 = 1 + 8 \times 11$.
   - **Proof**: If q divides $2^p - 1$ then $2^p \equiv 1 \pmod{q}$. By Fermat's Little Theorem, $2^{(q-1)} \equiv 1 \pmod{q}$. Assume p and $q - 1$ are relatively prime, a similar application of Fermat's Little Theorem says that $(q-1)^{(p-1)} \equiv 1 \pmod{p}$. Thus there is a number $x \equiv (q-1)^{(p-2)}$ for which $(q-1) \cdot x \equiv 1 \pmod{p}$, and therefore a number k for which $(q-1) \cdot x - 1 = kp$. Since $2^{(q-1)} \equiv 1 \pmod{q}$, raising both sides of the congruence to the power x gives $2^{(q-1)x} \equiv 1$, and since $2^p \equiv 1 \pmod{q}$, raising both sides of the congruence to the power k gives $2^{kp} \equiv 1$. Thus $2^{(q-1)x}/2^{kp} = 2^{(q-1)x - kp} \equiv 1 \pmod{q}$. But by definition, $(q-1)x - kp = 1$, implying that $2^1 \equiv 1 \pmod{q}$; in other words, that q divides 1. Thus the initial assumption that p and $q - 1$ are relatively prime is untenable. Since p is prime $q - 1$ must be a multiple of p.
   - **Note**: This fact provides a proof of the infinitude of primes distinct from Euclid's Theorem: if there were finitely many primes, with p being the largest, we reach an immediate contradiction since all primes dividing $2^p - 1$ must be larger than p.
4. If p is an odd prime, then any prime q that divides $2^p - 1$ must be congruent to $\pm 1 \pmod{8}$.
   - **Proof**: $2^{p+1} = 2 \pmod{q}$, so $2^{(p+1)/2}$ is a square root of 2 modulo q. By quadratic reciprocity, any prime modulo which 2 has a square root is congruent to $\pm 1 \pmod{8}$.
5. A Mersenne prime cannot be a Wieferich prime.
   - **Proof**: We show if $p = 2^m - 1$ is a Mersenne prime, then the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ does not satisfy. By Fermat's Little theorem, $m \mid p - 1$. Now write, $p - 1 = m\lambda$. If the given congruence satisfies, then $p^2 \mid 2^{m\lambda} - 1$,therefore
     $0 \equiv (2^{m\lambda} - 1)/(2^m - 1) = 1 + 2^m + 2^{2m} + \ldots + 2^{(\lambda-1)m} \equiv -\lambda \pmod{2^m - 1}$. Hence $2^m - 1 \mid \lambda$,and therefore $\lambda \geq 2^m - 1$. This leads to $p - 1 \geq m(2^m - 1)$, which is impossible since $m \geq 2$.

History

Mersenne primes were considered already by Euclid, who found a connection with the perfect numbers. They are named after 17th-century French scholar Marin Mersenne, who compiled a list of Mersenne primes with exponents up to 257. His list was only partially correct, as Mersenne mistakenly included M_{67} and M_{257} (which are composite), and omitted M_{61}, M_{89}, and M_{107} (which are prime). Mersenne gave little indication how he came up with his list,[6] and its rigorous verification was completed more than two centuries later.

List of known Mersenne primes

The table below lists all known Mersenne primes (sequence A000668 [21] in OEIS):

#	p	M_p	Digits in M_p	Date of discovery	Discoverer
1	2	3	1	5th century BC[7]	Ancient Greek mathematicians
2	3	7	1	5th century BC[7]	Ancient Greek mathematicians
3	5	31	2	3rd century BC[7]	Ancient Greek mathematicians
4	7	127	3	3rd century BC[7]	Ancient Greek mathematicians
5	13	8191	4	1456	*anonymous* [1]
6	17	131071	6	1588	Cataldi
7	19	524287	6	1588	Cataldi
8	31	2147483647	10	1772	Euler
9	61	2305843009213693951	19	1883	Pervushin
10	89	618970019…449562111	27	1911	Powers
11	107	162259276…010288127	33	1914	Powers[8]
12	127	170141183…884105727	39	1876	Lucas
13	521	686479766…115057151	157	January 30, 1952	Robinson, using SWAC
14	607	531137992…031728127	183	January 30, 1952	Robinson
15	1,279	104079321…168729087	386	June 25, 1952	Robinson
16	2,203	147597991…697771007	664	October 7, 1952	Robinson
17	2,281	446087557…132836351	687	October 9, 1952	Robinson
18	3,217	259117086…909315071	969	September 8, 1957	Riesel, using BESK
19	4,253	190797007…350484991	1,281	November 3, 1961	Hurwitz, using IBM 7090
20	4,423	285542542…608580607	1,332	November 3, 1961	Hurwitz
21	9,689	478220278…225754111	2,917	May 11, 1963	Gillies, using ILLIAC II
22	9,941	346088282…789463551	2,993	May 16, 1963	Gillies
23	11,213	281411201…696392191	3,376	June 2, 1963	Gillies
24	19,937	431542479…968041471	6,002	March 4, 1971	Tuckerman, using IBM 360/91
25	21,701	448679166…511882751	6,533	October 30, 1978	Noll & Nickel, using CDC Cyber 174
26	23,209	402874115…779264511	6,987	February 9, 1979	Noll
27	44,497	854509824…011228671	13,395	April 8, 1979	Nelson & Slowinski
28	86,243	536927995…433438207	25,962	September 25, 1982	Slowinski

29	110,503	521928313…465515007	33,265	January 28, 1988	Colquitt & Welsh
30	132,049	512740276…730061311	39,751	September 19, 1983[7]	Slowinski
31	216,091	746093103…815528447	65,050	September 1, 1985[7]	Slowinski
32	756,839	174135906…544677887	227,832	February 19, 1992	Slowinski & Gage on Harwell Lab Cray-2[9]
33	859,433	129498125…500142591	258,716	January 4, 1994[10]	Slowinski & Gage
34	1,257,787	412245773…089366527	378,632	September 3, 1996	Slowinski & Gage[11]
35	1,398,269	814717564…451315711	420,921	November 13, 1996	GIMPS / Joel Armengaud[12]
36	2,976,221	623340076…729201151	895,932	August 24, 1997	GIMPS / Gordon Spence[13]
37	3,021,377	127411683…024694271	909,526	January 27, 1998	GIMPS / Roland Clarkson[14]
38	6,972,593	437075744…924193791	2,098,960	June 1, 1999	GIMPS / Nayan Hajratwala[15]
39	13,466,917	924947738…256259071	4,053,946	November 14, 2001	GIMPS / Michael Cameron[16]
40	20,996,011	125976895…855682047	6,320,430	November 17, 2003	GIMPS / Michael Shafer[17]
41[*]	24,036,583	299410429…733969407	7,235,733	May 15, 2004	GIMPS / Josh Findley[18]
42[*]	25,964,951	122164630…577077247	7,816,230	February 18, 2005	GIMPS / Martin Nowak[19]
43[*]	30,402,457	315416475…652943871	9,152,052	December 15, 2005	GIMPS / Curtis Cooper & Steven Boone[20]
44[*]	32,582,657	124575026…053967871	9,808,358	September 4, 2006	GIMPS / Curtis Cooper & Steven Boone[21]
45[*]	37,156,667	202254406…308220927	11,185,272	September 6, 2008	GIMPS / Hans-Michael Elvenich[22]
46[*]	42,643,801	169873516…562314751	12,837,064	April 12, 2009[**]	GIMPS / Odd M. Strindmo
47[*]	43,112,609	316470269…697152511	12,978,189	August 23, 2008	GIMPS / Edson Smith[22]

[*] It is not known whether any undiscovered Mersenne primes exist between the 40th ($M_{20,996,011}$) and the 47th ($M_{43,112,609}$) on this chart; the ranking is therefore provisional. Primes are not always discovered in increasing order. For example, the 29th Mersenne prime was discovered *after* the 30th and the 31st. Similarly, the current record holder was followed by two smaller Mersenne primes, first 2 weeks later and then 8 months later.

[**] $M_{42,643,801}$ was first found by a machine on April 12, 2009; however, no human took notice of this fact until June 4. Thus, either April 12 or June 4 may be considered the 'discovery' date. The discoverer, Strindmo, apparently used the alias Stig M. Valstad.

To help visualize the size of the 47th known Mersenne prime, it would require 3,461 pages to display the number in base 10 with 75 digits per line and 50 lines per page.[7]

The largest known Mersenne prime ($2^{43,112,609} - 1$) is also the largest known prime number,[23] and was the first discovered prime number with more than 10 million base-10 digits.

In modern times, the largest known prime has almost always been a Mersenne prime.[24]

Factorization of Mersenne numbers

The factorization of a prime number is by definition the number itself. This section is about composite numbers. Mersenne numbers are very good test cases for the special number field sieve algorithm, so often the largest number factorized with this algorithm has been a Mersenne number. As of March 2007, $2^{1039} - 1$ is the record-holder,[25] after a calculation taking about a year on a couple of hundred computers, mostly at NTT in Japan and at EPFL in Switzerland. See integer factorization records for links to more information. The special number field sieve can factorize numbers with more than one large factor. If a number has only one very large factor then other algorithms can factorize larger numbers by first finding small factors and then making a primality test on the cofactor. As of 2010, the composite Mersenne number with largest proven prime factors is $2^{20887} - 1$, which is known to have a factor p with 6229 digits that was proven prime with ECPP.[26] The largest with probable prime factors allowed is $2^{684127} - 1 = 23765203727 \times q$, where q is a probable prime.[27]

Perfect numbers

Mersenne primes are interesting to many for their connection to perfect numbers. In the 4th century BC, Euclid demonstrated that if M_p is a Mersenne prime then

$$2^{p-1} \cdot (2^p - 1) = M_p(M_p + 1)/2$$

is an even perfect number (which is also the M_pth triangular number and the 2^{p-1}th hexagonal number). In the 18th century, Leonhard Euler proved that, conversely, all even perfect numbers have this form. It is unknown whether there are any odd perfect numbers, but it appears unlikely that there is one.

Generalization

The binary representation of $2^p - 1$ is the digit 1 repeated p times, for example, $2^5 - 1 = 11111_2$ in the binary notation. A Mersenne number is therefore a repunit in base 2, and Mersenne primes are the base 2 repunit primes.

The base 2 representation of a Mersenne number shows the factorization pattern for composite exponent. For example:

$$\begin{aligned}
&M_{35} = 2^{35} - 1 = (11111111111111111111111111111111111)_2 \\
&= (11111)_2 \cdot (10000100001000010000100001000010001)_2 = M_5 \cdot (10000100001000010000100001000010001)_2 \\
&= (1111111)_2 \cdot (10000001000000100000010000001)_2 = M_7 \cdot (10000001000000100000010000001)_2 \\
&= (11111)_2 \cdot (1111111)_2 \cdot [(10000101001010100101000001)_2 - (01000010100101001010000010)_2] \\
&= M_5 \cdot M_7 \cdot (10000101001010110101111111)_2.
\end{aligned}$$

Mersenne numbers in nature and elsewhere

In computer science, unsigned p-bit integers can be used to express numbers up to M_p.

In the mathematical problem Tower of Hanoi, solving a puzzle with a p-disc tower requires at least M_p steps.

The asteroid with minor planet number 8191 is named 8191 Mersenne after Marin Mersenne, because 8191 is the fifth Mersenne prime.[28] The asteroids with the previous four numbers corresponding to Mersenne primes (3 Juno, 7 Iris, 31 Euphrosyne, 127 Johanna) were already named after others.

See also

- Repunit
- Fermat prime
- Erdős–Borwein constant
- Mersenne conjectures
- Mersenne Twister
- Prime95 / MPrime
- Largest known prime number
- Double Mersenne number
- Wieferich prime
- Wagstaff prime
- Solinas prime

Notes

1. ^ Mersenne primes have already been described in Regius, H. (1536). Utrisque Arithmetices Epitome [29]

References

[1] The Prime Pages, Mersenne Primes: History, Theorems and Lists (http://primes.utm.edu/mersenne/).

[2] 12-million-digit prime number sets record, nets $100,000 prize (http://www.networkworld.com/community/node/46184)

[3] Brian Napper, The Mathematics Department and the Mark 1 (http://www.computer50.org/mark1/maths.html).

[4] The Prime Pages, The Prime Glossary: megaprime (http://primes.utm.edu/glossary/page.php?sort=Megaprime).

[5] UCLA mathematicians discover a 13-million-digit prime number, Los Angeles Times, September 27, 2008 (http://www.latimes.com/news/science/la-sci-prime27-2008sep27,0,2746766.story)

[6] The Prime Pages, Mersenne's conjecture (http://primes.utm.edu/glossary/page.php?sort=MersennesConjecture).

[7] Landon Curt Noll, Mersenne Prime Digits and Names (http://www.isthe.com/chongo/tech/math/prime/mersenne.html#largest).

[8] The Prime Pages, M_{107}: Fauquembergue or Powers? (http://primes.utm.edu/notes/fauquem.html).

[9] The Prime Pages, The finding of the 32*nd* Mersenne (http://primes.utm.edu/notes/756839.html).

[10] Chris Caldwell, The Largest Known Primes (http://www.math.unicaen.fr/~reyssat/largest.html).

[11] The Prime Pages, A Prime of Record Size! $2^{1257787}$-1 (http://primes.utm.edu/notes/1257787.html).

[12] GIMPS Discovers 35th Mersenne Prime (http://www.mersenne.org/primes/1398269.htm).

[13] GIMPS Discovers 36th Known Mersenne Prime (http://www.mersenne.org/primes/2976221.htm).

[14] GIMPS Discovers 37th Known Mersenne Prime (http://www.mersenne.org/primes/3021377.htm).

[15] GIMPS Finds First Million-Digit Prime, Stakes Claim to $50,000 EFF Award (http://www.mersenne.org/primes/6972593.htm).

[16] GIMPS, Researchers Discover Largest Multi-Million-Digit Prime Using Entropia Distributed Computing Grid (http://www.mersenne.org/primes/13466917.htm).

[17] GIMPS, Mersenne Project Discovers Largest Known Prime Number on World-Wide Volunteer Computer Grid (http://www.mersenne.org/primes/20996011.htm).

[18] GIMPS, Mersenne.org Project Discovers New Largest Known Prime Number, $2^{24,036,583}$-1 (http://www.mersenne.org/primes/24036583.htm).

[19] GIMPS, Mersenne.org Project Discovers New Largest Known Prime Number, $2^{25,964,951}$-1 (http://www.mersenne.org/primes/25964951.htm).

[20] GIMPS, Mersenne.org Project Discovers New Largest Known Prime Number, $2^{30,402,457}$-1 (http://www.mersenne.org/primes/30402457.htm).

[21] GIMPS, Mersenne.org Project Discovers Largest Known Prime Number, $2^{32,582,657}$-1 (http://www.mersenne.org/primes/32582657.htm).

[22] Titanic Primes Raced to Win $100,000 Research Award (http://mersenne.org/primes/m45and46.htm). Retrieved on 2008-09-16.

[23] 12-million-digit prime number sets record, nets $100,000 prize (http://www.networkworld.com/community/node/46184)

[24] The largest known prime has been a Mersenne prime since 1952, except between 1989 and 1992; see Caldwell, " The Largest Known Prime by Year: A Brief History (http://primes.utm.edu/notes/by_year.html)" from the Prime Pages website, University of Tennessee at Martin.

[25] Paul Zimmermann, "Integer Factoring Records" (http://www.loria.fr/~zimmerma/records/factor.html).

[26] Chris Caldwell, The Top Twenty: Mersenne cofactor (http://primes.utm.edu/top20/page.php?id=49) at The Prime Pages.

[27] Donovan Johnson, "Largest known probable prime Mersenne Cofactors" (http://donovanjohnson.com/mersenne.html).

[28] JPL Small-Body Database Browser (http://ssd.jpl.nasa.gov/sbdb.cgi?sstr=8191+Mersenne)

[29] http://books.google.de/books?id=hs85AAAAcAAJ&printsec=frontcover&dq=Utriusque+Arithmetices+epitome&hl=de&ei=o4cDTb10y_WyBur_8PkJ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCoQ6AEwAA#v=onepage&q=2047&f=false

External links

- GIMPS home page (http://www.mersenne.org)
- Mersenne Primes: History, Theorems and Lists (http://primes.utm.edu/mersenne/) — explanation
- GIMPS status (http://v5www.mersenne.org/report_milestones/) — status page gives various statistics on search progress, typically updated every week, including progress towards proving the ordering of primes 40–47
- $M_q = (8x)^2 - (3qy)^2$ Mersenne proof (http://tony.reix.free.fr/Mersenne/Mersenne8x3qy.pdf) (pdf)
- $M_q = x^2 + d \cdot y^2$ math thesis (http://www.math.leidenuniv.nl/scripties/jansen.ps) (ps)
- Mersenne prime bibliography (http://www.utm.edu/research/primes/mersenne/LukeMirror/biblio.htm) with hyperlinks to original publications
- **(German)** report about Mersenne primes (http://www.taz.de/pt/2005/03/11/a0355.nf/text) — detection in detail
- GIMPS wiki (http://mersennewiki.org/index.php/Main_Page)
- Will Edgington's Mersenne Page (http://www.garlic.com/~wedgingt/mersenne.html) — contains factors for small Mersenne numbers
- a file (ftp://mersenne.org/gimps/factors.zip) containing the smallest known factors of all tested Mersenne numbers (requires program (ftp://mersenne.org/gimps/decomp.zip) to open)
- Decimal digits and English names of Mersenne primes (http://www.isthe.com/chongo/tech/math/prime/mersenne.html)

MathWorld links

- Weisstein, Eric W., " Mersenne number (http://mathworld.wolfram.com/MersenneNumber.html)" from MathWorld.
- Weisstein, Eric W., " Mersenne prime (http://mathworld.wolfram.com/MersennePrime.html)" from MathWorld.
- 44th Mersenne Prime Found (http://mathworld.wolfram.com/news/2006-09-11/mersenne-44/)

Mills' constant

In number theory, **Mills' constant** is defined as the smallest positive real number A such that the floor of the double exponential function

$$\lfloor A^{3^n} \rfloor$$

is a prime number, for all positive integers n. This constant is named after William H. Mills who proved in 1947 the existence of A based on results of Guido Hoheisel and Albert Ingham on the prime gaps. Its value is unknown, but if the Riemann hypothesis is true it is approximately

$$A \approx 1.306377883863080690468614492 6\ldots$$ (sequence A051021 [1] in OEIS).

Mills primes

The primes generated by Mills' constant are known as Mills primes; if the Riemann hypothesis is true, the sequence begins

2, 11, 1361, 2521008887... (sequence A051254 [22] in OEIS).

If $a(i)$ denotes the ith prime in this sequence, then $a(i)$ can be calculated as the smallest prime number larger than $a(i-1)^3$. In order to ensure that rounding $A^3 n$, for n = 1, 2, 3, ..., produces this sequence of primes, it must be the case that $a(i) < (a(i-1) + 1)^3$. The Hoheisel-Ingham results guarantee that there exists a prime between any two sufficiently large cubic numbers, which is sufficient to prove this inequality if we start from a sufficiently large first prime $a(1)$. The Riemann hypothesis implies that there exists a prime between any two consecutive cubes, allowing the *sufficiently large* condition to be removed, and allowing the sequence of Mills' primes to begin at $a(1) = 2$.

Currently, the largest known Mills prime (under the Riemann hypothesis) is

$$(((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3+894)^3+3636)^3+70756)^3+97220,$$

which is 20,562 digits long.

Numerical calculation

By calculating the sequence of Mills primes, one can approximate Mills' constant as

$$A \approx a(n)^{1/3^n}.$$

Caldwell & Cheng (2005) used this method to compute almost seven thousand base 10 digits of Mills' constant under the assumption that the Riemann hypothesis is true. There is no closed-form formula known for Mills' constant, and it is not even known whether this number is rational (Finch 2003).

References

- Caldwell, Chris K.; Cheng, Yuanyou (2005), "Determining Mills' Constant and a Note on Honaker's Problem" [2], *Journal of Integer Sequences* **8** (05.4.1).
- Finch, Steven R. (2003), "Mills' Constant", *Mathematical Constants*, Cambridge University Press, pp. 130–133, ISBN 0521818052.
- Mills, W. H. (1947), "A prime-representing function", *Bulletin of the American Mathematical Society* **53**: 604, doi:10.1090/S0002-9904-1947-08849-2.

External links

- Weisstein, Eric W., "Mills' Constant [3]" from MathWorld.
- Who remembers the Mills number? [4], E. Kowalski.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa051021
[2] http://www.cs.uwaterloo.ca/journals/JIS/VOL8/Caldwell/caldwell78.html
[3] http://mathworld.wolfram.com/MillsConstant.html
[4] http://blogs.ethz.ch/kowalski/2009/04/02/who-remembers-the-mills-number/

Minimal prime (recreational mathematics)

In recreational number theory, a **minimal prime** is a prime number for which there is no shorter subsequence of its digits in a given base that form a prime. In base 10 there are exactly 26 minimal primes:

> 2, 3, 5, 7, 11, 19, 41, 61, 89, 409, 449, 499, 881, 991, 6469, 6949, 9001, 9049, 9649, 9949, 60649, 666649, 946669, 60000049, 66000049, 66600049 (sequence A071062 [23] in OEIS).

For example, 409 is a minimal prime because there is no prime among the shorter subsequences of the digits: 4, 0, 9, 40, 49, 09. The subsequence does not have to consist of consecutive digits, so 109 is not a minimal prime (because 19 is prime). But it does have to be in the same order; so, for example, 991 is still a minimal prime even though a subset of the digits can form the shorter prime 19 by changing the order.

Similarly, there are exactly 32 composite numbers which have no shorter composite subsequence:

> 4, 6, 8, 9, 10, 12, 15, 20, 21, 22, 25, 27, 30, 32, 33, 35, 50, 51, 52, 55, 57, 70, 72, 75, 77, 111, 117, 171, 371, 711, 713, 731 (sequence A071070 [1] in OEIS).

References

- Chris Caldwell, *The Prime Glossary: minimal prime* [2], from the Prime Pages
- J. Shallit, *Minimal primes* [3], *Journal of Recreational Mathematics*, **30**:2, pp. 113–117, 1999-2000.

References

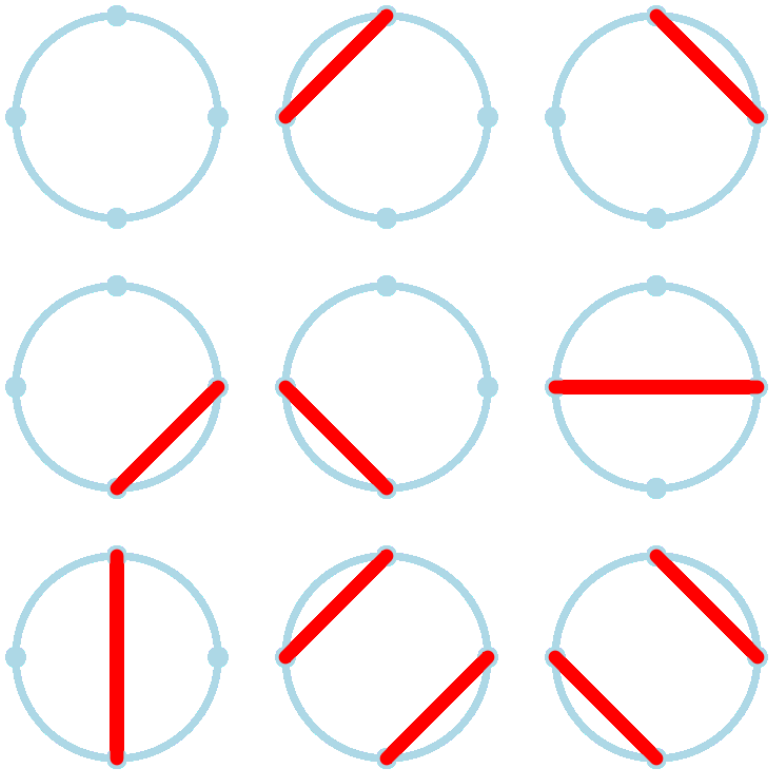
[1] http://en.wikipedia.org/wiki/Oeis%3Aa071070
[2] http://primes.utm.edu/glossary/page.php?sort=MinimalPrime
[3] http://www.cs.uwaterloo.ca/~shallit/Papers/minimal5.ps

Motzkin number

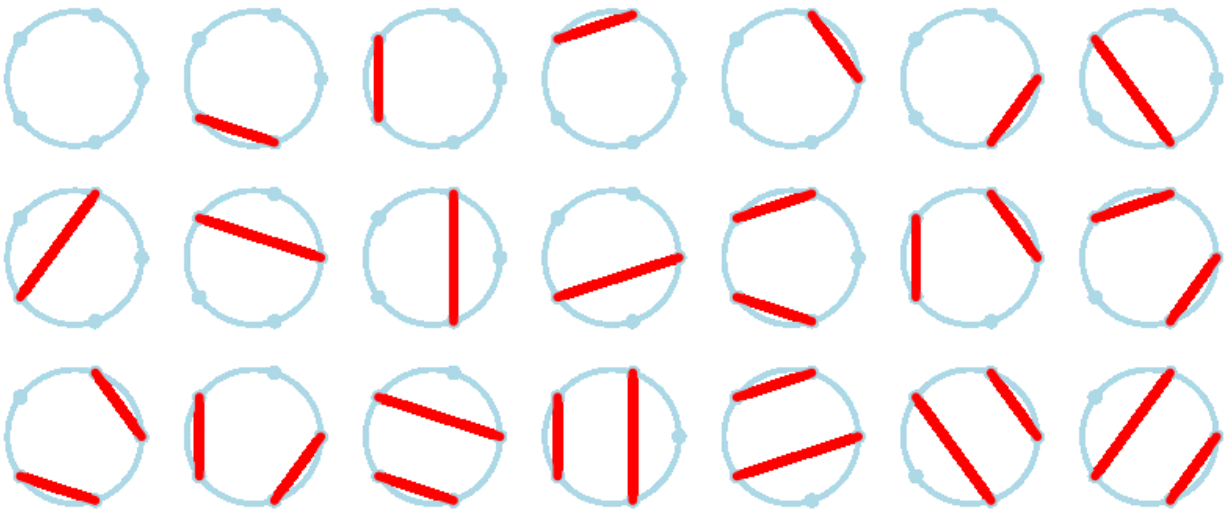
In mathematics, a **Motzkin number** for a given number n (named after Theodore Motzkin) is the number of different ways of drawing non-intersecting chords on a circle between n points. The Motzkin numbers have very diverse applications in geometry, combinatorics and number theory. The first few Motzkin numbers are (sequence A001006 [1] in OEIS):

1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798, 15511, 41835, 113634, 310572, 853467, 2356779, 6536382, 18199284, 50852019, 142547559, 400763223, 1129760415, 3192727797, 9043402501, 25669818476, 73007772802, 208023278209, 593742784829

The following figure shows the 9 ways to draw non-intersecting chords between 4 points on a circle.



The following figure shows the 21 ways to draw non-intersecting chords between 5 points on a circle.



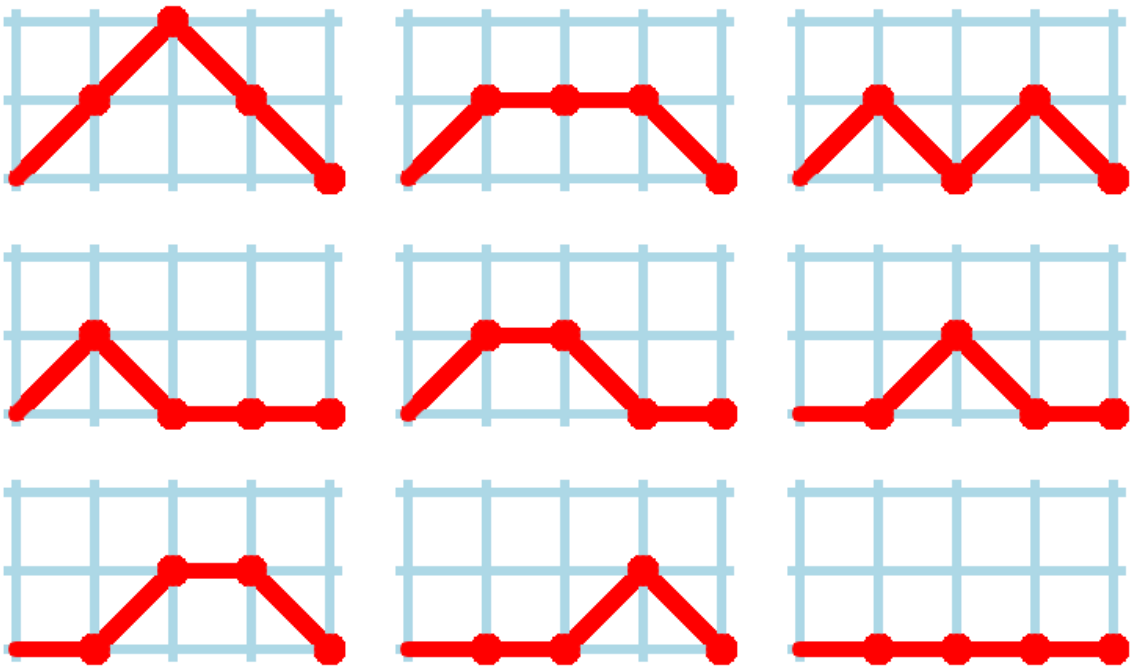
A **Motzkin prime** is a Motzkin number that is prime. As of October 2007, four such primes are known (sequence A092832 [24] in OEIS):

2, 127, 15511, 953467954114363

The Motzkin number for n is also the number of positive integer sequences $n-1$ long in which the opening and ending elements are either 1 or 2, and the difference between any two consecutive elements is −1, 0 or 1.

Also on the upper right quadrant of a grid, the Motzkin number for n gives the number of routes from coordinate (0, 0) to coordinate (n, 0) on n steps if one is allowed to move only to the right (up, down or straight) at each step but forbidden from dipping below the $y = 0$ axis.

For example, the following figure shows the 9 valid Motzkin paths from (0, 0) to (4, 0):



There are at least fourteen different manifestations of Motzkin numbers in different branches of mathematics, as enumerated by Donaghey and Shapiro in their 1977 survey of Motzkin numbers.

References

- Weisstein, Eric W., "Motzkin Number [2]" from MathWorld.
- Donaghey, R.; Shapiro, L. W. (1977), "Motzkin numbers", *Journal of Combinatorial Theory, Series A* **23** (3): 291–301, doi:10.1016/0097-3165(77)90020-6, MR0505544
- Motzkin, T. S. (1948), "Relations between hypersurface cross ratios, and a combinatorial formula for partitions of a polygon, for permanent preponderance, and for non-associative products", *Bulletin of the American Mathematical Society* **54**: 352–360, doi:10.1090/S0002-9904-1948-09002-4

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa001006
[2] http://mathworld.wolfram.com/MotzkinNumber.html

Newman–Shanks–Williams prime

In mathematics, a **Newman–Shanks–Williams prime (NSW prime)** is a prime number *p* which can be written in the form

$$S_{2m+1} = \frac{\left(1+\sqrt{2}\right)^{2m+1} + \left(1-\sqrt{2}\right)^{2m+1}}{2}.$$

NSW primes were first described by Morris Newman, Daniel Shanks and H. C. Williams in 1981 during the study of finite groups with square order.

The first few NSW primes are 7, 41, 239, 9369319, 63018038201, … (sequence A088165 [25] in OEIS), corresponding to the indices 3, 5, 7, 19, 29, … (A005850 [1]).

The sequence *S* alluded to in the formula can be described by the following recurrence relation:

$$S_0 = 1$$
$$S_1 = 1$$
$$S_n = 2S_{n-1} + S_{n-2} \qquad \text{for all } n \geq 2.$$

The first few terms of the sequence are 1, 1, 3, 7, 17, 41, 99, … (sequence A001333 [2] in OEIS). Each term in this sequence is half the corresponding term in the sequence of companion Pell numbers. These numbers also appear in the continued fraction convergents to √2.

Further reading

• Newman, M.; Shanks, D. & Williams, H. C. (1980), "Simple groups of square order and an interesting sequence of primes", *Acta Arithmetica* **38** (2): 129–140.

External links

• The Prime Glossary: NSW number [3]

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa005850
[2] http://en.wikipedia.org/wiki/Oeis%3Aa001333
[3] http://primes.utm.edu/glossary/page.php?sort=NSWNumber

Odd number

In mathematics, the **parity** of an object states whether it is even or odd.

This concept begins with integers. An **even number** is an integer that is "evenly divisible" by 2, i.e., divisible by 2 without remainder; an **odd number** is an integer that is not evenly divisible by 2. (The old-fashioned term "evenly divisible" is now almost always shortened to "divisible".) A formal definition of an odd number is that it is an integer of the form $n = 2k + 1$, where k is an integer. An even number has the form $n = 2k$ where k is an integer.

Examples of even numbers are −4, 8, and 1728. Examples of odd numbers are −5, 9, 3, and 71. This classification only applies to integers, i.e., a fractional number like 1/2 or 4.201 is neither even nor odd.

The sets of even and odd numbers can be defined as following:

- **Even** = $\{2k; \forall k \in \mathbb{Z}\}$
- **Odd** = $\{2k + 1; \forall k \in \mathbb{Z}\}$

A number (i.e., integer) expressed in the decimal numeral system is even or odd according to whether its last digit is even or odd. That is, if the last digit is 1, 3, 5, 7, or 9, then it's odd; otherwise it's even. The same idea will work using any even base. In particular, a number expressed in the binary numeral system is odd if its last digit is 1 and even if its last digit is 0. In an odd base, the number is even according to the sum of its digits – it is even if and only if the sum of its digits is even.

Arithmetic on even and odd numbers

The following laws can be verified using the properties of divisibility. They are a special case of rules in modular arithmetic, and are commonly used to check if an equality is likely to be correct by testing the parity of each side. As with ordinary arithmetic, multiplication and addition are commutative and associative, and multiplication is distibutive over addition. However, subtraction in parity is identical to addition, so subtraction also possesses these properties (which are absent from ordinary arithmetic).

Addition and subtraction

- even ± even = even;
- even ± odd = odd;
- odd ± odd = even;

Rules analogous to these for divisibility by 9 are used in the method of casting out nines.

Division

The division of two whole numbers does not necessarily result in a whole number. For example, 1 divided by 4 equals 1/4, which isn't even *or* odd, since the concepts even and odd apply only to integers. But when the quotient is an integer, it will be even if and only if the dividend has more factors of two than the divisor.

History

The ancient Greeks considered 1 to be neither fully odd nor fully even. Some of this sentiment survived into the 19th century: Friedrich Wilhelm August Fröbel's 1826 *The Education of Man* instructs the teacher to drill students with the claim that 1 is neither even nor odd, to which Fröbel attaches the philosophical afterthought,

> It is well to direct the pupil's attention here at once to a great far-reaching law of nature and of thought. It is this, that between two relatively different things or ideas there stands always a third, in a sort of balance, seeming to unite the two. Thus, there is here between odd and even numbers one number (one) which is neither of the two. Similarly, in form, the right angle stands between the acute and obtuse angles; and in language, the semi-vowels or aspirants between the mutes and vowels. A thoughtful teacher and a pupil taught to think for himself can scarcely help noticing this and other important laws.

Music theory

In wind instruments which are cylindrical and in effect closed at one end, such as the clarinet at the mouthpiece, the harmonics produced are odd multiples of the fundamental frequency. (With cylindrical pipes open at both ends, used for example in some organ stops such as the open diapason, the harmonics are even multiples of the same frequency, but this is the same as being all multiples of double the frequency and is usually perceived as such.) See harmonic series (music).

Higher mathematics

The even numbers form an ideal in the ring of integers, but the odd numbers do not — this is clear from the fact that the identity element for addition, zero, is an element of the even numbers only. An integer is even if it is congruent to 0 modulo this ideal, in other words if it is congruent to 0 modulo 2, and odd if it is congruent to 1 modulo 2.

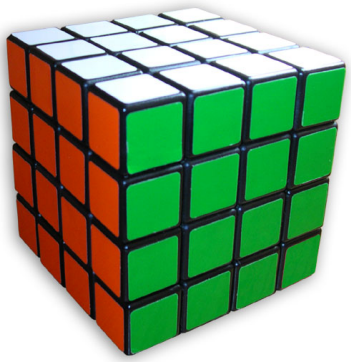
All prime numbers are odd, with one exception: the prime number 2. All known perfect numbers are even; it is unknown whether any odd perfect numbers exist.

The squares of all even numbers are even, and the squares of all odd numbers are odd. Since an even number can be expressed as 2x, $(2x)^2 = 4x^2$ which is even. Since an odd number can be expressed as 2x + 1, $(2x + 1)^2 = 4x^2 + 4x + 1$. $4x^2$ and 4x are even, which means that $4x^2 + 4x + 1$ is odd (since even + odd = odd).

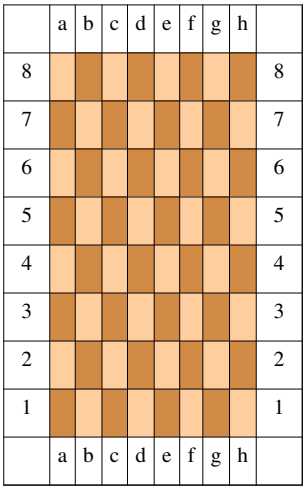
Goldbach's conjecture states that every even integer greater than 2 can be represented as a sum of two prime numbers. Modern computer calculations have shown this conjecture to be true for integers up to at least 4×10^{14}, but still no general proof has been found.

The Feit–Thompson theorem states that a finite group is always solvable if its order is an odd number. This is an example of odd numbers playing a role in an advanced mathematical theorem where the method of application of the simple hypothesis of "odd order" is far from obvious.

Parity for other objects



Rubik's Revenge in solved state



The two light bishops are confined to squares of opposite parity; the dark knight can only jump to squares of alternating parity.

Parity is also used to refer to a number of other properties.

- The parity of a permutation (as defined in abstract algebra) is the parity of the number of transpositions into which the permutation can be decomposed. For example (ABC) to (BCA) is even because it can be done by swapping A and B then C and A (two transpositions). It can be shown that no permutation can be decomposed both in an even and in an odd number of transpositions. Hence the above is a suitable definition. In Rubik's Revenge, Square-1, and other twisty puzzles, the moves of the puzzle allow only even permutations of the puzzle pieces, so parity is important in understanding the configuration space of these puzzles.
- The parity of a function describes how its values change when its arguments are exchanged with their negations. An even function, such as an even power of a variable, gives the same result for any argument as for its negation. An odd function, such as an odd power of a variable, gives for any argument the negation of its result when given the negation of that argument. It is possible for a function to be neither odd nor even, and for the case $f(x) = 0$, to be both odd and even.
- Integer coordinates of points in Euclidean spaces of two or more dimensions also have a parity, usually defined as the parity of the sum of the coordinates. For instance, the checkerboard lattice contains all integer points of even parity. This feature manifests itself in chess, as bishops are constrained to squares of the same parity; knights alternate parity between moves. This form of parity was famously used to solve the Mutilated chessboard problem.

Padovan sequence

The **Padovan sequence** is the sequence of integers $P(n)$ defined by the initial values

$$P(0) = P(1) = P(2) = 1,$$

and the recurrence relation

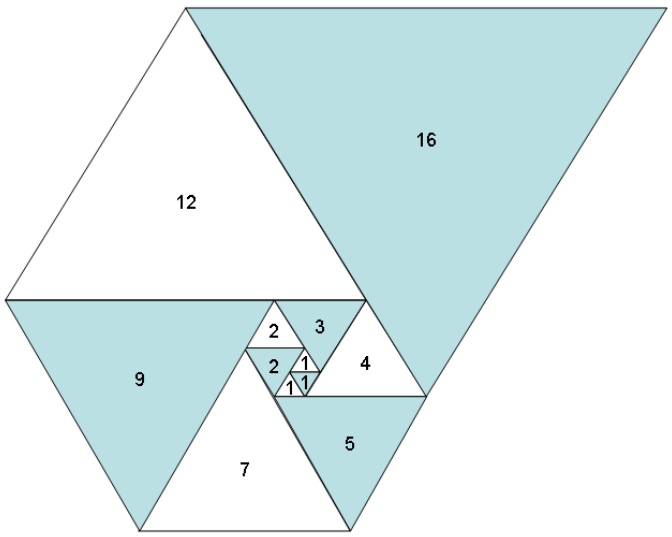
$$P(n) = P(n-2) + P(n-3).$$

The first few values of $P(n)$ are

1, 1, 1, 2, 2, 3, 4, 5, 7, 9, 12, 16, 21, 28, 37, 49, 65, 86, 114, 151, 200, 265, ... (sequence A000931 [1] in OEIS)

The Padovan sequence is named after Richard Padovan who attributed its discovery to Dutch architect Hans van der Laan in his 1994 essay *Dom. Hans van der Laan : Modern Primitive*. The sequence was described by Ian Stewart in his Scientific American column *Mathematical Recreations* in June 1996.

The above definition is the one given by Ian Stewart and by MathWorld. Other sources may start the sequence at a different place, in which case some of the identities in this article must be adjusted with appropriate offsets.



Spiral of equilateral triangles with side lengths which follow the Padovan sequence.

Recurrence relations

In the spiral, each triangle shares a side with two others giving a visual proof that the Padovan sequence also satisfies the recurrence relation

$$P(n) = P(n-1) + P(n-5)$$

Starting from this, the defining recurrence and other recurrences as they are discovered, one can create an infinite number of further recurrences by repeatedly replacing $P(m)$ by $P(m-2) + P(m-3)$

The Perrin sequence satisfies the same recurrence relations as the Padovan sequence, although it has different initial values. This is a property of recurrence relations.

The Perrin sequence can be obtained from the Padovan sequence by the following formula:

$$\mathrm{Perrin}(n) = P(n+1) + P(n-10).$$

Extension to negative parameters

As with any sequence defined by a recurrence relation, Padovan numers P(m) for m<0 can be defined by rewriting the recurrence relation as

$$P(n-3) = P(n-1) - P(n),$$

Starting with n=2 and working backwards. Extending $P(m)$ to negative indices gives the values

..., –7, 4, 0, –3, 4, –3, 1, 1, –2, 2, –1, 0, 1, –1, 1, 0, 0, 1, 0, 1, 1, 1, ...

Sums of terms

The sum of the first n terms in the Padovan sequence is 2 less than $P(n + 5)$ i.e.

$$\sum_{m=0}^{n} P(m) = P(n+5) - 2.$$

Sums of alternate terms, sums of every third term and sums of every fifth term are also related to other terms in the sequence:

$$\sum_{m=0}^{n} P(2m) = P(2n+3) - 1$$
$$\sum_{m=0}^{n} P(2m+1) = P(2n+4) - 1$$
$$\sum_{m=0}^{n} P(3m) = P(3n+2)$$
$$\sum_{m=0}^{n} P(3m+1) = P(3n+3) - 1$$
$$\sum_{m=0}^{n} P(3m+2) = P(3n+4) - 1$$
$$\sum_{m=0}^{n} P(5m) = P(5n+1).$$

Sums involving products of terms in the Padovan sequence satisfy the following identities:

$$\sum_{m=0}^{n} P(m)^2 = P(n+2)^2 - P(n-1)^2 - P(n-3)^2$$
$$\sum_{m=0}^{n} P(m)^2 P(m+1) = P(n)P(n+1)P(n+2)$$
$$\sum_{m=0}^{n} P(m)P(m+2) = P(n+2)P(n+3) - 1.$$

Other identities

The Padovan sequence also satisfies the identity

$$P(n)^2 - P(n+1)P(n-1) = P(-n-7).$$

The Padovan sequence is related to sums of binomial coefficients by the following identity:

$$\sum_{2m+n=k} \binom{m}{n} = P(k-2).$$

For example, for k = 12, the values for the pair (m, n) with $2m + n$ = 12 which give non-zero binomial coefficients are (6, 0), (5, 2) and (4, 4), and:

$$\binom{6}{0} + \binom{5}{2} + \binom{4}{4} = 1 + 10 + 1 = 12 = P(10).$$

Binet-like formula

The Padovan sequence numbers can be written in terms of powers of the roots of the equation

$$x^3 - x - 1 = 0.$$

This equation has 3 roots; one real root p (known as the plastic number) and two complex conjugate roots q and r. Given these three roots, the Padovan sequence can be expressed by a formula involving p,q and r:

$$P(n) = ap^n + bq^n + cr^n$$

where a, b and c are constants.

Since the magnitudes of the complex roots q and r are both less than 1 (and hence p is a Pisot–Vijayaraghavan number), the powers of these roots approach 0 for large n, and $P(n) - ap^n$ tends to zero.

For all $n \geq 0$, P(n) is the integer closest to $\frac{p^{n-1}}{s}$, where $s = p/a$ = 1.0453567932525329623... is the only real root of $s^3 - 2s^2 + 23s - 23 = 0$. The ratio of successive terms in the Padovan sequence approaches p, which has a value of approximately 1.324718. This constant bears the same relationship to the Padovan sequence and the Perrin sequence as the golden ratio does to the Fibonacci sequence.

Combinatorial interpretations

- $P(n)$ is the number of ways of writing $n + 2$ as an ordered sum in which each term is either 2 or 3 (i.e. the number of compositions of $n + 2$ in which each term is either 2 or 3). For example, $P(6) = 4$, and there are 4 ways to write 8 as an ordered sum of 2s and 3s:

  2 + 2 + 2 + 2 ; 2 + 3 + 3 ; 3 + 2 + 3 ; 3 + 3 + 2

- The number of ways of writing n as an ordered sum in which no term is 2 is $P(2n - 2)$. For example, $P(6) = 4$, and there are 4 ways to write 4 as an ordered sum in which no term is 2:

  4 ; 1 + 3 ; 3 + 1 ; 1 + 1 + 1 + 1

- The number of ways of writing n as a palindromic ordered sum in which no term is 2 is $P(n)$. For example, $P(6) = 4$, and there are 4 ways to write 6 as a palindromic ordered sum in which no term is 2:

  6 ; 3 + 3 ; 1 + 4 + 1 ; 1 + 1 + 1 + 1 + 1 + 1

- The number of ways of writing n as an ordered sum in which each term is congruent to 2 mod 3 is equal to $P(n - 4)$. For example, $P(6) = 4$, and there are 4 ways to write 10 as an ordered sum in which each term is congruent to 2 mod 3:

  8 + 2 ; 2 + 8 ; 5 + 5 ; 2 + 2 + 2 + 2 + 2

Generating function

The generating function of the Padovan sequence is

$$G(P(n);x) = \frac{1+x}{1-x^2-x^3}.$$

This can be used to prove identities involving products of the Padovan sequence with geometric terms, such as:

$$\sum_{n=0}^{\infty} \frac{P(n)}{2^n} = \frac{12}{5}.$$

Generalizations

In a similar way to the Fibonacci numbers that can be generalized to a set of polynomials called the Fibonacci polynomials, the Padovan sequence numbers can be generalized to yield the Padovan polynomials.

Padovan prime

A **Padovan prime** is $P(n)$ that is prime. The first few Padovan primes A100891 [26] are

2, 3, 5, 7, 37, 151, 3329, 23833, ...

Padovan L-system

If we define the following simple grammar:

variables : A B C

constants : none

start : A

rules : (A → B), (B → C), (C → AB)

then this Lindenmayer system or L-system produces the following sequence of strings:

n = 0 : A

n = 1 : B

n = 2 : C

n = 3 : AB

n = 4 : BC

n = 5 : CAB

n = 6 : ABBC

n = 7 : BCCAB

n = 8 : CABABBC

and if we count the length of each string, we obtain the Padovan sequence of numbers:

1 1 1 2 2 3 4 5 ...

Also, if you count the number of *A*s, *B*s and *C*s in each string, then for the nth string, you have $P(n-5)$ *A*s, $P(n-3)$ *B*s and $P(n-4)$ *C*s. The count of *BB* pairs, *AA* pairs and *CC* pairs are also Padovan numbers.

Padovan Cuboid Spiral

A spiral can be formed based on connecting the corners of a set of 3 dimensional cuboids. This is the Padovan cuboid spiral. Successive sides of this spiral have lengths that are the Padovan sequence numbers multiplied by the square root of 2.

External links

- Padovan sequence: A000931 [1] in the OEIS
- Weisstein, Eric W., "Padovan Sequence [2]" from MathWorld.
- *Dom Hans Van Der Laan And The Plastic Number* [3] by Richard Padovan
- *Tales of a Neglected Number* [4] by Ian Stewart
- A Padovan Sequence Calculator can be found here. [5]

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa000931
[2] http://mathworld.wolfram.com/PadovanSequence.html
[3] http://www.nexusjournal.com/conferences/N2002-Padovan.html
[4] http://members.fortunecity.com/templarser/padovan.html
[5] http://www.plenilune.pwp.blueyonder.co.uk/fibonacci-calculator.asp

Palindromic prime

A **palindromic prime** (sometimes called a **palprime**) is a prime number that is also a palindromic number. Palindromicity depends on the base of the numbering system and its writing conventions, while primality is independent of such concerns. The first few decimal palindromic primes (sequence A002385 [27] in OEIS) are:

> 2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929, 10301, 10501, 10601, 11311, …

Except for 11, all palindromic primes have an odd number of digits, because the divisibility test for 11 tells us that every palindromic number with an even number of digits is a multiple of 11. It is not known if there are infinitely many palindromic primes in base 10. The largest known as of September 2010 is $10^{200000} + 47960506974 \times 10^{99995} + 1$, found by Bernardo Boncompagni.[1]

On the other hand, it is known that, for any base, almost all palindromic numbers are composite (Banks et al. [2]).

In binary, the palindromic primes include the Mersenne primes and the Fermat primes. All binary palindromic primes except binary 11 (decimal 3) have an odd number of digits; those palindromes with an even number of digits are divisible by 3. The sequence of binary palindromic primes (A117697 [3], A016041 [4]) begins:

binary:	11,	101,	111,	10001,	11111,	1001001,	1101011,	1111111,	100000001,	100111001,	110111011,	10010101001, …
decimal:	3,	5,	7,	17,	31,	73,	107,	127,	257,	313,	443,	1193, …

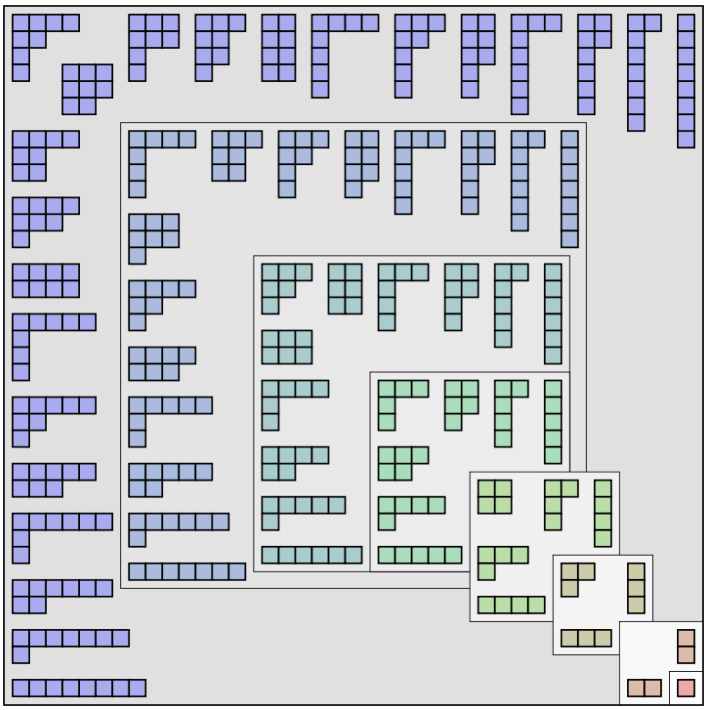
Ribenboim defines a **triply palindromic prime** as a prime p for which: p is a palindromic prime with q digits, where q is a palindromic prime with r digits, where r is also a palindromic prime.[5] For example, $p = 10^{11310} + 4661664 \times 10^{5652} + 1$, which has $q = 11311$ digits, and 11311 has $r = 5$ digits. The first (base-10) triply-palindromic prime is the 11-digit 10000500001. It's possible that a triply palindromic prime in base 10 may also be palindromic in another base, such as base 2, but it would be highly remarkable if it were also a triply palindromic prime in that base as well.

References

[1] Chris Caldwell, *The Top Twenty: Palindrome* (http://primes.utm.edu/top20/page.php?id=53)
[2] http://www.esi.ac.at/preprints/esi1456.pdf
[3] http://en.wikipedia.org/wiki/Oeis%3Aa117697
[4] http://en.wikipedia.org/wiki/Oeis%3Aa016041
[5] Paulo Ribenboim, *The New Book of Prime Number Records*

Partition (number theory)

In number theory, a **partition** of a positive integer n, also called an **integer partition**, is a way of writing n as a sum of positive integers. Two sums that differ only in the order of their summands are considered to be the same partition; if order matters then the sum becomes a composition. A summand in a partition is also called a **part**. The number of partitions of n is given by the partition function $p(n)$.



Ferrers diagrams showing the partitions of positive integers 1 through 8. They are so arranged that images under the reflection about the main diagonal of the square are conjugate partitions.

Examples

The partitions of 4 are listed below:

1. 4
2. 3 + 1
3. 2 + 2
4. 2 + 1 + 1
5. 1 + 1 + 1 + 1

The partitions of 8 are listed below:

1. 8
2. 7 + 1
3. 6 + 2
4. 6 + 1 + 1
5. 5 + 3
6. 5 + 2 + 1
7. 5 + 1 + 1 + 1
8. 4 + 4
9. 4 + 3 + 1
10. 4 + 2 + 2
11. 4 + 2 + 1 + 1
12. 4 + 1 + 1 + 1 + 1
13. 3 + 3 + 2
14. 3 + 3 + 1 + 1
15. 3 + 2 + 2 + 1
16. 3 + 2 + 1 + 1 + 1
17. 3 + 1 + 1 + 1 + 1 + 1

18. 2 + 2 + 2 + 2
19. 2 + 2 + 2 + 1 + 1
20. 2 + 2 + 1 + 1 + 1 + 1
21. 2 + 1 + 1 + 1 + 1 + 1 + 1
22. 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1

Partition function

In number theory, the **partition function** $p(n)$ represents the number of possible partitions of a natural number n, which is to say the number of distinct (and order independent) ways of representing n as a sum of natural numbers. For example, 4 can be partitioned in five distinct ways:

4, 3 + 1, 2 + 2, 2 + 1 + 1, 1 + 1 + 1 + 1.

The order dependent composition 1 + 3 is the same partition as 3 + 1, while 1 + 2 + 1 and 1 + 1 + 2 are the same partition as 2 + 1 + 1.

So $p(4) = 5$. By convention $p(0) = 1$, $p(n) = 0$ for n negative. Partitions can be graphically visualized with Young diagrams. They occur in a number of branches of mathematics and physics, including the study of symmetric polynomials, the symmetric group and in group representation theory in general.

Intermediate function

One way of getting a handle on the partition function involves an intermediate function $p(k, n)$, which represents the number of partitions of n using only natural numbers at least as large as k. For any given value of k, partitions counted by $p(k, n)$ fit into exactly one of the following categories:

1. smallest addend is k
2. smallest addend is strictly greater than k.

The number of partitions meeting the first condition is $p(k, n - k)$. To see this, imagine a list of all the partitions of the number $n - k$ into numbers of size at least k, then imagine appending "+ k" to each partition in the list. Now what is it a list of? As a side note, one can use this to define a sort of recursion relation for the partition function in term of the intermediate function, namely

$$1 + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} p(k, n-k) = p(n),$$

where $\lfloor n \rfloor$ is the floor function.

The number of partitions meeting the second condition is $p(k + 1, n)$ since a partition into parts of at least k that contains no parts of exactly k must have all parts at least $k + 1$.

Since the two conditions are mutually exclusive, the number of partitions meeting either condition is $p(k + 1, n) + p(k, n - k)$. The recursively defined function is thus:

- $p(k, n) = 0$ if $k > n$
- $p(k, n) = 1$ if $k = n$
- $p(k, n) = p(k+1, n) + p(k, n - k)$ otherwise.

This function tends to exhibit deceptive behavior.

$p(1, 4) = 5$

$p(2, 8) = 7$

$p(3, 12) = 9$

$p(4, 16) = 11$

$p(5, 20) = 13$

$p(6, 24) = \mathbf{16}$

Our original function $p(n)$ is just $p(1, n)$.

The values of this function:

		k									
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
n	**1**	1	0	0	0	0	0	0	0	0	0
	2	2	1	0	0	0	0	0	0	0	0
	3	3	1	1	0	0	0	0	0	0	0
	4	5	2	1	1	0	0	0	0	0	0
	5	7	2	1	1	1	0	0	0	0	0
	6	11	4	2	1	1	1	0	0	0	0
	7	15	4	2	1	1	1	1	0	0	0
	8	22	7	3	2	1	1	1	1	0	0
	9	30	8	4	2	1	1	1	1	1	0
	10	42	12	5	3	2	1	1	1	1	1

Generating function

A generating function for $p(n)$ is given by the reciprocal of Euler's function:

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} \left(\frac{1}{1-x^k}\right).$$

Expanding each term on the right-hand side as a geometric series, we can rewrite it as

$$(1 + x + x^2 + x^3 + ...)(1 + x^2 + x^4 + x^6 + ...)(1 + x^3 + x^6 + x^9 + ...) ....$$

The x^n term in this product counts the number of ways to write

$$n = a_1 + 2a_2 + 3a_3 + ... = (1 + 1 + ... + 1) + (2 + 2 + ... + 2) + (3 + 3 + ... + 3) + ...,$$

where each number i appears a_i times. This is precisely the definition of a partition of n, so our product is the desired generating function. More generally, the generating function for the partitions of n into numbers from a set A can be found by taking only those terms in the product where k is an element of A. This result is due to Euler.

The formulation of Euler's generating function is a special case of a q-Pochhammer symbol and is similar to the product formulation of many modular forms, and specifically the Dedekind eta function. It can also be used in conjunction with the pentagonal number theorem to derive a recurrence for the partition function stating that:

$$p(k) = p(k - 1) + p(k - 2) - p(k - 5) - p(k - 7) + p(k - 12) + p(k - 15) - p(k - 22) - ...$$

where the sum is taken over all generalized pentagonal numbers of the form $\frac{1}{2}n(3n - 1)$, for n running over positive and negative integers: successively taking $n = 1, -1, 2, -2, 3, -3, 4, -4$ ..., generates the values 1, 2, 5, 7, 12, 15, 22, 26, 35, 40, 51, ... The signs in the summation continue to alternate +, +, −, −, +, +, ...

Table of values

Some values of the partition function are as follows (sequence A000041 [1] in OEIS):

- $p(1) = 1$
- $p(2) = 2$
- $p(3) = 3$
- $p(4) = 5$
- $p(5) = 7$
- $p(6) = 11$
- $p(7) = 15$
- $p(8) = 22$
- $p(9) = 30$
- $p(10) = 42$
- $p(100) = 190{,}569{,}292$
- $p(200) = 3{,}972{,}999{,}029{,}388$
- $p(1000) = 24{,}061{,}467{,}864{,}032{,}622{,}473{,}692{,}149{,}727{,}991 \approx 2.4 \times 10^{31}$.

As of February 2010, the largest known prime number of this kind is $p(29099391)$, with 6002 decimal digits.[2]

Asymptotic behaviour

An asymptotic expression for $p(n)$ is given by

$$p(n) \sim \frac{\exp\left(\pi\sqrt{2n/3}\right)}{4n\sqrt{3}} \text{ as } n \to \infty.$$

This asymptotic formula was first obtained by G. H. Hardy and Ramanujan in 1918 and independently by J. V. Uspensky in 1920. Considering $p(1000)$, the asymptotic formula gives about 2.4402×10^{31}, reasonably close to the exact answer given above.

In 1937, Hans Rademacher was able to improve on Hardy and Ramanujan's results by providing a convergent series expression for $p(n)$. It is

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n)\, \sqrt{k}\, \frac{d}{dn} \left(\frac{\sinh\left(\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)}{\sqrt{n-\frac{1}{24}}} \right)$$

where

$$A_k(n) = \sum_{0 \le m < k\,;\,(m,k)=1} e^{\{\pi i[s(m,k)-2nm/k]\}}.$$

Here, the notation $(m, n) = 1$ implies that the sum should occur only over the values of m that are relatively prime to n. The function $s(m, k)$ is a Dedekind sum. The proof of Rademacher's formula is interesting in that it involves Ford circles, Farey sequences, modular symmetry and the Dedekind eta function in a central way.

Congruences

Srinivasa Ramanujan is credited with discovering that "congruences" in the number of partitions exist for integers ending in 4 and 9.

$$p(5k+4) \equiv 0 \pmod 5$$

For instance, the number of partitions for the integer 4 is 5. For the integer 9, the number of partitions is 30; for 14 there are 135 partitions. He also discovered congruences related to 7 and 11:

$$p(7k+5) \equiv 0 \pmod 7$$
$$p(11k+6) \equiv 0 \pmod{11}.$$

Since 5, 7, and 11 are consecutive primes, one might think that there would be such a congruence for the next prime 13, $p(13k+a) \equiv 0 \pmod{13}$ for some *a*. This is, however, false. It can also be shown that there is no congruence of the form $p(bk+a) \equiv 0 \pmod b$ for any prime *b* other than 5, 7, or 11.

In the 1960s, A. O. L. Atkin of the University of Illinois at Chicago discovered additional congruences for small prime moduli. For example:

$$p(17303k+237) \equiv 0 \pmod{13}.$$

In 2000, Ken Ono of the University of Wisconsin–Madison proved that there are such congruences for every prime modulus. A few years later Ono, together with Scott Ahlgren of the University of Illinois, proved that there are partition congruences modulo every integer coprime to 6.[3]

Restricted partitions

Among the 22 partitions for the number 8, 6 contain only *odd parts*:

- 7 + 1
- 5 + 3
- 5 + 1 + 1 + 1
- 3 + 3 + 1 + 1
- 3 + 1 + 1 + 1 + 1 + 1
- 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1

If we count the partitions of 8 with *distinct parts*, we also obtain the number 6:

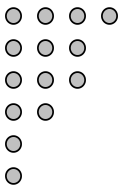
- 8
- 7 + 1
- 6 + 2
- 5 + 3
- 5 + 2 + 1
- 4 + 3 + 1

It is true for all positive numbers that the number of partitions with odd parts always equals the number of partitions with distinct parts. This result was proved by Leonard Euler in 1748.[4]

Some similar results about restricted partitions can be obtained by the aid of a visual tool, a **Ferrers graph** (also called **Ferrers diagram**, since it is not a *graph* in the graph-theoretical sense, or sometimes **Young diagram**, alluding to the Young tableau).

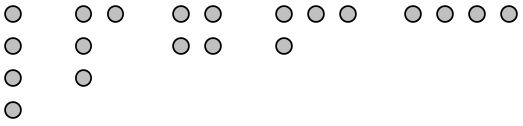
Ferrers diagram

The partition 6 + 4 + 3 + 1 of the positive number 14 can be represented by the following diagram; these diagrams are named in honor of Norman Macleod Ferrers:



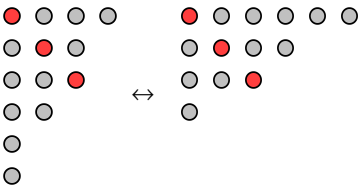
6+4+3+1

The 14 circles are lined up in 4 columns, each having the size of a part of the partition. The diagrams for the 5 partitions of the number 4 are listed below:



4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1

If we now flip the diagram of the partition 6 + 4 + 3 + 1 along its main diagonal, we obtain another partition of 14:

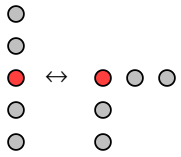


6+4+3+1 = 4+3+3+2+1+1

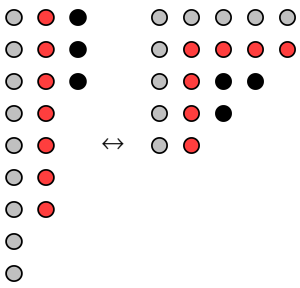
By turning the rows into columns, we obtain the partition 4 + 3 + 3 + 2 + 1 + 1 of the number 14. Such partitions are said to be *conjugate* of one another. In the case of the number 4, partitions 4 and 1 + 1 + 1 + 1 are conjugate pairs, and partitions 3 + 1 and 2 + 1 + 1 are conjugate of each other. Of particular interest is the partition 2 + 2, which has itself as conjugate. Such a partition is said to be *self-conjugate*.

Claim: The number of self-conjugate partitions is the same as the number of partitions with distinct odd parts.

Proof (sketch): The crucial observation is that every odd part can be "*folded*" in the middle to form a self-conjugate diagram:



One can then obtain a bijection between the set of partitions with distinct odd parts and the set of self-conjugate partitions, as illustrated by the following example:



Similar techniques can be employed to establish, for example, the following equalities:

- The number of partitions of n into no more than k parts is the same as the number of partitions of n into parts no larger than k.
- The number of partitions of n into no more than k parts is the same as the number of partitions of $n + k$ into exactly k parts.

See also

- Young's lattice
- Dominance order
- Partition of a set
- Plane partition
- Polite number, defined by partitions into consecutive integers
- Multiplicative partition
- Twelvefold way
- Ewens's sampling formula
- Faà di Bruno's formula
- Multiset
- Newton's identities
- Leibniz's distribution table for integer partitions
- Durfee square

Notes

[1] http://en.wikipedia.org/wiki/Oeis%3Aa000041

[2] http://primes.utm.edu/top20/page.php?id=54

[3] One, Ken; Ahlgren, Scott (2001). "Congruence properties for the partition function" (http://www.math.wisc.edu/~ono/reprints/061.pdf). *Proceedings of the National Academy of Sciences* **98** (23): 12882–12884. doi:10.1073/pnas.191488598. .

[4] Andrews, George E. *Number Theory*. W. B. Saunders Company, Philadelphia, 1971. Dover edition, page 149–150.

References

- George E. Andrews, *The Theory of Partitions* (1976), Cambridge University Press. *ISBN 0-521-63766-X* .
- Tom M. Apostol, *Modular functions and Dirichlet Series in Number Theory* (1990), Springer-Verlag, New York. ISBN 0-387-97127-0 *(See chapter 5 for a modern pedagogical intro to Rademacher's formula).*
- Sautoy, Marcus Du. The Music of the Primes. New York: Perennial-HarperCollins, 2003.
- D. H. Lehmer, *On the remainder and convergence of the series for the partition function* Trans. Amer. Math. Soc. **46**(1939) pp 362–373. *(Provides the main formula (no derivatives), remainder, and older form for $A_k(n)$.)*

- Gupta, Gwyther, Miller, *Roy. Soc. Math. Tables, vol 4, Tables of partitions*, (1962) *(Has text, nearly complete bibliography, but they (and Abramowitz) missed the Selberg formula for $A_k(n)$, which is in Whiteman.)*
- Ian G. Macdonald, *Symmetric functions and Hall polynomials*, Oxford University Press, 1979, ISBN 0-19-853530-9 (See section I.1)
- Ken Ono, *Distribution of the partition function modulo m*, Annals of Mathematics **151** (2000) pp 293–307. *(This paper proves congruences modulo every prime greater than 3)*
- Richard P. Stanley, *Enumerative Combinatorics*, Volumes 1 and 2 (http://www-math.mit.edu/~rstan/ec/). Cambridge University Press, 1999 ISBN 0-521-56069-1
- A. L. Whiteman, *A sum connected with the series for the partition function* (http://projecteuclid.org/Dienst/UI/1.0/Summarize/euclid.pjm/1103044252), Pacific Journal of Math. **6**:1 (1956) 159–176. *(Provides the Selberg formula. The older form is the finite Fourier expansion of Selberg.)*
- Hans Rademacher, *Collected Papers of Hans Rademacher*, (1974) MIT Press; v II, p 100–107, 108–122, 460–475.
- Miklós Bóna (2002). *A Walk Through Combinatorics: An Introduction to Enumeration and Graph Theory*. World Scientific Publishing. ISBN 981-02-4900-4. (qn elementary introduction to the topic of integer partition, including a discussion of Ferrers graphs)
- George E. Andrews, Kimmo Eriksson (2004). *Integer Partitions*. Cambridge University Press. ISBN 0-521-60090-1.
- 'A Disappearing Number', devised piece by Complicite, mention Ramanujan's work on the Partition Function, 2007

External links

- Partition and composition calculator (http://www.btinternet.com/~se16/js/partitions.htm)
- First 4096 values of the partition function (http://www.numericana.com/data/partition.htm)
- An algorithm to compute the partition function (http://www.numericana.com/answer/numbers.htm#partitions)
- Weisstein, Eric W., " Partition (http://mathworld.wolfram.com/Partition.html)" from MathWorld.
- Weisstein, Eric W., " Partition Function P (http://mathworld.wolfram.com/PartitionFunctionP.html)" from MathWorld.
- Pieces of Number (http://www.sciencenews.org/articles/20050618/bob9.asp) from Science News Online
- Lectures on Integer Partitions (http://www.math.upenn.edu/~wilf/PIMS/PIMSLectures.pdf) by Herbert S. Wilf
- Counting with partitions (http://www.luschny.de/math/seq/CountingWithPartitions.html) with reference tables to the On-Line Encyclopedia of Integer Sequences
- Integer::Partition Perl module (http://search.cpan.org/perldoc?Integer::Partition) from CPAN
- Fast Algorithms For Generating Integer Partitions (http://www.site.uottawa.ca/~ivan/F49-int-part.pdf)
- Generating All Partitions: A Comparison Of Two Encodings (http://arxiv.org/abs/0909.2331)

Pell number

In mathematics, the **Pell numbers** are an infinite sequence of integers that have been known since ancient times, the denominators of the closest rational approximations to the square root of 2. This sequence of approximations begins 1/1, 3/2, 7/5, 17/12, and 41/29, so the sequence of Pell numbers begins with 1, 2, 5, 12, and 29. The numerators of the same sequence of approximations are half the **companion Pell numbers** or **Pell-Lucas numbers**; these numbers form a second infinite sequence that begins with 2, 6, 14, 34, and 82.

Both the Pell numbers and the companion Pell numbers may be calculated by means of a recurrence relation similar to that for the Fibonacci numbers, and both sequences of numbers grow exponentially, proportionally to powers of the silver ratio $1 + \sqrt{2}$. As well as being used to approximate the square root of two, Pell numbers can be used to find square triangular numbers, to construct integer approximations to the right isosceles triangle, and to solve certain combinatorial enumeration problems.[1]

As with Pell's equation, the name of the Pell numbers stems from Leonhard Euler's mistaken attribution of the equation and the numbers derived from it to John Pell. The Pell-Lucas numbers are also named after Edouard Lucas, who studied sequences defined by recurrences of this type; the Pell and companion Pell numbers are Lucas sequences.

Pell numbers

The Pell numbers are defined by the recurrence relation

$$P_n = \begin{cases} 0 & \text{if } n = 0; \\ 1 & \text{if } n = 1; \\ 2P_{n-1} + P_{n-2} & \text{otherwise.} \end{cases}$$

In words, the sequence of Pell numbers starts with 0 and 1, and then each Pell number is the sum of twice the previous Pell number and the Pell number before that. The first few terms of the sequence are

0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378... (sequence A000129 [2] in OEIS).

The Pell numbers can also be expressed by the closed form formula

$$P_n = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}.$$

For large values of *n*, the $(1+\sqrt{2})^n$ term dominates this expression, so the Pell numbers are approximately proportional to powers of the silver ratio $(1+\sqrt{2})$, analogous to the growth rate of Fibonacci numbers as powers of the golden ratio.

A third definition is possible, from the matrix formula

$$\begin{pmatrix} P_{n+1} & P_n \\ P_n & P_{n-1} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^n.$$

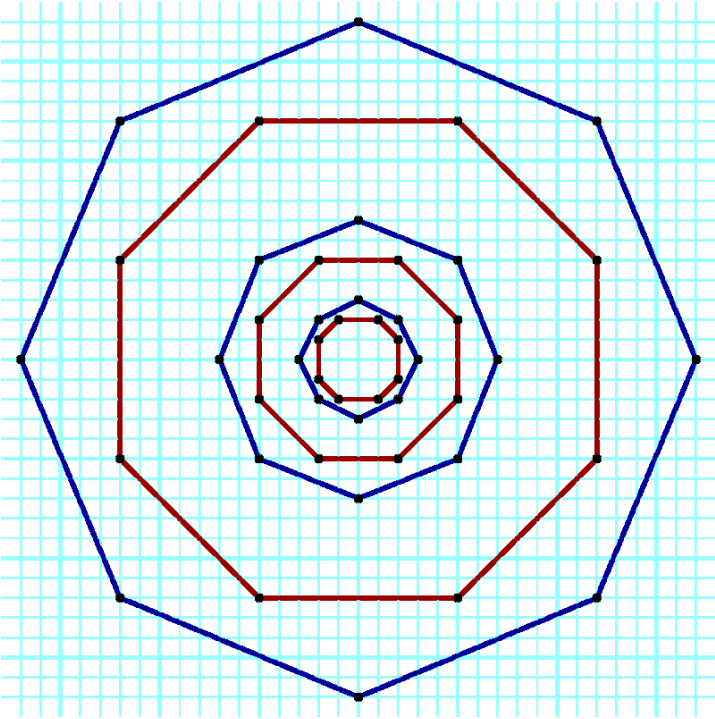
Many identities can be derived or proven from these definitions; for instance an identity analogous to Cassini's identity for Fibonacci numbers,

$$P_{n+1}P_{n-1} - P_n^2 = (-1)^n,$$

is an immediate consequence of the matrix formula (found by considering the determinants of the matrices on the left and right sides of the matrix formula).[3]

Approximation to the square root of two

Pell numbers arise historically and most notably in the rational approximation to the square root of 2. If two large integers *x* and *y* form a solution to the Pell equation



Rational approximations to regular octagons, with coordinates derived from the Pell numbers.

$$x^2 - 2y^2 = \pm 1,$$

then their ratio $\frac{x}{y}$ provides a close approximation to $\sqrt{2}$. The sequence of approximations of this form is

$$1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \dots$$

where the denominator of each fraction is a Pell number and the numerator is the sum of a Pell number and its predecessor in the sequence. That is, the solutions have the form $\frac{P_{n-1}+P_n}{P_n}$. The approximation

$$\sqrt{2} \approx \frac{577}{408}$$

of this type was known to Indian mathematicians in the third or fourth century B.C.[4] The Greek mathematicians of the fifth century B.C. also knew of this sequence of approximations;[5] they called the denominators and numerators of this sequence **side and diameter numbers** and the numerators were also known as **rational diagonals** or **rational diameters**.[6]

These approximations can be derived from the continued fraction expansion of $\sqrt{2}$:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}}.$$

Truncating this expansion to any number of terms produces one of the Pell-number-based approximations in this sequence; for instance,

$$\frac{577}{408} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2}}}}}}}.$$

As Knuth (1994) describes, the fact that Pell numbers approximate $\sqrt{2}$ allows them to be used for accurate rational approximations to a regular octagon with vertex coordinates $(\pm P_i, \pm P_{i+1})$ and $(\pm P_{i+1}, \pm P_i)$. All vertices are equally distant from the origin, and form nearly uniform angles around the origin. Alternatively, the points $(\pm(P_i + P_{i-1}), 0)$, $(0, \pm(P_i + P_{i-1}))$, and $(\pm P_i, \pm P_i)$ form approximate octagons in which the vertices are nearly equally distant from the origin and form uniform angles.

Primes and squares

A **Pell prime** is a Pell number that is prime. The first few Pell primes are

2, 5, 29, 5741, ... (sequence A086383 [29] in OEIS).

As with the Fibonacci numbers, a Pell number P_n can only be prime if *n* itself is prime.

The only Pell numbers that are squares, cubes, or any higher power of an integer are 0, 1, and 169 = 13^2.[7]

However, despite having so few squares or other powers, Pell numbers have a close connection to square triangular numbers.[8] Specifically, these numbers arise from the following identity of Pell numbers:

$$\left((P_{k-1} + P_k) \cdot P_k\right)^2 = \frac{(P_{k-1} + P_k)^2 \cdot \left((P_{k-1} + P_k)^2 - (-1)^k\right)}{2}.$$

The left side of this identity describes a square number, while the right side describes a triangular number, so the result is a square triangular number.

Santana and Diaz-Barrero (2006) prove another identity relating Pell numbers to squares and showing that the sum of the Pell numbers up to P_{4n+1} is always a square:

$$\sum_{i=0}^{4n+1} P_i = \left(\sum_{r=0}^{n} 2^r \binom{2n+1}{2r}\right)^2 = (P_{2n} + P_{2n+1})^2.$$

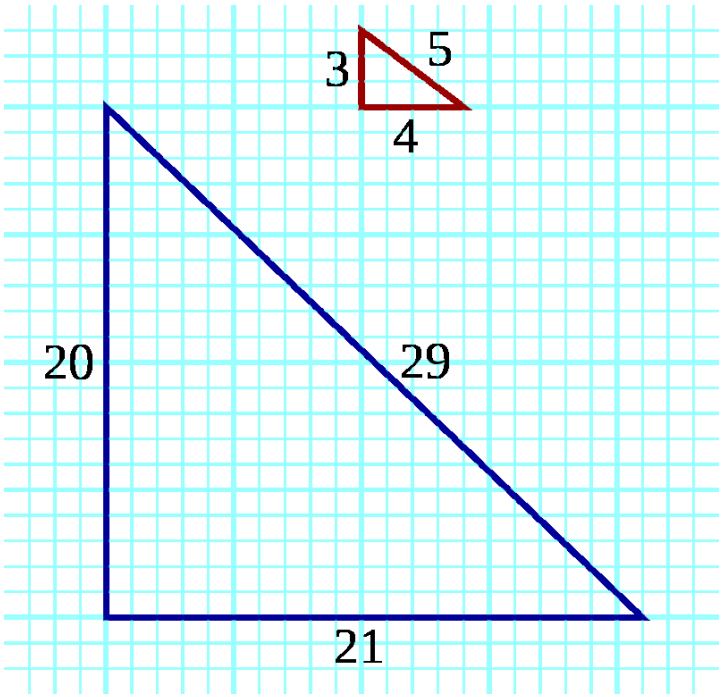
For instance, the sum of the Pell numbers up to P_5, $0 + 1 + 2 + 5 + 12 + 29 = 49$, is the square of $P_2 + P_3 = 2 + 5 = 7$. The numbers $P_{2n} + P_{2n+1}$ forming the square roots of these sums,

1, 7, 41, 239, 1393, 8119, 47321, ... (sequence A002315 [9] in OEIS),

are known as the Newman–Shanks–Williams (NSW) numbers.

Pythagorean triples

If a right triangle has integer side lengths *a*, *b*, *c* (necessarily satisfying the Pythagorean theorem $a^2+b^2=c^2$), then (*a*,*b*,*c*) is known as a Pythagorean triple. As Martin (1875) describes, the Pell numbers can be used to form Pythagorean triples in which *a* and *b* are one unit apart, corresponding to right triangles that are nearly isosceles. Each such triple has the form



Integer right triangles with nearly equal legs, derived from the Pell numbers.

$$(2P_nP_{n+1}, P_{n+1}^2 - P_n^2, P_{n+1}^2 + P_n^2 = P_{2n+1}).$$

The sequence of Pythagorean triples formed in this way is

(4,3,5), (20,21,29), (120,119,169), (696,697,985), ...

Pell-Lucas numbers

The **companion Pell numbers** or **Pell-Lucas numbers** are defined by the recurrence relation

$$Q_n = \begin{cases} 2 & \text{if } n = 0; \\ 2 & \text{if } n = 1; \\ 2Q_{n-1} + Q_{n-2} & \text{otherwise.} \end{cases}$$

In words: the first two numbers in the sequence are both 2, and each successive number is formed by adding twice the previous Pell-Lucas number to the Pell-Lucas number before that, or equivalently, by adding the next Pell number to the previous Pell number: thus, 82 is the companion to 29, and 82 = 2 * 34 + 14 = 70 + 12. T he first few terms of the sequence are (sequence A002203 [10] in OEIS): 2, 2, 6, 14, 34, 82, 198, 478...

The companion Pell numbers can be expressed by the closed form formula

$$Q_n = (1+\sqrt{2})^n + (1-\sqrt{2})^n.$$

These numbers are all even; each such number is twice the numerator in one of the rational approximations to $\sqrt{2}$ discussed above.

Computations and connections

The following table gives the first few powers of the silver ratio $\delta = \delta_S = 1 + \sqrt{2}$and its conjugate $\bar{\delta} = 1 - \sqrt{2}$.

n	$(1+\sqrt{2})^n$	$(1-\sqrt{2})^n$
0	$1 + 0\sqrt{2} = 1.0$	$1 - 0\sqrt{2} = 1.0$
1	$1 + 1\sqrt{2} = 2.41421\ldots$	$1 - 1\sqrt{2} = -0.41421\ldots$
2	$3 + 2\sqrt{2} = 5.82842\ldots$	$3 - 2\sqrt{2} = 0.17157\ldots$
3	$7 + 5\sqrt{2} = 14.07106\ldots$	$7 - 5\sqrt{2} = -0.07106\ldots$
4	$17 + 12\sqrt{2} = 33.97056\ldots$	$17 - 12\sqrt{2} = 0.02943\ldots$
5	$41 + 29\sqrt{2} = 82.01219\ldots$	$41 - 29\sqrt{2} = -0.01219\ldots$
6	$99 + 70\sqrt{2} = 197.9949\ldots$	$99 - 70\sqrt{2} = 0.0050\ldots$
7	$239 + 169\sqrt{2} = 478.00209\ldots$	$239 - 169\sqrt{2} = -0.00209\ldots$
8	$577 + 408\sqrt{2} = 1153.99913\ldots$	$577 - 408\sqrt{2} = 0.00086\ldots$
9	$1393 + 985\sqrt{2} = 2786.00035\ldots$	$1393 - 985\sqrt{2} = -0.00035\ldots$
10	$3363 + 2378\sqrt{2} = 6725.99985\ldots$	$3363 - 2378\sqrt{2} = 0.00014\ldots$
11	$8119 + 5741\sqrt{2} = 16238.00006\ldots$	$8119 - 5741\sqrt{2} = -0.00006\ldots$
12	$19601 + 13860\sqrt{2} = 39201.99997\ldots$	$19601 - 13860\sqrt{2} = 0.00002\ldots$

The coefficients are the Half companion Pell numbers H_n and The Pell numbers P_n which are the (non-negative) solutions to $H^2 - 2P^2 = \pm 1$. A Square triangular number is a number $N = \dfrac{t(t+1)}{2} = s^2$which is both the t th triangular number and the s th square number. A *near isosceles Pythagorean triple* is an integer solution to $a^2 + b^2 = c^2$where $a + 1 = b$.

The next table shows that splitting the odd number H_n into nearly equal halves gives a square triangular number when n is even and a near isosceles Pythagorean triple when n is odd. All solutions arise in this manner.

n	H_n	P_n	**t**	**t+1**	**s**	a	b	c
0	1	0	0	0	0			
1	1	1				0	1	1
2	3	2	1	2	1			
3	7	5				3	4	5
4	17	12	8	9	6			
5	41	29				20	21	29
6	99	70	49	50	35			
7	239	169				119	120	169
8	577	408	288	289	204			
9	1393	985				696	697	985
10	3363	2378	1681	1682	1189			
11	8119	5741				4059	4060	5741
12	19601	13860	9800	9801	6930			

Definitions

The half companion Pell Numbers H_n and the Pell numbers P_n can be derived in a number of easily equivalent ways:

Raising to powers:

$$(1+\sqrt{2})^n = H_n + P_n\sqrt{2}$$
$$(1-\sqrt{2})^n = H_n - P_n\sqrt{2}.$$

From this it follows that there are *closed forms*:

$$H_n = \frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2}.$$

and

$$P_n\sqrt{2} = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2}.$$

Paired recurrences:

$$H_n = \begin{cases} 1 & \text{if } n = 0; \\ H_{n-1} + 2P_{n-1} & \text{otherwise.} \end{cases}$$

$$P_n = \begin{cases} 0 & \text{if } n = 0; \\ H_{n-1} + P_{n-1} & \text{otherwise.} \end{cases}$$

and *matrix formulations*:

$$\begin{pmatrix} H_n \\ P_n \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} H_{n-1} \\ P_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

So

$$\begin{pmatrix} H_n & 2P_n \\ P_n & H_n \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^n.$$

Approximations

The difference between H_n and $P_n\sqrt{2}$ is $(1-\sqrt{2})^n \approx (-0.41421)^n$ which goes rapidly to zero. So $(1+\sqrt{2})^n = H_n + P_n\sqrt{2}$ is extremely close $2H_n$.

From this last observation it follows that the integer ratios $\frac{H_n}{P_n}$ rapidly approach $\sqrt{2}$ while $\frac{H_n}{H_{n-1}}$ and $\frac{P_n}{P_{n-1}}$ rapidly approach $1+\sqrt{2}$.

$H^2 - 2P^2 = \pm 1$

Since $\sqrt{2}$ is irrational, we can't have $\frac{H}{P} = 2$ i.e. $\frac{H^2}{P^2} = \frac{2P^2}{P^2}$. The best we can achieve is either $\frac{H^2}{P^2} = \frac{2P^2-1}{P^2}$ or $\frac{H^2}{P^2} = \frac{2P^2+1}{P^2}$.

The (non-negative) solutions to $H^2 - 2P^2 = 1$ are exactly the pairs H_n, P_n with n even and the solutions to $H^2 - 2P^2 = -1$ are exactly the pairs H_n, P_n with n odd. To see this, note first that

$$H_{n+1}^2 - 2P_{n+1}^2 = (H_n + 2P_n)^2 - 2(H_n + P_n)^2 = -(H_n^2 - 2P_n^2)$$

so that these differences, starting with $H_0^2 - 2P_0^2 = 1$ are alternately 1 and -1. Then note that that every positive solution comes in this way from a solution with smaller integers since $(2P - H)^2 - 2(H - P)^2 = -(H^2 - 2P^2)$. The smaller solution also has positive integers with the one

exception $H = P = 1$ which comes from $H_0 = 1$ and $P_0 = 0$.

Square triangular numbers

The required equation $\frac{t(t+1)}{2} = s^2$ is equivalent to $4t^2 + 4t + 1 = 8s^2 + 1$ which becomes $H^2 = 2P^2 + 1$ with the substitutions $H = 2t + 1$ and $P = 2s$. Hence the nth solution is $t_n = \frac{H_{2n} - 1}{2}$ and $s_n = \frac{P_{2n}}{2}$.

Observe that t and $t + 1$ are relatively prime so that $\frac{t(t+1)}{2} = s^2$ happens exactly when they are adjacent integers, one a square H^2 and the other twice a square $2P^2$. Since we know all solutions of that equation, we also have

$$t_n = \begin{cases} 2P_n^2 & \text{if } n \text{ is even;} \\ H_n^2 & \text{if } n \text{ is odd.} \end{cases}$$

and $s_n = H_n P_n$

This alternate expression is seen in the next table.

n	H_n	P_n	t	t+1	s	a	b	c
0	1	0						
1	1	1	1	2	1	1	0	1
2	3	2	8	9	6	3	4	5
3	7	5	49	50	35	21	20	29
4	17	12	288	289	204	119	120	169
5	41	29	1681	1682	1189	697	696	985
6	99	70	9800	9801	6930	4059	4060	5741

Pythagorean triples

The equality $c^2 = a^2 + (a+1)^2 = 2a^2 + 2a + 1$ occurs exactly when $2c^2 = 4a^2 + 4a + 2$ which becomes $2P^2 = H^2 + 1$ with the substitutions $H = 2a + 1$ and $P = c$. Hence the nth solution is $a_n = \frac{H_{2n+1} - 1}{2}$ and $c_n = P_{2n+1}$.

The table above shows that, in one order or the other, a_n and $b_n = a_n + 1$ are $H_n H_{n+1}$ and $2P_n P_{n+1}$ while $c_n = H_{n+1} P_n + P_{n+1} H_n$.

Notes

[1] For instance, Sellers (2002) proves that the number of perfect matchings in the Cartesian product of a path graph and the graph K_4-e can be calculated as the product of a Pell number with the corresponding Fibonacci number.

[2] http://en.wikipedia.org/wiki/Oeis%3Aa000129

[3] For the matrix formula and its consequences see Ercolano (1979) and Kilic and Tasci (2005). Additional identities for the Pell numbers are listed by Horadam (1971) and Bicknell (1975).

[4] As recorded in the Shulba Sutras; see e.g. Dutka (1986), who cites Thibaut (1875) for this information.

[5] See Knorr (1976) for the fifth century date, which matches Proclus' claim that the side and diameter numbers were discovered by the Pythagoreans. For more detailed exploration of later Greek knowledge of these numbers see Thompson (1929), Vedova (1951), Ridenhour (1986), Knorr (1998), and Filep (1999).

[6] For instance, as several of the references from the previous note observe, in Plato's Republic there is a reference to the "rational diameter of 5", by which Plato means 7, the numerator of the approximation 7/5 of which 5 is the denominator.

[7] Pethő (1992); Cohn (1996). Although the Fibonacci numbers are defined by a very similar recurrence to the Pell numbers, Cohn writes that an analogous result for the Fibonacci numbers seems much more difficult to prove.

[8] Sesskin (1962). See the square triangular number article for a more detailed derivation.

[9] http://en.wikipedia.org/wiki/Oeis%3Aa002315

[10] http://en.wikipedia.org/wiki/Oeis%3Aa002203

References

- Bicknell, Marjorie (1975). "A primer on the Pell sequence and related sequences". *Fibonacci Quarterly* **13** (4): 345–349. MR0387173.
- Cohn, J. H. E. (1996). "Perfect Pell powers". *Glasgow Mathematical Journal* **38** (1): 19–20. doi:10.1017/S0017089500031207. MR1373953.
- Dutka, Jacques (1986). "On square roots and their representations". *Archive for History of Exact Sciences* **36** (1): 21–39. doi:10.1007/BF00357439. MR0863340.
- Ercolano, Joseph (1979). "Matrix generators of Pell sequences". *Fibonacci Quarterly* **17** (1): 71–77. MR0525602.
- Filep, László (1999). "Pythagorean side and diagonal numbers" (http://www.emis.de/journals/AMAPN/vol15/filep.pdf). *Acta Mathematica Academiae Paedagogiace Nyíregyháziensis* **15**: 1–7.
- Horadam, A. F. (1971). "Pell identities". *Fibonacci Quarterly* **9** (3): 245–252, 263. MR0308029.
- Kilic, Emrah; Tasci, Dursun (2005). "The linear algebra of the Pell matrix". *Boletín de la Sociedad Matemática Mexicana, Tercera Serie* **11** (2): 163–174. MR2207722.
- Knorr, Wilbur (1976). "Archimedes and the measurement of the circle: A new interpretation". *Archive for History of Exact Sciences* **15** (2): 115–140. doi:10.1007/BF00348496. MR0497462.
- Knorr, Wilbur (1998). ""Rational diameters" and the discovery of incommensurability" (http://jstor.org/stable/3109803). *American Mathematical Monthly* **105** (5): 421–429. doi:10.2307/3109803.
- Knuth, Donald E. (1994). "Leaper graphs" (http://jstor.org/stable/3620202). *The Mathematical Gazette* **78** (483): 274–297. doi:10.2307/3620202. arXiv:math.CO/9411240.
- Martin, Artemas (1875). "Rational right angled triangles nearly isosceles" (http://www.jstor.org/stable/2635906). *The Analyst* **3** (2): 47–50. doi:10.2307/2635906.
- Pethő, A. (1992). "The Pell sequence contains only trivial perfect powers". *Sets, graphs, and numbers (Budapest, 1991)*. Colloq. Math. Soc. János Bolyai, 60, North-Holland. pp. 561–568. MR1218218.
- Ridenhour, J. R. (1986). "Ladder approximations of irrational numbers" (http://www.jstor.org/stable/2690427). *Mathematics Magazine* **59** (2): 95–105. doi:10.2307/2690427.
- Santana, S. F.; Diaz-Barrero, J. L. (2006). "Some properties of sums involving Pell numbers" (http://www.math-cs.cmsu.edu/~mjms/2006.1/diazbar.pdf). *Missouri Journal of Mathematical Sciences* **18** (1).
- Sellers, James A. (2002). "Domino tilings and products of Fibonacci and Pell numbers" (http://www.emis.de/journals/JIS/VOL5/Sellers/sellers4.pdf). *Journal of Integer Sequences* **5**. MR1919941.
- Sesskin, Sam (1962). "A "converse" to Fermat's last theorem?" (http://links.jstor.org/sici?sici=0025-570X(196209)35:4<215:A"TFLT>2.0.CO;2-6). *Mathematics Magazine* **35** (4): 215–217.

doi:10.2307/2688551.
- Thibaut, George (1875). "On the Súlvasútras". *Journal of the Royal Asiatic Society of Bengal* **44**: 227–275.
- Thompson, D'Arcy Wentworth (1929). "III.—Excess and defect: or the little more and the little less" (http://www.jstor.org/stable/2249223). *Mind: New Series* **38** (149): 43–55.
- Vedova, G. C. (1951). "Notes on Theon of Smyrna" (http://jstor.org/stable/2307978). *American Mathematical Monthly* **58** (10): 675–683. doi:10.2307/2307978.

External links

- Weisstein, Eric W., " Pell Number (http://mathworld.wolfram.com/PellNumber.html)" from MathWorld.

Permutable prime

A **permutable prime** is a prime number, which, in a given base, can have its digits switched to any possible permutation and still spell a prime number. H. E. Richert, who supposedly first studied these primes, called them permutable primes[1] , but later they were also called **absolute prime**s[2] .

In base 10, all the permutable primes with less than 49081 digits are (sequence A003459 [30] in OEIS):

2, 3, 5, 7, 11, 13, 17, 31, 37, 71, 73, 79, 97, 113, 131, 199, 311, 337, 373, 733, 919, 991, 1111111111111111, 11111111111111111111, R_{317}, R_{1031}

where $R_n = \frac{10^n-1}{9}$ is the number with n ones.

Any repunit prime is a permutable prime with the above definition, but some definitions require at least two distinct digits.[3]

All permutable primes of two or more digits are composed from the digits 1, 3, 7, 9, because no prime number except 2 is even, and no prime number besides 5 is divisible by 5. It is proved[4] that no permutable prime exists which contains three different of the four digits 1, 3, 7, 9, as well as that there exists no permutable prime composed of two or more of each of two digits selected from 1, 3, 7, 9.

There is no n-digit permutable prime for $3 < n < 6 \cdot 10^{175}$ which is not a repunit[1] . It is conjectured that there are no non-repunit permutable primes other than those listed above.

In base 2, only repunits can be permutable primes, because any 0 permuted to the one's place results in an even number; unless we consider 1 a prime number and 10 permutable with 01. Therefore the base 2 permutable primes are the Mersenne primes. The generalization can safely be made that for any positional number system, permutable primes with more than one digit can only have digits that are coprime with the radix of the number system. One-digit primes, meaning any prime below the radix, are always permutable.

References

[1] H. E. Richert, "On permutable primtall," *Norsk Matematiske Tiddskrift* **33** (1951), 50–54.

[2] T. Bhargava & P. Doyle, "On the existence of absolute primes," *Math. Mag.* **47** (1974), 233.

[3] Chris Caldwell, The Prime Glossary: permutable prime (http://primes.utm.edu/glossary/page.php?sort=PermutablePrime) at The Prime Pages.

[4] A.W. Johnson, "Absolute primes," *Mathematics Magazine* **50** (1977), 100–103.

Perrin number

In mathematics, the **Perrin numbers** are defined by the recurrence relation

$P(0) = 3, P(1) = 0, P(2) = 2,$

and

$P(n) = P(n - 2) + P(n - 3)$ for $n > 2$.

The sequence of Perrin numbers starts with

3, 0, 2, 3, 2, 5, 5, 7, 10, 12, 17, 22, 29, 39 ... (sequence A001608 [1] in OEIS)

The number of different maximal independent sets in an n-vertex cycle graph is counted by the nth Perrin number.[2]

History

This sequence was analyzed by Edouard Lucas (1878). In 1899, the same sequence was mentioned by R. Perrin. The most extensive treatment of this sequence was given by Adams and Shanks (1982).

Properties

Generating function

The generating function of the Perrin sequence is

$$G(P(n); x) = \frac{3 - x^2}{1 - x^2 - x^3}.$$

Matrix formula

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}^n \begin{pmatrix} 3 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} P(n) \\ P(n+1) \\ P(n+2) \end{pmatrix}$$

Binet-like formula

The Perrin sequence numbers can be written in terms of powers of the roots of the equation

$$x^3 - x - 1 = 0.$$

This equation has 3 roots; one real root p (known as the plastic number) and two complex conjugate roots q and r. Given these three roots, the Perrin sequence analogue of the Fibonacci sequence Binet formula is

$$P(n) = p^n + q^n + r^n.$$

Since the magnitudes of the complex roots q and r are both less than 1, the powers of these roots approach 0 for large n. For large n the formula reduces to

$$P(n) \approx p^n$$

This formula can be used to quickly calculate values of the Perrin sequence for large n. The ratio of successive terms in the Perrin sequence approaches p, a.k.a. the plastic number, which has a value of approximately 1.324718. This constant bears the same relationship to the Perrin sequence and the Padovan sequence as the golden ratio does to the Fibonacci sequence and the silver ratio does to the Pell numbers.

Multiplication formula

From the Binet formula, we can obtain a formula for $G(kn)$ in terms of $G(n-1)$, $G(n)$ and $G(n+1)$; we know

$$\begin{aligned} G(n-1) &= p^{-1}p^n + q^{-1}q^n + r^{-1}r^n \\ G(n) &= p^n + q^n + r^n \\ G(n+1) &= pp^n + qq^n + rr^n \end{aligned}$$

which gives us three linear equations with coefficients over the splitting field of $x^3 - x - 1$; by inverting a matrix we can solve for p^n, q^n, r^n and then we can raise them to the kth power and compute the sum.
Example magma code:

```
P<x> := PolynomialRing(Rationals());
S<t> := SplittingField(x^3-x-1);
P2<y> := PolynomialRing(S);
p,q,r := Explode([r[1] : r in Roots(y^3-y-1)]);
Mi:=Matrix([[1/p,1/q,1/r],[1,1,1],[p,q,r]])^(-1);
T<u,v,w> := PolynomialRing(S,3);
v1 := ChangeRing(Mi,T) *Matrix([[u],[v],[w]]);
[p^i*v1[1,1]^3 + q^i*v1[2,1]^3 + r^i*v1[3,1]^3 : i in [-1..1]];
```

with the result that, if we have $u = G(n-1), v = G(n), w = G(n+1)$, then

$$\begin{aligned} 23G(2n-1) &= 4u^2 + 3v^2 + 9w^2 + 18uv - 12uw - 4vw \\ 23G(2n) &= -6u^2 + 7v^2 - 2w^2 - 4uv + 18uw + 6vw \\ 23G(2n+1) &= 9u^2 + v^2 + 3w^2 + 6uv - 4uw + 14vw \\ 23G(3n-1) &= (-4u^3 + 2v^3 - w^3 + 9(uv^2 + vw^2 + wu^2) + 3v^2w + 6uvw) \\ 23G(3n) &= (3u^3 + 2v^3 + 3w^3 - 3(uv^2 + uw^2 + vw^2 + vu^2) + 6v^2w + 18uvw) \\ 23G(3n+1) &= (v^3 - w^3 + 6uv^2 + 9uw^2 + 6vw^2 + 9vu^2 - 3wu^2 + 6wv^2 - 6uvw) \end{aligned}$$

The number 23 here arises from the discriminant of the defining polynomial of the sequence.

This allows you to compute the nth Perrin number using integer arithmetic in $O(\log n)$ multiplies.

Primes and divisibility

Perrin pseudoprimes

It has been proven that for all primes p, p divides $P(p)$. However, the converse is not true: for some composite numbers n, n may still divide $P(n)$. If n has this property, it is called a **Perrin pseudoprime**.

The question of the existence of Perrin pseudoprimes was considered by Perrin himself, but it was not known whether they existed until Adams and Shanks (1982) discovered the smallest one, $271441 = 521^2$; the next-smallest is 904631 = 7 x 13 x 9941. There are seventeen of them less than a billion;[3] Jon Grantham has proved[4] that there are infinitely many Perrin pseudoprimes.

Perrin primes

A **Perrin prime** is a Perrin number that is prime. The first few Perrin primes are:

2, 3, 5, 7, 17, 29, 277, 367, 853, 14197, 43721, 1442968193, 792606555396977, 18727865918041723432 1, 6624116048878014107157986479 7 (sequence A074788 [31] in OEIS)

E. W. Weisstein found a 32,147 digit probable Perrin prime *P*(263226) in May 2006.

Notes

[1] http://en.wikipedia.org/wiki/Oeis%3Aa001608

[2] Füredi (1987)

[3] (sequence A013998 (http://en.wikipedia.org/wiki/Oeis:a013998) in OEIS)

[4] Jon Grantham (2010). "There are infinitely many Perrin pseudoprimes" (http://www.pseudoprime.com/pseudo3.pdf). *Journal of Number Theory* **130** (5): 1117–1128. doi:10.1016/j.jnt.2009.11.008. .

References

- Adams, William; Shanks, Daniel (1982). "Strong primality tests that are not sufficient" (http://jstor.org/stable/2007637). *Mathematics of Computation* (American Mathematical Society) **39** (159): 255–300. doi:10.2307/2007637. MR0658231.
- Füredi, Z. (1987). "The number of maximal independent sets in connected graphs". *Journal of Graph Theory* **11** (4): 463–470. doi:10.1002/jgt.3190110403.
- Lucas, E. (1878). "Théorie des fonctions numériques simplement périodiques" (http://jstor.org/stable/2369311). *American Journal of Mathematics* (The Johns Hopkins University Press) **1** (3): 197–240. doi:10.2307/2369311.
- Perrin, R. (1899). "Query 1484". *L'Intermediaire Des Mathematiciens* **6**: 76.

External links

- Zentrum für Hirnforschung Institut für Medizinische Kybernetik und Artificial Intelligence (http://www.ai.univie.ac.at/perrin.html)
- MathPages - Lucas Pseudoprimes (http://www.mathpages.com/home/kmath127.htm)
- MathPages - Perrin's Sequence (http://www.mathpages.com/home/kmath345.htm)

Pierpont prime

A **Pierpont prime** is a prime number of the form

$$2^u 3^v + 1$$

for some nonnegative integers u and v. They are named after the mathematician James Pierpont.

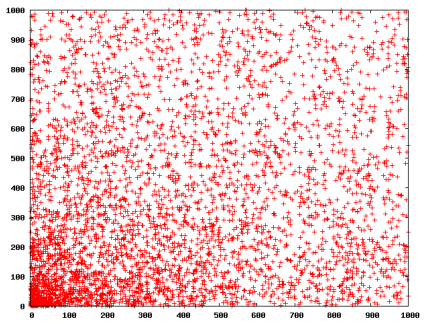
It is possible to prove that if $v = 0$ and $u > 0$, then u must be a power of 2, making the prime a Fermat prime. If v is positive then u must also be positive, and the Pierpont prime is of the form $6k + 1$ (because if $u = 0$ and $v > 0$ then $2^u 3^v + 1$ is an even number greater than 2 and therefore composite).

The first few Pierpont primes are:

2, 3, 5, 7, 13, 17, 19, 37, 73, 97, 109, 163, 193, 257, 433, 487, 577, 769. (sequence A005109 [32] in OEIS)

Distribution of Pierpont primes

Andrew Gleason conjectured there are infinitely many Pierpont primes. They are not particularly rare and there are few restrictions from algebraic factorisations, so there are no requirements like the Mersenne prime condition that the exponent must be prime. There are 36 Pierpont primes less than 10^6, 59 less than 10^9, 151 less than 10^{20}, and 789 less than 10^{100}; conjecturally there are O(log N) Pierpont primes smaller than N, as opposed to the conjectured O(log log N) Mersenne primes in that range.



Distribution of the exponents for the smaller Pierpont primes

Pierpont primes found as factors of Fermat numbers

As part of the ongoing worldwide search for factors of Fermat numbers, some Pierpont primes have been announced as factors. The following table[1] gives values of m, k, and n such that

$$k \cdot 2^n + 1 \text{ divides } 2^{2^m} + 1.$$

The left-hand side is a Pierpont prime when k is a power of 3; the right-hand side is a Fermat number.

m	k	n	Year	Discoverer
38	3	41	1903	Cullen, Cunningham & Western
63	9	67	1956	Robinson
207	3	209	1956	Robinson
452	27	455	1956	Robinson
9428	9	9431	1983	Keller
12185	81	12189	1993	Dubner
28281	81	28285	1996	Taura
157167	3	157169	1995	Young
213319	3	213321	1996	Young
303088	3	303093	1998	Young

382447	3	382449	1999	Cosgrave & Gallot
461076	9	461081	2003	Nohara, Jobling, Woltman & Gallot
672005	27	672007	2005	Cooper, Jobling, Woltman & Gallot
2145351	3	2145353	2003	Cosgrave, Jobling, Woltman & Gallot
2478782	3	2478785	2003	Cosgrave, Jobling, Woltman & Gallot

As of 2008, the largest known Pierpont prime is $3 \times 2^{2478785} + 1$,[2] whose primality was discovered by John B. Cosgrave in 2003 with software by Paul Jobling, George Woltman, and Yves Gallot.[3]

In the mathematics of paper folding, the Huzita–Hatori axioms define six of the seven types of fold possible. It has been shown that these folds are sufficient to allow any regular polygon of N sides to be formed, as long as $N > 3$ and of the form $2^m 3^n \rho$, where ρ is a product of distinct Pierpont primes. This is the same class of regular polygons as those that can be constructed with a ruler, straightedge, and angle-trisector. Regular polygons which can be constructed with only ruler and straightedge (constructible polygons) are the special case where $n = 0$ and ρ is a product of distinct Fermat primes, themselves a subset of Pierpont primes.

Notes

[1] Wilfrid Keller, Fermat factoring status (http://www.prothsearch.net/fermat.html).

[2] Chris Caldwell, The largest known primes (http://primes.utm.edu/primes/lists/short.txt) at The Prime Pages.

[3] Proof-code: g245 (http://primes.utm.edu/bios/code.php?code=g245) at The Prime Pages.

References

- Weisstein, Eric W., " Pierpont Prime (http://mathworld.wolfram.com/PierpontPrime.html)" from MathWorld.

Pillai prime

A **Pillai prime** is a prime number p for which there is an integer $n > 0$ such that the factorial of n is one less than a multiple of the prime, but the prime is not one more than a multiple of n. To put it algebraically, $n! \equiv -1 \mod p$ but $p \not\equiv 1 \mod n$. The first few Pillai primes are

23, 29, 59, 61, 67, 71, 79, 83, 109, 137, 139, 149, 193, ... (sequence A063980 [33] in OEIS)

Pillai primes are named after the mathematician Subbayya Sivasankaranarayana Pillai, who asked about these numbers. Their infinitude has been proved several times, by Subbarao, Erdős, and Hardy & Subbarao.

References

- Guy, R. K. (2004), *Unsolved Problems in Number Theory* (3rd ed.), New York: Springer-Verlag, p. A2, ISBN 0387208607.
- Hardy, G. E. & Subbarao, M. V. (2002), "A modified problem of Pillai and some related questions", *American Mathematical Monthly* **109** (6): 554–559, doi:10.2307/2695445.
- Pillai prime [1] on PlanetMath

References

[1] http://planetmath.org/?op=getobj&from=objects&id=8739

Prime gap

A **prime gap** is the difference between two successive prime numbers. The n-th prime gap, denoted g_n, is the difference between the $(n + 1)$-th and the n-th prime number, i.e.

$$g_n = p_{n+1} - p_n.$$

We have $g_1 = 1$, $g_2 = g_3 = 2$, and $g_4 = 4$. The sequence (g_n) of prime gaps has been extensively studied. One also writes $g(p_n)$ for g_n.

The first 30 prime gaps are:

1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, 4, 2, 4, 2, 4, 14 (sequence A001223 [1] in OEIS).

Simple observations

For any prime number P, we write $P\#$ for *P primorial*, that is, the product of all prime numbers up to and including P. If Q is the prime number following P, then the sequence

$$P\# + 2, P\# + 3, ..., P\# + (Q - 1)$$

is a sequence of $Q - 2$ consecutive composite integers, so here there is a prime gap of at least length $Q - 1$. Therefore, there exist gaps between primes which are arbitrarily large, i.e., for any prime number P, there is an integer n with $g_n \geq P$. (This is seen by choosing n so that p_n is the greatest prime number less than $P\# + 2$.) Another way to see that arbitrarily large prime gaps must exist is the fact that the density of primes approaches zero, according to the Prime number theorem.

In reality, prime gaps of P numbers can occur at numbers much smaller than $P\#$. For instance, the smallest sequence of 71 consecutive composite numbers occurs between 31398 and 31468, whereas 71# has *twenty-seven digits* - its full decimal expansion being **557940830126698960967415390**.

Although the average gap between primes increases as the natural logarithm of the integer, the ratio of the maximum prime gap to the integers involved also increases as larger and larger numbers and gaps are encountered.

In the opposite direction, the twin prime conjecture asserts that $g_n = 2$ for infinitely many integers n.

Numerical results

As of 2009 the largest known prime gap with identified probable prime gap ends has length 2254930, with 86853-digit probable primes found by H. Rosenthal and J. K. Andersen. [2] The largest known prime gap with identified proven primes as gap ends has length 337446, with 7996-digit primes found by T. Alm, J. K. Andersen and François Morain. [3]

We say that g_n is a *maximal gap* if $g_m < g_n$ for all $m < n$. As of August 2009 the largest known maximal gap has length 1476, found by Tomás Oliveira e Silva. It is the 75th maximal gap, and it occurs after the prime 1425172824437699411. [4]

The largest known value of g_n / ln(p_n) is 1476 / ln(1425172824437699411) = 35.31. Usually this number is called the *merit* of the gap g_n . [5]

Number 1 to 25

#	g_n	p_n
1	1	2
2	2	3
3	4	7
4	6	23
5	8	89
6	14	113
7	18	523
8	20	887
9	22	1129
10	34	1327
11	36	9551
12	44	15683
13	52	19609
14	72	31397
15	86	155921
16	96	360653
17	112	370261
18	114	492113
19	118	1349533
20	132	1357201
21	148	2010733
22	154	4652353
23	180	17051707
24	210	20831323
25	220	47326693

The first 75 maximal gaps

Number 26 to 50

#	g_n	p_n
26	222	122164747
27	234	189695659
28	248	191912783
29	250	387096133
30	282	436273009
31	288	1294268491
32	292	1453168141
33	320	2300942549

34	336	3842610773
35	354	4302407359
36	382	10726904659
37	384	20678048297
38	394	22367084959
39	456	25056082087
40	464	42652618343
41	468	127976334671
42	474	182226896239
43	486	241160624143
44	490	297501075799
45	500	303371455241
46	514	304599508537
47	516	416608695821
48	532	461690510011
49	534	614487453523
50	540	738832927927

Number 51 to 75

#	g_n	p_n
51	582	1346294310749
52	588	1408695493609
53	602	1968188556461
54	652	2614941710599
55	674	7177162611713
56	716	13829048559701
57	766	19581334192423
58	778	42842283925351
59	804	90874329411493
60	806	171231342420521
61	906	218209405436543
62	916	1189459969825483
63	924	1686994940955803
64	1132	1693182318746371
65	1184	43841547845541059
66	1198	55350776431903243
67	1220	80873624627234849
68	1224	203986478517455989
69	1248	218034721194214273

70	1272	305405826521087869
71	1328	352521223451364323
72	1356	401429925999153707
73	1370	418032645936712127
74	1442	804212830686677669
75	1476	1425172824437699411

n

Further results

Upper bounds

Bertrand's postulate states that there is always a prime number between k and $2k$, so in particular $p_{n+1} < 2p_n$, which means $g_n < p_n$.

The prime number theorem says that the "average length" of the gap between a prime p and the next prime is $\ln p$. The actual length of the gap might be much more or less than this. However, from the prime number theorem one can also deduce an upper bound on the length of prime gaps: for every $\varepsilon > 0$, there is a number N such that $g_n < \varepsilon p_n$ for all $n > N$.

Hoheisel was the first to show[6] that there exists a constant $\theta < 1$ such that

$$\pi(x + x^\theta) - \pi(x) \sim \frac{x^\theta}{\log(x)} \text{ as } x \text{ tends to infinity,}$$

hence showing that

$$g_n < p_n^\theta,$$

for sufficiently large n.

One can deduce that the gaps get arbitrarily smaller in proportion to the primes: the quotient g_n/p_n approaches zero as n goes to infinity.

Hoheisel obtained the possible value 32999/33000 for θ. This was improved to 249/250 by Heilbronn,[7] and to $\theta = 3/4 + \varepsilon$, for any $\varepsilon > 0$, by Chudakov.[8]

A major improvement is due to Ingham,[9] who showed that if

$$\zeta(1/2 + it) = O(t^c)$$

for some positive constant c, where O refers to the big O notation, then

$$\pi(x + x^\theta) - \pi(x) \sim \frac{x^\theta}{\log(x)}$$

for any $\theta > (1 + 4c)/(2 + 4c)$. Here, as usual, ζ denotes the Riemann zeta function and π the prime-counting function. Knowing that any $c > 1/6$ is admissible, one obtains that θ may be any number greater than 5/8.

An immediate consequence of Ingham's result is that there is always a prime number between n^3 and $(n + 1)^3$ if n is sufficiently large. Note however that not even the Lindelöf hypothesis, which assumes that we can take c to be any positive number, implies that there is a prime number between n^2 and $(n + 1)^2$, if n is sufficiently large (see Legendre's conjecture). To verify this, a stronger result such as Cramér's conjecture would be needed.

Huxley showed that one may choose $\theta = 7/12$.[10]

A recent result, due to Baker, Harman and Pintz, shows that θ may be taken to be 0.525.[11]

Lower bounds

Robert Rankin proved the existence of a constant $c > 0$ such that the inequality

$$g_n > \frac{c \log n \log\log n \log\log\log\log n}{(\log\log\log n)^2}$$

holds for infinitely many values n. The best known value of the constant c is currently $c = 2e^{\gamma}$, where γ is the Euler–Mascheroni constant.[12] Paul Erdős offered a $5,000 prize for a proof or disproof that the constant c in the above inequality may be taken arbitrarily large.[13]

Conjectures about gaps between primes

Even better results are possible if it is assumed that the Riemann hypothesis is true. Harald Cramér proved that, under this assumption, the gap $g(p_n)$ satisfies

$$g(p_n) = O(\sqrt{p_n} \ln p_n),$$

using the big O notation. Later, he conjectured that the gaps are even smaller. Roughly speaking he conjectured that

$$g(p_n) = O\left((\ln p_n)^2\right).$$

At the moment, the numerical evidence seems to point in this direction. See Cramér's conjecture for more details.

Andrica's conjecture states that

$$g(p_n) < 2\sqrt{p_n} + 1.$$

This is a slight strengthening of Legendre's conjecture that between successive square numbers there is always a prime.

As an arithmetic function

The gap g_n between the nth and $(n + 1)$st prime numbers is an example of an arithmetic function. In this context it is usually denoted d_n and called the prime difference function.[13] The function is neither multiplicative nor additive.

See also

- Bonse's inequality

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa001223

[2] http://users.cybercity.dk/~dsl522332/math/primegaps/megagap2.htm

[3] http://users.cybercity.dk/~dsl522332/math/primegaps/gap337446.htm

[4] http://users.cybercity.dk/~dsl522332/math/primegaps/maximal.htm

[5] http://users.cybercity.dk/~dsl522332/math/primegaps/gaps20.htm#top20merit

[6] G. Hoheisel, *Primzahlprobleme in der Analysis*, Sitzunsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin, **33**, pages 3-11, (1930)

[7] H. A. Heilbronn, *Über den Primzahlsatz von Herrn Hoheisel*, Mathematische Zeitschrift, **36**, pages 394–423, (1933)

[8] N. G. Tchudakoff, *On the difference between two neighboring prime numbers*, Math. Sb., **1**, pages 799–814, (1936)

[9] Ingham, A. E. *On the difference between consecutive primes*, Quarterly Journal of Mathematics (Oxford Series), **8**, pages 255–266, (1937)

[10] Huxley, M. N. (1972). "*On the Difference between Consecutive Primes*". *Inventiones mathematicae* **15**: 164–170. doi:10.1007/BF01418933.

[11] Baker, R. C.; G. Harman, G. and J. Pintz (2001). "*The difference between consecutive primes, II*". *Proceedings of the London Mathematical Society* **83**: 532–562. doi:10.1112/plms/83.3.532.

[12] J. Pintz, *Very large gaps between consecutive primes*, J. Number Theory, **63**, pages 286–301, (1997).

[13] R.K. Guy, *Unsolved problems in number theory, Third edition*, Springer, (2004), p.31.

External links

- Thomas R. Nicely, Some Results of Computational Research in Prime Numbers -- Computational Number Theory (http://www.trnicely.net/). This reference web site includes a list of all first known occurrence prime gaps.
- Weisstein, Eric W., " Prime Difference Function (http://mathworld.wolfram.com/PrimeDifferenceFunction.html)" from MathWorld.
- Prime Difference Function (http://planetmath.org/?op=getobj&from=objects&id=3143) on PlanetMath
- Chris Caldwell, *Gaps Between Primes* (http://primes.utm.edu/notes/gaps.html)

Prime quadruplet

A **prime quadruplet** (sometimes called **prime quadruple**) is a set of four primes of the form {p, p+2, p+6, p+8}.[1] This represents the closest possible grouping of four primes larger than 3. The first prime quadruplets are

{5, 7, 11, 13}, {11, 13, 17, 19}, {101, 103, 107, 109}, {191, 193, 197, 199}, {821, 823, 827, 829}, {1481, 1483, 1487, 1489}, {1871, 1873, 1877, 1879}, {2081, 2083, 2087, 2089}, {3251, 3253, 3257, 3259}, {3461, 3463, 3467, 3469}, {5651, 5653, 5657, 5659}, {9431, 9433, 9437, 9439}, {13001, 13003, 13007, 13009}, {15641, 15643, 15647, 15649}, {15731, 15733, 15737, 15739}, {16061, 16063, 16067, 16069}, {18041, 18043, 18047, 18049}, {18911, 18913, 18917, 18919}, {19421, 19423, 19427, 19429}, {21011, 21013, 21017, 21019}, {22271, 22273, 22277, 22279}, {25301, 25303, 25307, 25309}, {31721, 31723, 31727, 31729}, {34841, 34843, 34847, 34849}, {43781, 43783, 43787, 43789}, {51341, 51343, 51347, 51349}, {55331, 55333, 55337, 55339}, {62981, 62983, 62987, 62989}, {67211, 67213, 67217, 67219}, {69491,69493, 69497, 69499}, {72221, 72223, 72227, 72229}, {77261, 77263, 77267, 77269}, {79691, 79693, 79697, 79699}, {81041, 81043, 81047, 81049}, {82721, 82723, 82727, 82729}, {88811, 88813, 88817, 88819}, {97841, 97843, 97847, 97849}, {99131,99133, 99137, 99139} (sequence A007530 [37] in OEIS)

All prime quadruplets except {5, 7, 11, 13} are of the form {30n + 11, 30n + 13, 30n + 17, 30n + 19} for some integer n. (This structure is necessary to ensure that none of the four primes is divisible by 2, 3 or 5). A prime quadruplet of this form is also called a **prime decade**.

Some sources also call {2, 3, 5, 7} or {3, 5, 7, 11} prime quadruplets, while some other sources exclude {5, 7, 11, 13}. [2]

A prime quadruplet contains two pairs of twin primes and two overlapping prime triplets.

It is not known if there are infinitely many prime quadruplets. A proof that there are infinitely many would imply the twin prime conjecture, but it is consistent with current knowledge that there may be infinitely many pairs of twin primes and only finitely many prime quadruplets. The number of prime quadruplets with n digits in base 10 for n = 2, 3, 4, ... is 1, 3, 7, 26, 128, 733, 3869, 23620, 152141, 1028789, 7188960, 51672312, 381226246, 2873279651 (sequence A120120 [3] in OEIS).

As of 2007 the largest known prime quadruplet has 2058 digits.[4] It was found by Norman Luhn in 2005 and starts with

p = 4104082046 × 4799# + 5651, where 4799# is a primorial

The constant representing the sum of the reciprocals of all prime quadruplets, Brun's constant for prime quadruplets, denoted by B_4, is the sum of the reciprocals of all prime quadruplets:

$$B_4 = \left(\frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13}\right) + \left(\frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19}\right) + \left(\frac{1}{101} + \frac{1}{103} + \frac{1}{107} + \frac{1}{109}\right) + \cdots$$

with value:

$B_4 = 0.87058\ 83800 \pm 0.00000\ 00005$.

This constant should not be confused with the **Brun's constant for cousin primes**, prime pairs of the form (p, p + 4), which is also written as B_4.

The prime quadruplet {11, 13, 17, 19} is alleged to appear on the Ishango bone although this is disputed.

Prime quintuplets

If {p, p+2, p+6, p+8} is a prime quadruplet and p−4 or p+12 is also prime, then the five primes form a **prime quintuplet** which is the closest admissible constellation of five primes. The first few prime quintuplets with p+12 are (sequence A022006 [5] in OEIS):

{5, 7, 11, 13, 17}, {11, 13, 17, 19, 23}, {101, 103, 107, 109, 113}, {1481, 1483, 1487, 1489, 1493}, {16061, 16063, 16067, 16069, 16073}, {19421, 19423, 19427, 19429, 19433}, {21011, 21013, 21017, 21019, 21023}, {22271, 22273, 22277, 22279, 22283}, {43781, 43783, 43787, 43789, 43793}, {55331, 55333, 55337, 55339, 55343}

The first prime quintuplets with p−4 are (A022007 [6]):

{7, 11, 13, 17, 19}, {97, 101, 103, 107, 109}, {1867, 1871, 1873, 1877, 1879}, {3457, 3461, 3463, 3467, 3469}, {5647, 5651, 5653, 5657, 5659}, {15727, 15731, 15733, 15737, 15739}, {16057, 16061, 16063, 16067, 16069}, {19417, 19421, 19423, 19427, 19429}, {43777, 43781, 43783, 43787, 43789}, {79687, 79691, 79693, 79697, 79699}, {88807, 88811, 88813, 88817, 88819}

A prime quintuplet contains two close pairs of twin primes, a prime quadruplet, and three overlapping prime triplets.

It is not known if there are infinitely many prime quintuplets. Once again, proving the twin prime conjecture might not necessarily prove that there are also infinitely many prime quintuplets. Also, proving that there are infinitely many prime quadruplets might not necessarily prove that there are infinitely many prime quintuplets.

If both p−4 and p+12 are prime then it becomes a **prime sextuplet**. The first few:

{7, 11, 13, 17, 19, 23}, {97, 101, 103, 107, 109, 113}, {16057, 16061, 16063, 16067, 16069, 16073}, {19417, 19421, 19423, 19427, 19429, 19433}, {43777, 43781, 43783, 43787, 43789, 43793}

Some sources also call {5, 7, 11, 13, 17, 19} a prime sextuplet. Our definition, all cases of primes {p-4, p, p+2, p+6, p+8, p+12}, follows from defining a prime sextuplet as the closest admissible constellation of six primes.

A prime sextuplet contains two close pairs of twin primes, a prime quadruplet, four overlapping prime triplets, and two overlapping prime quintuplets.

It is not known if there are infinitely many prime sextuplets. Once again, proving the twin prime conjecture might not necessarily prove that there are also infinitely many prime sextuplets. Also, proving that there are infinitely many prime quintuplets might not necessarily prove that there are infinitely many prime sextuplets.

References

[1] Weisstein, Eric W., " Prime Quadruplet (http://mathworld.wolfram.com/PrimeQuadruplet.html)" from MathWorld. Retrieved on 2007-06-15.

[2] http://primes.utm.edu/glossary/page.php?sort=PrimeConstellation

[3] http://en.wikipedia.org/wiki/Oeis%3Aa120120

[4] Tony Forbes. *Prime k-tuplets* (http://anthony.d.forbes.googlepages.com/ktuplets.htm). Retrieved on 2007-09-01.

[5] http://en.wikipedia.org/wiki/Oeis%3Aa022006

[6] http://en.wikipedia.org/wiki/Oeis%3Aa022007

Prime triplet

In mathematics, a **prime triplet** is a set of three prime numbers of the form $(p, p + 2, p + 6)$ or $(p, p + 4, p + 6)$.[1] With the exceptions of (2, 3, 5) and (3, 5, 7), this is the closest possible grouping of three prime numbers, since every third odd number greater than 3 is divisible by 3, and hence not prime.

The first prime triplets (sequence A098420 [2] in OEIS) are

(5, 7, 11), (7, 11, 13), (11, 13, 17), (13, 17, 19), (17, 19, 23), (37, 41, 43), (41, 43, 47), (67, 71, 73), (97, 101, 103), (101, 103, 107), (103, 107, 109), (107, 109, 113), (191, 193, 197), (193, 197, 199), (223, 227, 229), (227, 229, 233), (277, 281, 283), (307, 311, 313), (311, 313, 317), (347, 349, 353), (457, 461, 463), (461, 463, 467), (613, 617, 619), (641, 643, 647), (821, 823, 827), (823, 827, 829), (853, 857, 859), (857, 859, 863), (877, 881, 883), (881, 883, 887)

A prime triplet contains a pair of twin primes (p and $p + 2$, or $p + 4$ and $p + 6$), a pair of cousin primes (p and $p + 4$, or $p + 2$ and $p + 6$), and a pair of sexy primes (p and $p + 6$).

A prime can be a member of up to three prime triplets - for example, 103 is a member of (97, 101, 103), (101, 103, 107) and (103, 107, 109). When this happens, the five involved primes form a prime quintuplet.

A prime quadruplet $(p, p + 2, p + 6, p + 8)$ contains two overlapping prime triplets, $(p, p + 2, p + 6)$ and $(p + 2, p + 6, p + 8)$.

Similarly to the twin prime conjecture, it is conjectured that there are infinitely many prime triplets. As of March 2010 the largest known prime triplet contains primes with 10047 digits.[3] It is the first known gigantic prime triplet and was found in 2008 by Norman Luhn and François Morain. The primes are $(p, p + 2, p + 6)$ with $p = 2072644824759 \times 2^{33333} - 1$.

References

[1] Chris Caldwell. The Prime Glossary: prime triple (http://primes.utm.edu/glossary/page.php?sort=PrimeTriple) from the Prime Pages. Retrieved on 2010-03-22.

[2] http://en.wikipedia.org/wiki/Oeis%3Aa098420

[3] The Top Twenty: Triplet (http://primes.utm.edu/top20/page.php?id=61) from the Prime Pages. Retrieved on 2010-03-22.

External links

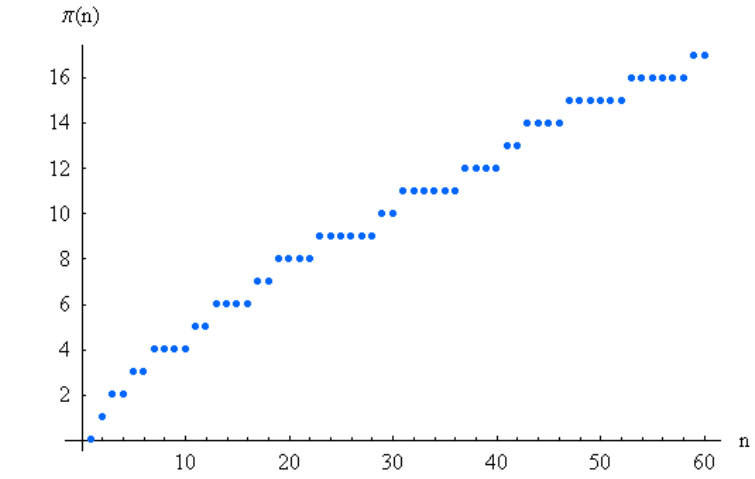
- Weisstein, Eric W., " Prime Triplet (http://mathworld.wolfram.com/PrimeTriplet.html)" from MathWorld.
- A022004 (http://en.wikipedia.org/wiki/Oeis:a022004) in OEIS
- A022005 (http://en.wikipedia.org/wiki/Oeis:a022005)

Prime-counting function

In mathematics, the **prime-counting function** is the function counting the number of prime numbers less than or equal to some real number x.[1] [2] It is denoted by $\pi(x)$(this does not refer to the number π).

History

Of great interest in number theory is the growth rate of the prime-counting function.[3] [4] It was conjectured in the end of the 18th century by Gauss and by Legendre to be approximately



The values of $\pi(n)$ for the first 60 integers

$$x/\ln(x)$$

in the sense that

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

This statement is the prime number theorem. An equivalent statement is

$$\lim_{x\to\infty} \pi(x)/\mathrm{li}(x) = 1$$

where *li* is the logarithmic integral function. The prime number theorem was first proved in 1896 by Jacques Hadamard and by Charles de la Vallée Poussin independently, using properties of the Riemann zeta function introduced by Riemann in 1859.

More precise estimates of $\pi(x)$ are now known; for example

$$\pi(x) = \mathrm{li}(x) + O\left(xe^{-\sqrt{\ln x}/15}\right)$$

where the O is big O notation. Most of the time $\mathrm{li}(x)$ is greater than $\pi(x)$, but infinitely often the opposite is true. For a discussion of this, see Skewes' number.

Proofs of the prime number theorem not using the zeta function or complex analysis were found around 1948 by Atle Selberg and by Paul Erdős (for the most part independently).[5]

Table of $\pi(x)$, x / ln x, and li(x)

The table shows how the three functions $\pi(x)$, x / ln x and li(x) compare at powers of 10. See also [3], [6], [7] and [8].

x	$\pi(x)$	$\pi(x) - x / \ln x$	$\mathrm{li}(x) - \pi(x)$	$x / \pi(x)$
10	4	−0.3	2.2	2.500
10^2	25	3.3	5.1	4.000
10^3	168	23	10	5.952
10^4	1,229	143	17	8.137
10^5	9,592	906	38	10.425
10^6	78,498	6,116	130	12.740
10^7	664,579	44,158	339	15.047
10^8	5,761,455	332,774	754	17.357
10^9	50,847,534	2,592,592	1,701	19.667
10^{10}	455,052,511	20,758,029	3,104	21.975
10^{11}	4,118,054,813	169,923,159	11,588	24.283
10^{12}	37,607,912,018	1,416,705,193	38,263	26.590
10^{13}	346,065,536,839	11,992,858,452	108,971	28.896
10^{14}	3,204,941,750,802	102,838,308,636	314,890	31.202
10^{15}	29,844,570,422,669	891,604,962,452	1,052,619	33.507
10^{16}	279,238,341,033,925	7,804,289,844,393	3,214,632	35.812
10^{17}	2,623,557,157,654,233	68,883,734,693,281	7,956,589	38.116
10^{18}	24,739,954,287,740,860	612,483,070,893,536	21,949,555	40.420
10^{19}	234,057,667,276,344,607	5,481,624,169,369,960	99,877,775	42.725
10^{20}	2,220,819,602,560,918,840	49,347,193,044,659,701	222,744,644	45.028
10^{21}	21,127,269,486,018,731,928	446,579,871,578,168,707	597,394,254	47.332
10^{22}	201,467,286,689,315,906,290	4,060,704,006,019,620,994	1,932,355,208	49.636
10^{23}	1,925,320,391,606,803,968,923	37,083,513,766,578,631,309	7,250,186,216	51.939
10^{24}	18,435,599,767,349,200,867,866	339,996,354,713,708,049,069	17,146,907,278	54.243

In the On-Line Encyclopedia of Integer Sequences, the $\pi(x)$ column is sequence A006880 [9], $\pi(x)$ - x / ln x is sequence A057835 [10], and $\mathrm{li}(x) - \pi(x)$ is sequence A057752 [11]. The value for $\pi(10^{24})$ is by J. Franke et al. and assumes the Riemann hypothesis.[12]

Algorithms for evaluating π(x)

A simple way to find $\pi(x)$, if x is not too large, is to use the sieve of Eratosthenes to produce the primes less than or equal to x and then to count them.

A more elaborate way of finding $\pi(x)$ is due to Legendre: given x, if p_1, p_2, ..., p_k are distinct prime numbers, then the number of integers less than or equal to x which are divisible by no p_i is

$$\lfloor x \rfloor - \sum_i \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \sum_{i<j<k} \left\lfloor \frac{x}{p_i p_j p_k} \right\rfloor + \cdots,$$

(where $\lfloor \cdot \rfloor$ denotes the floor function). This number is therefore equal to

$$\pi(x) - \pi\left(\sqrt{x}\right) + 1$$

when the numbers $p_1, p_2, \ldots, p_k$ are the prime numbers less than or equal to the square root of x.

In a series of articles published between 1870 and 1885, Ernst Meissel described (and used) a practical combinatorial way of evaluating $\pi(x)$. Let p_1, p_2, ..., p_n be the first n primes and denote by $\Phi(m, n)$ the number of natural numbers not greater than m which are divisible by no p_i. Then

$$\Phi(m, n) = \Phi(m, n-1) - \Phi\left(\left\lfloor \frac{m}{p_n} \right\rfloor, n-1\right).$$

Given a natural number m, if $n = \pi\left(\sqrt[3]{m}\right)$ and if $\mu = \pi\left(\sqrt{m}\right) - n$, then

$$\pi(m) = \Phi(m, n) + n(\mu + 1) + \frac{\mu^2 - \mu}{2} - 1 - \sum_{k=1}^{\mu} \pi\left(\frac{m}{p_{n+k}}\right).$$

Using this approach, Meissel computed $\pi(x)$, for x equal to 5×10^5, 10^6, 10^7, and 10^8.

In 1959, Derrick Henry Lehmer extended and simplified Meissel's method. Define, for real m and for natural numbers n, and k, $P_k(m, n)$ as the number of numbers not greater than *m* with exactly *k* prime factors, all greater than p_n. Furthermore, set $P_0(m, n) = 1$. Then

$$\Phi(m, n) = \sum_{k=0}^{+\infty} P_k(m, n),$$

where the sum actually has only finitely many nonzero terms. Let y denote an integer such that $\sqrt[3]{m} \le y \le \sqrt{m}$, and set $n = \pi(y)$. Then $P_1(m, n) = \pi(m) - n$ and $P_k(m, n) = 0$ when $k \ge 3$. Therefore

$$\pi(m) = \Phi(m, n) + n - 1 - P_2(m, n).$$

The computation of $P_2(m, n)$ can be obtained this way:

$$P_2(m, n) = \sum_{y < p \le \sqrt{m}} \left(\pi\left(\frac{m}{p}\right) - \pi(p) + 1\right).$$

On the other hand, the computation of $\Phi(m, n)$ can be done using the following rules:

1. $\Phi(m, 0) = \lfloor m \rfloor$;
2. $\Phi(m, b) = \Phi(m, b-1) - \Phi\left(\frac{m}{p_b}, b-1\right)$.

Using his method and an IBM 701, Lehmer was able to compute $\pi\left(10^{10}\right)$.

Further improvements to this method were made by Lagarias, Miller, Odlyzko, Deléglise and Rivat [13].

The Chinese mathematician Hwang Cheng, in a conference about prime number functions at the University of Bordeaux[14], used the following identities:

$$e^{(a-1)\Theta} f(x) = f(ax),$$

$$J(x) = \sum_{n=1}^{\infty} \frac{\pi(x^{1/n})}{n},$$

and setting $x = e^t$, Laplace-transforming both sides and applying a geometric sum on $e^{n\Theta}$got the expression

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} g(s) t^s \, ds = \pi(t),$$

$$\frac{\ln \zeta(s)}{s} = (1 - e^{\Theta(s)})^{-1} g(s)$$

$$\Theta(s) = s \frac{d}{ds}.$$

Other prime-counting functions

Other prime-counting functions are also used because they are more convenient to work with. One is Riemann's prime-counting function, usually denoted as $\Pi_0(x)$ or $J_0(x)$. This has jumps of *1/n* for prime powers p^n, with it taking a value half-way between the two sides at discontinuities. That added detail is because then it may be defined by an inverse Mellin transform. Formally, we may define $\Pi_0(x)$ by

$$\Pi_0(x) = \frac{1}{2}\left(\sum_{p^n < x} \frac{1}{n} + \sum_{p^n \le x} \frac{1}{n} \right)$$

where *p* is a prime.

We may also write

$$\Pi_0(x) = \sum_{2}^{x} \frac{\Lambda(n)}{\ln n} - \frac{1}{2} \frac{\Lambda(x)}{\ln x} = \sum_{n=1}^{\infty} \frac{1}{n} \pi_0(x^{1/n})$$

where Λ(*n*) is the von Mangoldt function and

$$\pi_0(x) = \lim_{\varepsilon \to 0} \frac{\pi(x-\varepsilon) + \pi(x+\varepsilon)}{2}.$$

Möbius inversion formula then gives

$$\pi_0(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \Pi_0(x^{1/n})$$

Knowing the relationship between log of the Riemann zeta function and the von Mangoldt function Λ, and using the Perron formula we have

$$\ln \zeta(s) = s \int_0^{\infty} \Pi_0(x) x^{-s-1} \, dx$$

The Chebyshev function weights primes or prime powers p^n by ln(*p*):

$$\theta(x) = \sum_{p \le x} \ln p$$

$$\psi(x) = \sum_{p^n \le x} \ln p = \sum_{n=1}^{\infty} \theta(x^{1/n}) = \sum_{n \le x} \Lambda(n).$$

Formulas for prime-counting functions

These come in two kinds, arithmetic formulas and analytic formulas. The latter are what allow us to prove the prime number theorem. They stem from the work of Riemann and von Mangoldt, and are generally known as explicit formulas [15].

We have the following expression for ψ:

$$\psi_0(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \ln 2\pi - \frac{1}{2}\ln(1 - x^{-2})$$

where

$$\psi_0(x) = \lim_{\varepsilon \to 0} \frac{\psi(x-\varepsilon) + \psi(x+\varepsilon)}{2}.$$

Here ρ are the zeros of the Riemann zeta function in the critical strip, where the real part of ρ is between zero and one. The formula is valid for values of x greater than one, which is the region of interest. The sum over the roots is conditionally convergent, and should be taken in order of increasing absolute value of the imaginary part. Note that the same sum over the trivial roots gives the last subtrahend in the formula.

For $\Pi_0(x)$ we have a more complicated formula

$$\Pi_0(x) = \operatorname{li}(x) - \sum_\rho \operatorname{li}(x^\rho) - \ln 2 + \int_x^\infty \frac{dt}{t(t^2-1)\ln t}.$$

Again, the formula is valid for $x > 1$, while ρ are the nontrivial zeros of the zeta function ordered according to their absolute value, and, again, the latter integral, taken with minus sign, is just the same sum, but over the trivial zeros. The first term li(x) is the usual logarithmic integral function; the expression li(x^ρ) in the second term should be considered as Ei(ρ ln x), where Ei is the analytic continuation of the exponential integral function from positive reals to the complex plane with branch cut along the negative reals.

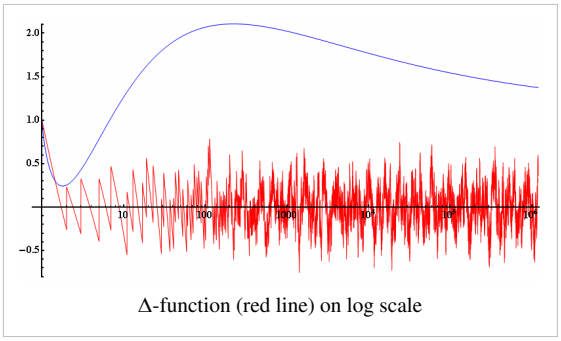
Thus, Möbius inversion formula gives us[16]

$$\pi_0(x) = \mathrm{R}(x) - \sum_\rho \mathrm{R}(x^\rho) - \frac{1}{\ln x} + \frac{1}{\pi}\arctan\frac{\pi}{\ln x}$$

valid for $x > 1$, where

$$\mathrm{R}(x) = \sum_{n=1}^\infty \frac{\mu(n)}{n}\operatorname{li}(x^{1/n}) = 1 + \sum_{k=1}^\infty \frac{(\ln x)^k}{k!k\zeta(k+1)}$$

is so-called Riemann's R-function [17]. The latter series for it is known as Gram series [18] and converges for all positive x.



Λ-function (red line) on log scale

The sum over non-trivial zeta zeros in the formula for $\pi_0(x)$ describes the fluctuations of $\pi_0(x)$, while the remaining terms give the "smooth" part of prime-counting function [19], so one can use

$$\mathrm{R}(x) - \frac{1}{\ln x} + \frac{1}{\pi}\arctan\frac{\pi}{\ln x}$$

as the best estimator [20] of $\pi(x)$ for $x > 1$.

The amplitude of the "noisy" part is heuristically about $\sqrt{x}/\ln x$, so the fluctuations of the distribution of primes may be clearly represented with the Δ-function:

$$\Delta(x) = \left(\pi_0(x) - \mathrm{R}(x) + \frac{1}{\ln x} - \frac{1}{\pi}\arctan\frac{\pi}{\ln x}\right)\frac{\ln x}{\sqrt{x}}.$$

An extensive table of the values of $\Delta(x)$ is available [7].

Inequalities

Here are some useful inequalities for $\pi(x)$.

$$\pi(x) < 1.25506\frac{x}{\log x} \text{ for } x > 1.$$

$$\frac{x}{\log x + 2} < \pi(x) < \frac{x}{\log x - 4} \text{ for } x \geq 55.$$

Here are some inequalities for the n^{th} prime, p_n.

$$n\ \ln n + n\ln\ln n - n < p_n < n\ln n + n\ln\ln n \text{ for } n \geq 6.$$

The left inequality holds for $n \geq 1$ and the right inequality holds for $n \geq 6$.

An approximation for the n^{th} prime number is

$$p_n = n\ln n + n\ln\ln n - n + \frac{n\ln\ln n - 2n}{\ln n} + O\left(\frac{n(\ln\ln n)^2}{(\ln n)^2}\right).$$

The Riemann hypothesis

The Riemann hypothesis is equivalent to a much tighter bound on the error in the estimate for $\pi(x)$, and hence to a more regular distribution of prime numbers,

$$\pi(x) = \mathrm{li}(x) + O(\sqrt{x}\log x).$$

Specifically,[21]

$$|\pi(x) - \mathrm{li}(x)| < \frac{1}{8\pi}\sqrt{x}\,\log(x), \qquad \text{for all } x \geq 2657.$$

See also

- Bertrand's postulate
- Opperman's conjecture

References

[1] Bach, Eric; Shallit, Jeffrey (1996). *Algorithmic Number Theory*. MIT Press. volume 1 page 234 section 8.8. ISBN 0-262-02405-5.

[2] Weisstein, Eric W., " Prime Counting Function (http://mathworld.wolfram.com/PrimeCountingFunction.html)" from MathWorld.

[3] "How many primes are there?" (http://primes.utm.edu/howmany.shtml). Chris K. Caldwell. . Retrieved 2008-12-02.

[4] Dickson, Leonard Eugene (2005). *History of the Theory of Numbers I: Divisibility and Primality*. Dover Publications. ISBN 0-486-44232-2.

[5] Ireland, Kenneth; Rosen, Michael (1998). *A Classical Introduction to Modern Number Theory* (Second ed.). Springer. ISBN 0-387-97329-X.

[6] "Tables of values of pi(x) and of pi2(x)" (http://www.ieeta.pt/~tos/primes.html). Tomás Oliveira e Silva. . Retrieved 2008-09-14.

[7] "Values of π(x) and Δ(x) for various x's" (http://www.primefan.ru/stuff/primes/table.html). Andrey V. Kulsha. . Retrieved 2008-09-14.

[8] "A table of values of pi(x)" (http://numbers.computation.free.fr/Constants/Primes/pixtable.html). Xavier Gourdon, Pascal Sebah, Patrick Demichel. . Retrieved 2008-09-14.

[9] http://en.wikipedia.org/wiki/Oeis%3Aa006880

[10] http://en.wikipedia.org/wiki/Oeis%3Aa057835

[11] http://en.wikipedia.org/wiki/Oeis%3Aa057752

[12] "Conditional Calculation of pi(10^{24})" (http://primes.utm.edu/notes/pi(10^24).html). Chris K. Caldwell. . Retrieved 2010-08-03.

[13] "Computing π(x): The Meissel, Lehmer, Lagarias, Miller, Odlyzko method" (http://www.ams.org/mcom/1996-65-213/S0025-5718-96-00674-6/S0025-5718-96-00674-6.pdf). Marc Deléglise and Jöel Rivat, *Mathematics of Computation*, vol. **65**, number 33, January 1996, pages 235–245. . Retrieved 2008-09-14.

[14] Hwang H., Cheng (2001), *Démarches de la Géométrie et des Nombres de l'Université du Bordeaux*, *Prime Magic* conference

[15] Titchmarsh, E.C. (1960). *The Theory of Functions, 2nd ed.*. Oxford University Press.

[16] Riesel, Hans; Göhl, Gunnar (1970). "Some calculations related to Riemann's prime number formula" (http://jstor.org/stable/2004630). *Mathematics of Computation* (American Mathematical Society) **24** (112): 969–983. doi:10.2307/2004630. MR0277489. ISSN 0025-5718. .

[17] Weisstein, Eric W., " Riemann Prime Counting Function (http://mathworld.wolfram.com/RiemannPrimeCountingFunction.html)" from MathWorld.

[18] Weisstein, Eric W., " Gram Series (http://mathworld.wolfram.com/GramSeries.html)" from MathWorld.

[19] "The encoding of the prime distribution by the zeta zeros" (http://www.secamlocal.ex.ac.uk/people/staff/mrwatkin/zeta/encoding1.htm). Matthew Watkins. . Retrieved 2008-09-14.

[20] http://primefan.ru:8014/WWW/stuff/primes/best_estimator.gif

[21] Schoenfeld, Lowell (1976). "Sharper bounds for the Chebyshev functions θ(x) and ψ(x). II" (http://jstor.org/stable/2005976). *Mathematics of Computation* (American Mathematical Society) **30** (134): 337–360. doi:10.2307/2005976. MR0457374. ISSN 0025-5718. .

External links

- Chris Caldwell, *The Nth Prime Page* (http://primes.utm.edu/nthprime/) at The Prime Pages.

Primeval prime

In mathematics, a **primeval number** is a natural number *n* for which the number of prime numbers which can be obtained by permuting all or some of its digits (in base 10) is larger than the number of primes obtainable in the same way for any smaller natural number. Primeval numbers were first described by Mike Keith.

The first few primeval numbers are

1, 2, 13, 37, 107, 113, 137, 1013, 1037, 1079, 1237, 1367, ... (sequence A072857 [1] in OEIS)

The number of primes that can be obtained from the primeval numbers is

0, 1, 3, 4, 5, 7, 11, 14, 19, 21, 26, 29, ... (A076497 [2])

The largest number of primes that can be obtained from a primeval number with *n* digits is

1, 4, 11, 31, 106, ... (A076730 [3])

The smallest *n*-digit prime to achieve this number of primes is

2, 37, 137, 1379, 13679, ... (A134596 [4])

Primeval numbers can be composite. The first is 1037 = 17×61. A **Primeval prime** is a primeval number which is also a prime number:

2, 13, 37, 107, 113, 137, 1013, 1237, 1367, 10079, ... (A119535 [34])

The following table shows the first six primeval numbers with the obtainable primes and the number of them.

Primeval number	Primes obtained	Number of primes
A072857 [1]	(ordered permutations)	A076497 [2]
1	none	0
2	2	1
13	3, 13, 31	3
37	3, 7, 37, 73	4
107	7, 17, 71, 107, 701	5
113	3, 11, 13, 31, 113, 131, 311	7

See also

- Permutable prime
- Truncatable prime

External links

- Chris Caldwell, The Prime Glossary: Primeval number [5] at The Prime Pages
- Mike Keith, *Integers Containing Many Embedded Primes* [6]

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa072857
[2] http://en.wikipedia.org/wiki/Oeis%3Aa076497
[3] http://en.wikipedia.org/wiki/Oeis%3Aa076730
[4] http://en.wikipedia.org/wiki/Oeis%3Aa134596
[5] http://primes.utm.edu/glossary/page.php?sort=Primeval
[6] http://www.cadaeic.net/primeval.htm

Primorial prime

In mathematics, **primorial primes** are prime numbers of the form $p_n\# \pm 1$, where:

$p_n\#$ is the primorial of p_n (that is, the product of the first n primes).

$p_n\# - 1$ is prime for n = 2, 3, 5, 6, 13, 24, ... (sequence A057704 [1] in OEIS)

$p_n\# + 1$ is prime for n = 1, 2, 3, 4, 5, 11, ... (A014545 [2])

The first few primorial primes are

3, 5, 7, 29, 31, 211, 2309, 2311, 30029, 200560490131, 304250263527209

As of 2010, the largest known primorial prime is 843301# - 1 with 365,851 digits, found in 2010 by the PrimeGrid project.[3]

It is widely believed, but false, that the idea of primorial primes appears in Euclid's proof of the infinitude of the prime numbers: First, assume that the first n primes are the only primes that exist. If either $p_n\# + 1$ or $p_n\# - 1$ is a primorial prime, it means that there are larger primes than the nth prime (if neither is a prime, that also proves the infinitude of primes, but less directly; note that each of these two numbers has a remainder of either $p-1$ or 1 when divided by any of the first n primes, and hence cannot be a multiple of any of them).

In fact, Euclid's proof did not assume that a finite set contains all primes that exist. Rather, it said: consider any finite set of primes (not necessarily the first n primes; e.g. it could have been the set {3, 11, 47}), and then went on from there to the conclusion that at least one prime exists that is not in that set. [4]

See also

- Primorial
- Factorial prime
- Euclid number
- PrimeGrid

References

- A. Borning, "Some Results for $k! + 1$ and $2 \cdot 3 \cdot 5 \cdot p + 1$" *Math. Comput.* **26** (1972): 567 - 570.
- Chris Caldwell, *The Top Twenty: Primorial* [5] at The Prime Pages.
- Weisstein, Eric W., "Primorial Prime [6]" from MathWorld.
- Harvey Dubner, "Factorial and Primorial Primes." *J. Rec. Math.* **19** (1987): 197 - 203.
- Paulo Ribenboim, *The New Book of Prime Number Records*. New York: Springer-Verlag (1989): 4.

[1] http://en.wikipedia.org/wiki/Oeis%3Aa057704

[2] http://en.wikipedia.org/wiki/Oeis%3Aa014545

[3] Primegrid.com (http://www.primegrid.com/download/prs-843301.pdf); official anouncement, 24 December 2010

[4] http://aleph0.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html

[5] http://primes.utm.edu/top20/page.php?id=5

[6] http://mathworld.wolfram.com/PrimorialPrime.html

Probable prime

In number theory, a **probable prime (PRP)** is an integer that satisfies a specific condition also satisfied by all prime numbers. Different types of probable primes have different specific conditions. While there may be probable primes that are composite (called pseudoprimes), the condition is generally chosen in order to make such exceptions rare.

Fermat's test for compositeness, which is based on Fermat's little theorem, works as follows: given an integer n, choose some integer a coprime to n and calculate a^{n-1} modulo n. If the result is different from 1, n is composite. If it is 1, n may or may not be prime; n is then called a **(weak) probable prime to base** a.

Properties

Probable primality is a basis for efficient primality testing algorithms, which find application in cryptography. These algorithms are usually probabilistic in nature. The idea is that while there are composite probable primes to base a for any fixed a, we may hope there exists some fixed $P<1$ such that for *any* given composite n, if we choose a randomly the probability that n is pseudoprime to base a is at most P. If we repeat this test k times, choosing a new a each time, the probability of n being pseudoprime to all the as tested is hence at most P^k, and as this decreases exponentially, only moderate k is required to make this probability negligibly small (compared to, for example, the probability of computer hardware error).

This is unfortunately false for weak probable primes, because there exist Carmichael numbers; but it is true for more refined notions of probable primality, such as strong probable primes ($P = 1/4$, Miller–Rabin algorithm), or Euler probable primes ($P = 1/2$, Solovay–Strassen algorithm).

Even when a deterministic primality proof is required, a useful first step is to test for probable primality. This can quickly eliminate (with certainty) most composites.

A PRP test is sometimes combined with a table of small pseudoprimes to quickly establish the primality of a given number smaller than some threshold.

Variations

An **Euler probable prime to base** a is an integer that is indicated prime by the somewhat stronger theorem that for any prime p, $a^{(p-1)/2}$ equals $\left(\frac{a}{p}\right)$ modulo p, where $\left(\frac{a}{p}\right)$ is the Legendre symbol. An Euler probable prime which is composite is called an Euler–Jacobi pseudoprime to base a.

This test may be improved by using the fact that the only square roots of 1 modulo a prime are 1 and −1. Write $n = d \cdot 2^s + 1$, where d is odd. The number n is a **strong probable prime (SPRP) to base** a if one of the following conditions holds:

$$a^d \equiv 1 \pmod{n},$$
$$a^{d \cdot 2^r} \equiv -1 \pmod{n} \text{ for some } 0 \leq r \leq s-1.$$

A composite strong probable prime to base a is called a strong pseudoprime to base a. Every strong probable prime to base a is also an Euler probable prime to the same base, but not vice versa.

External links

- The prime glossary – Probable prime [1]
- The PRP Top 10000 (the largest known probable primes) [2]
- Generalized repunit probable primes [3]

References

[1] http://primes.utm.edu/glossary/page.php?sort=PRP
[2] http://www.primenumbers.net/prptop/
[3] http://phi.redgolpe.com

Proth number

In number theory, a **Proth number**, named after the mathematician François Proth, is a number of the form

$$k \cdot 2^n + 1$$

where k is an odd positive integer and n is a positive integer such that $2^n > k$. Without the latter condition, all odd integers greater than 1 would be Proth numbers.[1]

The first Proth numbers are (sequence A080075 [2] in OEIS):

3, 5, 9, 13, 17, 25, 33, 41, 49, 57, 65, 81, 97, 113, 129, 145, 161, 177, 193, 209, 225

The Cullen numbers ($n \cdot 2^n+1$) and Fermat numbers (2^2n+1) are special cases of Proth numbers.

Proth primes

A **Proth prime** is a Proth number which is prime. The first Proth primes are (A080076 [36]):

3, 5, 13, 17, 41, 97, 113, 193, 241, 257, 353, 449, 577, 641, 673, 769, 929, 1153, 1217, 1409, 1601, 2113, 2689, 2753, 3137, 3329, 3457, 4481, 4993, 6529, 7297, 7681, 7937, 9473, 9601, 9857.

The primality of a Proth number can be tested with Proth's theorem which states[3] that a Proth number p is prime if and only if there exists an integer a for which the following is true:

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

The largest known Proth prime as of 2010 is $19249 \cdot 2^{13018586} + 1$.[4] It was found by Konstantin Agafonov in the Seventeen or Bust distributed computing project which announced it 5 May 2007.[5] It is also the largest known non-Mersenne prime.[6]

References

[1] Weisstein, Eric W., " Proth Number (http://mathworld.wolfram.com/ProthNumber.html)" from MathWorld.
[2] http://en.wikipedia.org/wiki/Oeis%3Aa080075
[3] Weisstein, Eric W., " Proth's Theorem (http://mathworld.wolfram.com/ProthsTheorem.html)" from MathWorld.
[4] Chris Caldwell, The Top Twenty: Proth (http://primes.utm.edu/top20/page.php?id=66), from The Prime Pages.
[5] Press Release by Seventeen or Bust (http://www.seventeenorbust.com/documents/press-050507.mhtml). 5 May 2007.
[6] Chris Caldwell, The Top Twenty: Largest Known Primes (http://primes.utm.edu/top20/page.php?id=3), from The Prime Pages.

Pseudoprime

A **pseudoprime** is a probable prime (an integer that shares a property common to all prime numbers) which is not actually prime. Pseudoprimes can be classified according to which property they satisfy.

Fermat pseudoprimes

Fermat's little theorem states that if p is prime and a is coprime to p, then $a^{p-1} - 1$ is divisible by p. If a composite integer x is coprime to an integer $a > 1$ and x divides $a^{x-1} - 1$, then x is called a Fermat pseudoprime to base a. Some sources use variations of this definition, for example to only allow odd numbers to be pseudoprimes.[1]

An integer x that is a Fermat pseudoprime to all values of a that are coprime to x is called a Carmichael number.

Classes

- Fermat pseudoprime
- Euler pseudoprime
- Euler–Jacobi pseudoprime
- Extra strong Lucas pseudoprime
- Fibonacci pseudoprime
- Lucas pseudoprime
- Perrin pseudoprime
- Somer–Lucas pseudoprime
- Strong Frobenius pseudoprime
- Strong Lucas pseudoprime
- Strong pseudoprime

References

[1] Weisstein, Eric W., " Fermat Pseudoprime (http://mathworld.wolfram.com/FermatPseudoprime.html)" from MathWorld.

Pythagorean prime

A **Pythagorean prime** is prime number of the form $4n + 1$. These are exactly the primes that can be the hypotenuse of a Pythagorean triangle.

The first few Pythagorean primes are

5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, … (sequence A002144 [2] in OEIS).

Fermat's theorem on sums of two squares states that these primes can be represented as sums of two squares uniquely (up to order), and that no other primes can be represented this way, aside from $2=1^2+1^2$. Thus these primes (and 2) occur as norms of Gaussian integers, while other primes do not.

The law of quadratic reciprocity says that if p and q are odd primes, at least one of which is Pythagorean, then p is a quadratic residue mod q if and only if q is a quadratic residue mod p; by contrast, if neither p nor q is Pythagorean, then p is a quadratic residue mod q if and only if q is **not** a quadratic residue mod p. -1 is a quadratic residue mod p if and only if p is a Pythagorean prime (or 2).

In the field Z/p with p a Pythagorean prime, the polynomial x^2 = -1 has two solutions.

Ramanujan prime

In mathematics, a **Ramanujan prime** is a prime number that satisfies a result proven by Srinivasa Ramanujan relating to the prime-counting function.

Origins and definition

In 1919, Ramanujan published a new proof of Bertrand's postulate which, as he says, was first proved by Chebyshev.[1] At the end of the two-page published paper, Ramanujan derived a generalized result, and that is:

$\pi(x) - \pi(x/2) \geq$ 1, 2, 3, 4, 5, ... for all $x \geq$ 2, 11, 17, 29, 41, ... (sequence A104272 [41] in OEIS) respectively,

where $\pi(x)$ is the prime-counting function, that is, the number of primes less than or equal to x.

The converse of this result is the definition of Ramanujan primes, and the numbers 2, 11, 17, 29, 41 are the first few such primes. In other words:

The nth Ramanujan prime is the integer R_n that is the **smallest** to satisfy the condition

$\pi(x) - \pi(x/2) \geq n$, for all $x \geq R_n$.[2]

Another way to put this is:

Ramanujan primes are the integers R_n that are the **smallest** to guarantee there are n primes between x and $x/2$ for all $x \geq R_n$.

Since R_n is the smallest such number, it must be a prime: $\pi(x) - \pi(x/2)$ and, hence, $\pi(x)$ must increase by obtaining another prime at $x = R_n$. Since $\pi(x) - \pi(x/2)$ can increase by at most 1,

$\pi(R_n) - \pi(R_n/2) = n$.

Bounds and an asymptotic formula

For all $n \geq 1$, the bounds

$$2n \ln 2n < R_n < 4n \ln 4n$$

hold. If $n > 1$, then also

$$p_{2n} < R_n < p_{3n},$$

where p_n is the nth prime number.

As n tends to infinity, R_n is asymptotic to the $2n$th prime, i.e.,

$$R_n \sim p_{2n} \ (n \to \infty).$$

All these results were proved by Sondow (2009),[3] except for the upper bound $R_n < p_{3n}$ which was conjectured by him and proved by Laishram (2010).[4]

Ramanujan prime corollary

$$2p_{i-n} > p_i \text{ for } i > k \text{ where } k = \pi(p_k) = \pi(R_n)\,,$$

i.e. p_k is the kth prime and the nth Ramanujan prime.

This is very useful in showing the number of primes in the range $[p_k, 2*p_{i-n}]$ is greater than or equal to 1. By taking into account the size of the gaps between primes in $[p_{i-n},p_k]$, one can see that the average prime gap is about $\ln(p_k)$ using the following $R_n / (2*n) \sim \ln(R_n)$.

Proof of Corollary: If $p_i > R_n$, then p_i is odd and $p_i - 1 \geq R_n$, and hence $\pi(p_i - 1) - \pi(p_i / 2) = \pi(p_i - 1) - \pi((p_i - 1) / 2) \geq n$. Thus $p_i - 1 \geq p_{i-1} > p_{i-2} > p_{i-3} > ... > p_{i-n} > p_i / 2$, and so $2 p_{i-n} > p_i$.

An example of this corollary:

With n = 1000, R_n = p_k = 19403, and k = 2197, therefore i ≥ 2198 and i-n ≥ 1198. The smallest i-n prime is p_{i-n} = 9719, therefore 2 * p_{i-n} = 2 * 9719 = 19438. The 2198th prime, p_i, is between p_k = 19403 and 2 * p_{i-n} = 19438 and is 19417.

References

[1] Ramanujan, S. (1919), "A proof of Bertrand's postulate" (http://www.imsc.res.in/~rao/ramanujan/CamUnivCpapers/Cpaper24/page1.htm), *Journal of the Indian Mathematical Society* **11**: 181–182,

[2] Jonathan Sondow, " Ramanujan Prime (http://mathworld.wolfram.com/RamanujanPrime.html)" from MathWorld.

[3] Sondow, J. (2009), "Ramanujan primes and Bertrand's postulate", *Amer. Math. Monthly* **116**: 630–635, arXiv:0907.5232

[4] Laishram, S. (2010), "On a conjecture on Ramanujan primes" (http://www.mendeley.com/download/public/460091/1703715971/192edbf2a1d55948919e050abff63f6ba54cae60/dl.pdf), *International Journal of Number Theory*, .

Regular prime

In number theory, a **regular prime** is a prime number $p > 2$ that does not divide the class number of the p-th cyclotomic field. Ernst Kummer (Kummer 1850) showed that an equivalent criterion for regularity is that p does not divide the numerator of any of the Bernoulli numbers B_k for $k = 2, 4, 6, \ldots, p - 3$. This is called **Kummer's criterion**. Kummer was able to prove that Fermat's last theorem holds true for regular prime exponents.

The first few regular primes are: 3, 5, 7, 11, 13, 17, 19, 23, 29, ... (sequence A007703 [1] in OEIS).

It has been conjectured that there are infinitely many regular primes. More precisely Siegel conjectured (1964) that $e^{-1/2}$, or about 61%, of all prime numbers are regular, in the asymptotic sense of natural density. Neither conjecture has been proven as of 2010.

An odd prime that is not regular is an **irregular prime**. The number of Bernoulli numbers B_k with a numerator divisible by p is called the **irregularity index** of p. K. L. Jensen has shown in 1915 that there are infinitely many irregular primes.

The first few irregular primes are: 37, 59, 67, 101, 103, 131, 149, ... (sequence A000928 [2] in OEIS)

References

- Kummer, E. E. (1850), "Allgemeiner Beweis des Fermat'schen Satzes, dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten (λ-3)/2 Bernoulli'schen Zahlen als Factoren nicht vorkommen" [3], *J. Reine Angew. Math.* **40**: 131–138.
- Keith Conrad, *Fermat's last theorem for regular primes* [4].
- Richard K. Guy, *Unsolved Problems in Number Theory* (3rd ed), Springer Verlag, 2004 ISBN 0-387-20860-7; section D2.
- Carl Ludwig Siegel, *Zu zwei Bemerkungen Kummers.* Nachr. Akad. d. Wiss. Goettingen, Math. Phys. K1., II, 1964, 51-62.

External links

- Chris Caldwell, The Prime Glossary: regular prime [5] at The Prime Pages.

Repunit

In recreational mathematics, a **repunit** is a number like 11, 111, or 1111 that contains only the digit 1. The term stands for **rep**eated **unit** and was coined in 1966 by Albert H. Beiler. A **repunit prime** is a repunit that is also a prime number.

Definition

The base-*b* repunits are defined as

$$R_n^{(b)} = \frac{b^n - 1}{b - 1} \qquad \text{for } b \geq 2, n \geq 1.$$

Thus, the number $R_n^{(b)}$ consists of *n* copies of the digit 1 in base b representation. The first two repunits base *b* for *n*=1 and *n*=2 are

$$R_1^{(b)} = \frac{b - 1}{b - 1} = 1 \qquad \text{and} \qquad R_2^{(b)} = \frac{b^2 - 1}{b - 1} = b + 1 \qquad \text{for } b \geq 2.$$

In particular, the *decimal (base-10) repunits* that are often referred to as simply *repunits* are defined as

$$R_n = R_n^{(10)} = \frac{10^n - 1}{10 - 1} = \frac{10^n - 1}{9} \qquad \text{for } n \geq 1.$$

Thus, the number $R_n = R_n^{(10)}$ consists of *n* copies of the digit 1 in base 10 representation. The sequence of repunits base 10 starts with

1, 11, 111, 1111, ... (sequence A002275 [1] in OEIS).

Similarly, the repunits base 2 are defined as

$$R_n^{(2)} = \frac{2^n - 1}{2 - 1} = 2^n - 1 \qquad \text{for } n \geq 1.$$

Thus, the number $R_n^{(2)}$ consists of *n* copies of the digit 1 in base 2 representation. In fact, the base-2 repunits are the well-respected Mersenne numbers $M_n = 2^n - 1$.

Properties

- Any repunit in any base having a composite number of digits is necessarily composite. Only repunits (in any base) having a prime number of digits might be prime (necessary but not sufficient condition). For example,

  $R_{35}^{(b)}$ = 11111111111111111111111111111111111 = 11111 × 100001000010000100001000010000100001 = 1111111 × 100000010000001000000010000001,

  since 35 = 7 × 5 = 5 × 7. This repunit factorization does not depend on the base *b* in which the repunit is expressed.
- Any positive multiple of the repunit $R_n^{(b)}$ contains at least *n* nonzero digits in base *b*.
- The only known numbers that are repunits with at least 3 digits in more than one base simultaneously are 31 (111 in base 5, 11111 in base 2) and 8191 (111 in base 90, 1111111111111 in base 2). The Goormaghtigh conjecture says there are only these two cases.
- It is easy to prove[2] that given *n*, such that *n* is not exactly divisible by 2 or *p*, there exists a repunit in base 2*p* that is a multiple of *n*.

Factorization of decimal repunits

$R_1 = 1$

$R_2 = 11$

$R_3 = 3 \cdot 37$

$R_4 = 11 \cdot 101$

$R_5 = 41 \cdot 271$

$R_6 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$

$R_7 = 239 \cdot 4649$

$R_8 = 11 \cdot 73 \cdot 101 \cdot 137$

$R_9 = 3 \cdot 3 \cdot 37 \cdot 333667$

$R_{10} = 11 \cdot 41 \cdot 271 \cdot 9091$

$R_{11} = 21649 \cdot 513239$

$R_{12} = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901$

$R_{13} = 53 \cdot 79 \cdot 265371653$

$R_{14} = 11 \cdot 239 \cdot 4649 \cdot 909091$

$R_{15} = 3 \cdot 31 \cdot 37 \cdot 41 \cdot 271 \cdot 2906161$

$R_{16} = 11 \cdot 17 \cdot 73 \cdot 101 \cdot 137 \cdot 5882353$

$R_{17} = 2071723 \cdot 5363222357$

$R_{18} = 3 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 37 \cdot 52579 \cdot 333667$

$R_{19} = 1111111111111111111$

$R_{20} = 11 \cdot 41 \cdot 101 \cdot 271 \cdot 3541 \cdot 9091 \cdot 27961$

Repunit primes

The definition of repunits was motivated by recreational mathematicians looking for prime factors of such numbers. It is easy to show that if *n* is divisible by *a*, then $R_n^{(b)}$ is divisible by $R_a^{(b)}$:

$$R_n^{(b)} = \frac{1}{b-1} \prod_{d|n} \Phi_d(b)$$

where $\Phi_d(x)$ is the d^{th} cyclotomic polynomial and *d* ranges over the divisors of *n*. For *p* prime, $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$, which has the expected form of a repunit when *x* is substituted with *b*.

For example, 9 is divisible by 3, and thus R_9 is divisible by R_3—in fact, $111111111 = 111 \cdot 1001001$. The corresponding cyclotomic polynomials $\Phi_3(x)$ and $\Phi_9(x)$ are $x^2 + x + 1$ and $x^6 + x^3 + 1$ respectively. Thus, for R_n to be prime *n* must necessarily be prime. But it is not sufficient for *n* to be prime; for example, $R_3 = 111 = 3 \cdot 37$ is not prime. Except for this case of R_3, *p* can only divide R_n for prime *n* if *p = 2kn + 1* for some *k*.

Decimal repunit primes

R_n is prime for n = 2, 19, 23, 317, 1031,... (sequence A004023 in OEIS). R_{49081} and R_{86453} are probably prime. On April 3, 2007 Harvey Dubner (who also found R_{49081}) announced that R_{109297} is a probable prime.[3] He later announced there are no others from R_{86453} to R_{200000}.[4] On July 15, 2007 Maksym Voznyy announced R_{270343} to be probably prime [5] , along with his intent to search to 400000. As of September 2010, all further candidates up to $R_{1300000}$ have been tested, but no new probable primes have been found so far.

It has been conjectured that there are infinitely many repunit primes[6] and they seem to occur roughly as often as the prime number theorem would predict: the exponent of the *N*th repunit prime is generally around a fixed multiple of the exponent of the (*N*-1)th.

The prime repunits are a trivial subset of the permutable primes, i.e., primes that remain prime after any permutation of their digits.

Base-2 repunit primes

See the article on Mersenne primes.

Base-3 repunit primes

The first few base-3 repunit primes are

13, 1093, 797161, 375473325748986240197335797912877 3,
695759652988215296899222525183588718147845154701 3, ... (sequence A076481 [7] in OEIS),

corresponding to n of

3, 7, 13, 71, 103, ... (sequence A028491 [8] in OEIS).

Base-4 repunit primes

The only base-4 repunit prime is 5 (11_4). $4^n - 1 = (2^n + 1)(2^n - 1)$, and 3 always divides $2^n + 1$ when *n* is odd and $2^n - 1$ when *n* is even.

These repunits factor as follows: $1 \cdot 1, 1 \cdot 5, 3 \cdot 7, 5 \cdot 17, 11 \cdot 31, 21 \cdot 65, \cdots,$ so no repunit after the second (11_4 = 5) can be prime.

Base 5 repunit primes

The first few base-5 (quinary) repunit primes are

31, 19531, 12207031, 305175781, 177635683940025046467781066894531, (sequence A086122 [9] in OEIS)

corresponding to n of

3, 7, 11, 13, 47, ... (sequence A004061 [10] in OEIS).

Base 6 repunit primes

The first few base-6 repunit primes are

7, 43, 55987, 7369130657357778596659,
3546245297457217493590449191748546458005595187661976371, ..., (sequence A165210 [11] in OEIS)

corresponding to n of

2, 3, 7, 29, 71, ... (sequence A004062 [12] in OEIS)

Base 7 repunit primes

The first few base 7 repunit primes are

2801, 16148168401,
85053461164796801949539541639542805770666392330682673302530819774105141531698707146930307290253537320
13850221271010340870077438103313550392666332499331763172922779065732516331034183322777594542605263709

corresponding to n of

5, 13, 131, 149, ... (sequence A004063 [13] in OEIS)

Base 8 and 9 repunit primes

The only base-8 *or* base-9 repunit prime is 73 (111_8). $8^n - 1 = (4^n + 2^n + 1)(2^n - 1)$, and 7 divides $4^n + 2^n + 1$ when *n* is not divisible by 3 and $2^n - 1$ when *n* is a multiple of 3. $9^n - 1 = (3^n + 1)(3^n - 1)$, and 2 always divides both $3^n + 1$ and $3^n - 1$.

Factorization of base 8 and base 9 repunits

Base 8 repunits factor thus: $1 \cdot 1, 3 \cdot 3, 1 \cdot 73, 5 \cdot 39, 31 \cdot 151, 9 \cdot 4161, 127 \cdot 2359, \cdots,$ so no repunit except the third (111_8 = 73) can be prime.
Base 9 repunits factor thus: $2 \cdot 5, 7 \cdot 13, 20 \cdot 41, 61 \cdot 121, 182 \cdot 365, 547 \cdot 1093, \cdots,$

Base 20 (vigesimal) repunit primes

The only known vigesimal (base 20) repunit primes or probable primes are for n of

3, 11, 17, 1487, 31013, 48859, 61403 ((sequence A127995 [14] in OEIS))

The first three of these in decimal are

421, 10778947368421 and 689852631578947368421

History

Although they were not then known by that name, repunits in base 10 were studied by many mathematicians during the nineteenth century in an effort to work out and predict the cyclic patterns of recurring decimals[15] .

It was found very early on that for any prime *p* greater than 5, the period of the decimal expansion of 1/*p* is equal to the length of the smallest repunit number that is divisible by *p*. Tables of the period of reciprocal of primes up to 60,000 had been published by 1860 and permitted the factorization by such mathematicians as Reuschle of all repunits up to R_{16} and many larger ones. By 1880, even R_{17} had been factored[16] and it is curious that, though Edouard Lucas showed no prime below three million had period nineteen, there was no attempt to test any repunit for primality until early in the twentieth century. The American mathematician Oscar Hoppe proved R_{19} to be prime in 1916[17] and Lehmer and Kraitchik independently found R_{23} to be prime in 1929.

Further advances in the study of repunits did not occur until the 1960s, when computers allowed many new factors of repunits to be found and the gaps in earlier tables of prime periods corrected. R_{317} was found to be a probable prime circa 1966 and was proved prime eleven years later, when R_{1031} was shown to be the only further possible prime repunit with fewer than ten thousand digits. It was proven prime in 1986, but searches for further prime repunits in the following decade consistently failed. However, there was a major side-development in the field of generalized repunits, which produced a large number of new primes and probable primes.

Since 1999, four further probably prime repunits have been found, but it is unlikely that any of them will be proven prime in the foreseeable future because of their huge size.

The Cunningham project endeavours to document the integer factorizations of (among other numbers) the repunits to base 2, 3, 5, 6, 7, 10, 11, and 12.

Notes

[1] http://en.wikipedia.org/wiki/Oeis%3Aa002275
[2] (http://www.caliban.org.uk/pmwiki/pmwiki.php?n=Blogs.RichardRothwell.RepUnits)
[3] Harvey Dubner, *New Repunit R(109297)* (http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0704&L=nmbrthry&T=0&P=178)
[4] Harvey Dubner, *Repunit search limit* (http://tech.groups.yahoo.com/group/primeform/message/8546)
[5] Maksym Voznyy, *New PRP Repunit R(270343)* (http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0707&L=nmbrthry&T=0&P=1086)
[6] Chris Caldwell, " The Prime Glossary: repunit (http://primes.utm.edu/glossary/page.php?sort=Repunit)" at The Prime Pages.
[7] http://en.wikipedia.org/wiki/Oeis%3Aa076481
[8] http://en.wikipedia.org/wiki/Oeis%3Aa028491
[9] http://en.wikipedia.org/wiki/Oeis%3Aa086122
[10] http://en.wikipedia.org/wiki/Oeis%3Aa004061
[11] http://en.wikipedia.org/wiki/Oeis%3Aa165210
[12] http://en.wikipedia.org/wiki/Oeis%3Aa004062
[13] http://en.wikipedia.org/wiki/Oeis%3Aa004063
[14] http://en.wikipedia.org/wiki/Oeis%3Aa127995
[15] Dickson, Leonard Eugene and Cresse, G.H.; *History of the Theory of Numbers*; pp. 164-167 ISBN 0-8218-1934-8
[16] Dickson and Cresse, pp. 164-167
[17] Francis, Richard L.; "Mathematical Haystacks: Another Look at Repunit Numbers" in The College Mathematics Journal, Vol. 19, No. 3. (May, 1988), pp. 240-246.

External links

Web sites

- Weisstein, Eric W., " Repunit (http://mathworld.wolfram.com/Repunit.html)" from MathWorld.
- The main tables (http://www.cerias.purdue.edu/homes/ssw/cun/third/pmain901) of the Cunningham project (http://www.cerias.purdue.edu/homes/ssw/cun/).
- Repunit (http://primes.utm.edu/glossary/page.php?sort=Repunit) at The Prime Pages (http://primes.utm.edu/) by Chris Caldwell.
- Repunits and their prime factors (http://www.worldofnumbers.com/repunits.htm) at World!Of Numbers (http://www.worldofnumbers.com).
- Prime generalized repunits (http://www.primes.viner-steward.org/andy/titans.html) of at least 1000 decimal digits by Andy Steward
- Repunit Primes Project (http://www.gruppoeratostene.com/ric-repunit/repunit.htm) Giovanni Di Maria's repunit primes page.
- The Repunit Primes Project (http://www.repunit.org/)
- Factorizations of 11...11 (Repunit) (http://homepage2.nifty.com/m_kamada/math/11111.htm) by Makoto Kamada

Books

- S. Yates, *Repunits and repetends*. ISBN 0-9608652-0-9.
- A. Beiler, *Recreations in the theory of numbers*. ISBN 0-486-21096-0. Chapter 11, of course.
- Paulo Ribenboim, *The New Book Of Prime Number Records*. ISBN 0-387-94457-5.

Safe prime

A **safe prime** is a prime number of the form $2p + 1$, where p is also a prime. (Conversely, the prime p is a Sophie Germain prime.) The first few safe primes are

5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467, 479, 503, 563, 587, 719, 839, 863, 887, 983, 1019, 1187, 1283, 1307, 1319, 1367, 1439, 1487, 1523, 1619, 1823, 1907. (sequence A005385 [44] in OEIS)

With the exception of 7, a safe prime q is of the form $6k - 1$ or, equivalently, $q \equiv 5 \pmod 6$ — as is $p > 3$ (c.f. Sophie Germain prime, second paragraph). Similarly, with the exception of 5, a safe prime q is of the form $4k - 1$ or, equivalently, $q \equiv 3 \pmod 4$ — trivially true since $(q - 1) / 2$ must evaluate to an odd natural number. Combining both forms using lcm(6,4) we determine that a safe prime $q > 7$ also must be of the form $12k-1$ or, equivalently, $q \equiv 11 \pmod{12}$.

Applications

These primes are called "safe" because of their relationship to strong primes. A prime number q is a *strong* prime if $q + 1$ and $q - 1$ both have large prime factors. For a safe prime $q = 2p + 1$, the number $q - 1$ naturally has a large prime factor, namely p, and so safe prime q meets part of the criteria for being a strong prime. The running times of some methods of factoring a number with q as a prime factor depend partly on the size of the prime factors of $q - 1$. This is true, for instance, of the Pollard rho +1 and −1 methods. Although the most efficient known integer factorization methods do not depend on the size of the prime factors of $q-1$, this is nonetheless considered important in cryptography: for instance, the ANSI X9.31 standard mandates that *strong* primes (not *safe* primes) be used for RSA moduli.

Safe primes are also important in cryptography because of their use in discrete logarithm-based techniques like Diffie-Hellman key exchange. If $2p + 1$ is a safe prime, the multiplicative group of numbers modulo $2p + 1$ has a subgroup of large prime order. It is usually this prime-order subgroup that is desirable, and the reason for using safe primes is so that the modulus is as small as possible relative to p.

Safe primes obeying certain congruences can be used to generate pseudo-random numbers of use in Monte Carlo simulation.

Further properties

There is no special primality test for safe primes the way there is for Fermat primes and Mersenne primes. However, Pocklington's criterion can be used to prove the primality of $2p+1$ once one has proven the primality of p.

With the exception of 5, there are no Fermat primes that are also safe primes. Since Fermat primes are of the form $F = 2^n + 1$, it follows that $(F - 1)/2$ is a power of two.

With the exception of 7, there are no Mersenne primes that are also safe primes. This follows from the statement above that all safe primes except 7 are of the form $6k - 1$. Mersenne primes are of the form $2^m - 1$, but $2^m - 1 = 6k - 1$ would imply that 2^m is divisible by 6, which is impossible.

Just as every term except the last one of a Cunningham chain of the first kind is a Sophie Germain prime, so every term except the first of such a chain is a safe prime. Safe primes ending in 7, that is, of the form $10n + 7$, are the last terms in such chains when they occur, since $2(10n + 7) + 1 = 20n + 15$ is divisible by 5.

If a safe prime q is congruent to 7 mod 8, then it is a divisor of the Mersenne number with its matching Sophie Germain prime as exponent.

Records

As of March 2010, the largest known safe prime is $183027 \cdot 2^{265441} - 1$. This prime, along with the corresponding largest known Sophie Germain prime, was found by Tom Wu on March 22, 2010 using the programs sgsieve and LLR.[1]

On June 18, 2005, Antoine Joux and Reynald Lercier announced that they computed a discrete logarithm modulo a 130-digit safe prime.[2]

References

[1] http://primes.utm.edu/primes/page.php?id=92222

[2] http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0506&L=nmbrthry&T=0&P=2037

- M. Abramowitz and I. A. Stegun, eds., *Handbook of Mathematical Functions*, National Bureau of Standards, Applied Math. Series 55, Tenth Printing, (1972): 870

External links

- Safe prime (http://planetmath.org/encyclopedia/SafePrime.html) at planetmath.org

Self number

A **self number**, **Colombian number** or **Devlali number** is an integer which, in a given base, cannot be generated by any other integer added to the sum of that other integer's digits. For example, 21 is not a self number, since it can be generated by the sum of 15 and the digits comprising 15, that is, 21 = 15 + 1 + 5. No such sum will generate the integer 20, hence it is a self number. These numbers were first described in 1949 by the Indian mathematician D. R. Kaprekar.

The first few base 10 self numbers are:

> 1, 3, 5, 7, 9, 20, 31, 42, 53, 64, 75, 86, 97, 108, 110, 121, 132, 143, 154, 165, 176, 187, 198, 209, 211, 222, 233, 244, 255, 266, 277, 288, 299, 310, 312, 323, 334, 345, 356, 367, 378, 389, 400, 411, 413, 424, 435, 446, 457, 468, 479, 490, 501, 512, 514, 525 (sequence A003052 [1] in OEIS)

In general, for even bases, all odd numbers below the base number are self numbers, since any number below such an odd number would have to also be a 1-digit number which when added to its digit would result in an even number. For odd bases, all odd numbers are self numbers.

A search for self numbers can turn up self-descriptive numbers, which are similar to self numbers in being base-dependent, but quite different in definition and much fewer in frequency.

Recurrent formula

The following recurrence relation generates some base 10 self numbers:

$$C_k = 8 \cdot 10^{k-1} + C_{k-1} + 8$$

(with $C_1 = 9$)

And for binary numbers:

$$C_k = 2^j + C_{k-1} + 1$$

(where *j* stands for the number of digits) we can generalize a recurrence relation to generate self numbers in any base *b*:

$$C_k = (b-2)b^{k-1} + C_{k-1} + (b-2)$$

in which $C_1 = b - 1$ for even bases and $C_1 = b - 2$ for odd bases.

The existence of these recurrence relations shows that for any base there are infinitely many self numbers.

Self primes

A **self prime** is a self number that is prime. The first few self primes (sequence A006378 [45] in OEIS) are

3, 5, 7, 31, 53, 97, 211, 233, 277, 367, 389

In October 2006 Luke Pebody demonstrated that the largest known Mersenne prime that is at the same time a self number is $2^{24036583}-1$. This is then the largest known self prime as of 2006.

Selfness tests

Reduction tests

Luke Pebody showed (Oct 2006) that a link can be made between the self property of a large number *n* and a low-order portion of that number, adjusted for digit sums:

a) In general, *n* is self if and only if *m* = R(*n*)+SOD(R(*n*))-SOD(*n*) is self

Where:

R(*n*) is the smallest rightmost digits of *n*, greater than 9.d(*n*)

d(*n*) is the number of digits in *n*

SOD(*x*) is the sum of digits of *x*, the function $S_{10}(x)$ from above.

b) If *n* = *a*.10^*b*+*c*, *c*<10^*b*, then *n* is self if and only if both {*m1* & *m2*} are negative or self

Where:

m1 = *c* - SOD(*a*)

m2 = SOD(*a*-1)+9.*b*-(*c*+1)

c) For the simple case of *a*=1 & *c*=0 in the previous model (i.e. *n*=10^*b*), then *n* is self if and only if (9.*b*-1) is self

Effective test

Kaprekar demonstrated that:

$$n \text{ is self if } [n - DR*(n) - 9 \cdot i] + SOD([n - DR*(n) - 9 \cdot i]) \neq n \quad \forall i \in 0 \ldots d(n)$$

Where:

$$DR*(n) = \begin{cases} \frac{DR(n)}{2}, & \text{if } DR(n) \text{ is even} \\ \frac{DR(n)+9}{2}, & \text{if } DR(n) \text{ is odd} \end{cases}$$

$$DR(n) = \begin{cases} 9, & \text{if } SOD(n) \mod 9 = 0 \\ SOD(n) \mod 9, & \text{otherwise} \end{cases}$$

$$= (n-1) \mod 9 + 1$$

$SOD(n)$ is the sum of all digits in n

$d(n)$ is the number of digits in n

Excerpt from the table of bases where 2007 is self or Colombian

The following table was calculated in 2007.

Base	Certificate	Sum of digits
40	$1959 = [1, 8, 39]_{40}$	48
41	-	-
42	$1967 = [1, 4, 35]_{42}$	40
43	-	-
44	$1971 = [1, 0, 35]_{44}$	36
44	$1928 = [43, 36]_{44}$	79
45	-	-
46	$1926 = [41, 40]_{46}$	81
47	-	-
48	-	-
49	-	-
50	$1959 = [39, 9]_{50}$	48
51	-	-
52	$1947 = [37, 23]_{52}$	60
53	-	-
54	$1931 = [35, 41]_{54}$	76
55	-	-
56	$1966 = [35, 6]_{56}$	41
57	-	-
58	$1944 = [33, 30]_{58}$	63
59	-	-
60	$1918 = [31, 58]_{60}$	89

References

- Kaprekar, D. R. *The Mathematics of New Self-Numbers* Devaiali (1963): 19 - 20.
- Patel, R. B. "Some Tests for -Self Numbers" *Math. Student* **56** (1991): 206 - 210.
- B. Recaman, "Problem E2408" *Amer. Math. Monthly* **81** (1974): 407
- Weisstein, Eric W., "Self Number [2]" from MathWorld.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa003052

[2] http://mathworld.wolfram.com/SelfNumber.html

Sexy prime

In mathematics, a **sexy prime** is a prime number that differs from another prime number by six. For example, the numbers 5 and 11 are both sexy primes, because they differ by 6. If $p + 2$ or $p + 4$ is also prime, then the sexy prime is part of a prime triplet.

The term "sexy prime" stems from the Latin word for six: *sex*.

n# notation

As used in this article, n# stands for the product $2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots$ of all the primes ≤ n.

Types of groupings

Sexy prime pairs

The sexy primes (sequences A023201 [46] and A046117 [47] in OEIS) below 500 are:

(5,11), (7,13), (11,17), (13,19), (17,23), (23,29), (31,37), (37,43), (41,47), (47,53), (53,59), (61,67), (67,73), (73,79), (83,89), (97,103), (101,107), (103,109), (107,113), (131,137), (151,157), (157,163), (167,173), (173,179), (191,197), (193,199), (223,229), (227,233), (233,239), (251,257), (257,263), (263,269), (271,277), (277,283), (307,313), (311,317), (331,337), (347,353), (353,359), (367,373), (373,379), (383,389), (433,439), (443,449), (457,463), (461,467).

As of May 2009 the largest known sexy prime was found by Ken Davis and has 11593 digits. The primes are (p, p+6) for

$p = (117924851 \times 587502 \times 9001\# \times (587502 \times 9001\# + 1) + 210) \times (587502 \times 9001\# - 1)/35 + 5$.[1]

9001# = 2×3×5×...×9001 is a primorial, i.e. the product of primes ≤ 9001.

Sexy prime triplets

Sexy primes can be extended to larger constellations. Triplets of primes (p, $p + 6$, $p + 12$) such that $p + 18$ is composite are called **sexy prime triplets**. Those below 1000 are (A046118 [2], A046119 [3], A046120 [4]):

(5,11,17), (7,13,19), (17,23,29), (31,37,43), (47,53,59), (67,73,79), (97,103,109), (101,107,113), (151,157,163), (167,173,179), (227,233,239), (257,263,269), (271,277,283), (347,353,359), (367,373,379), (557,563,569), (587,593,599), (607,613,619), (647,653,659), (727,733,739), (941,947,953), (971,977,983).

As of April 2006 the largest known sexy prime triplet, found by Ken Davis had 5132 digits:

$p = (84055657369 \cdot 205881 \cdot 4001\# \cdot (205881 \cdot 4001\# + 1) + 210) \cdot (205881 \cdot 4001\# - 1) / 35 + 1$.[5]

Sexy prime quadruplets

Sexy prime quadruplets (p, $p + 6$, $p + 12$, $p + 18$) can only begin with primes ending in a 1 in their decimal representation (except for the quadruplet with $p = 5$). The sexy prime quadruplets below 1000 are (A023271 [6], A046122 [7], A046123 [8], A046124 [9]):

(5,11,17,23), (11,17,23,29), (41,47,53,59), (61,67,73,79), (251,257,263,269), (601,607,613,619), (641,647,653,659).

In November 2005 the largest known sexy prime quadruplet, found by Jens Kruse Andersen had 1002 digits:

$p = 411784973 \cdot 2347\# + 3301$.[10]

In September 2010 Ken Davis announced a 1004-digit quadruplet with $p = 2^{3333} + 1582534968299$.[11]

Sexy prime quintuplets

In an arithmetic progression of five terms with common difference 6, because 6>5 and the two numbers are relatively prime, one of the terms must be divisible by 5. Thus, the only sexy prime quintuplet is (5,11,17,23,29) with no longer sequence of sexy primes possible.

See also

- Twin prime (two primes that differ by 2)
- Cousin prime (two primes that differ by 4)
- Prime k-tuple

References

[1] Ken Davis, "11593 digit sexy prime pair" (http://tech.groups.yahoo.com/group/primenumbers/message/20207). Retrieved 2009-05-06.
[2] http://en.wikipedia.org/wiki/Oeis%3Aa046118
[3] http://en.wikipedia.org/wiki/Oeis%3Aa046119
[4] http://en.wikipedia.org/wiki/Oeis%3Aa046120
[5] Jens K. Andersen, "The largest known CPAP-3" (http://users.cybercity.dk/~dsl522332/math/cpap.htm#k3). Retrieved 2009-01-27.
[6] http://en.wikipedia.org/wiki/Oeis%3Aa023271
[7] http://en.wikipedia.org/wiki/Oeis%3Aa046122
[8] http://en.wikipedia.org/wiki/Oeis%3Aa046123
[9] http://en.wikipedia.org/wiki/Oeis%3Aa046124
[10] Jens K. Andersen, "Gigantic sexy and cousin primes" (http://groups.yahoo.com/group/primeform/message/6637). Retrieved 2009-01-27.
[11] Ken Davis, "1004 sexy prime quadruplet" (http://tech.groups.yahoo.com/group/primenumbers/message/21783). Retrieved 2010-09-02.

- Weisstein, Eric W., " Sexy Primes (http://mathworld.wolfram.com/SexyPrimes.html)" from MathWorld. Retrieved on 2007-02-28 (requires composite p+18 in a sexy prime triplet, but no other similar restrictions)

Smarandache–Wellin number

In mathematics, a **Smarandache–Wellin number** is an integer that in a given base is the concatenation of the first *n* prime numbers written in that base. Smarandache–Wellin numbers are named after Florentin Smarandache and Paul R. Wellin.

The first decimal Smarandache–Wellin numbers are:

2, 23, 235, 2357, 235711, ... (sequence A019518 [1] in OEIS).

Smarandache–Wellin primes

A Smarandache–Wellin number that is also prime is called a **Smarandache–Wellin prime**. The first three are 2, 23 and 2357 (A069151 [48]). The fourth has 355 digits and ends with the digits 719.[2]

The primes at the end of the concatenation in the Smarandache–Wellin primes are

2, 3, 7, 719, 1033, 2297, 3037, 11927?, ... (A046284 [3]).

The indices of the Smarandache–Wellin primes in the sequence of Smarandache–Wellin numbers are:

1, 2, 4, 128, 174, 342, 435, 1429?, ... (A046035 [4]).

The 1429th Smarandache–Wellin number is a probable prime with 5719 digits ending in 11927, discovered by Eric W. Weisstein in 1998.[5] If it is proven prime, it will be the eighth Smarandache–Wellin prime. In July 2006 Weisstein's search showed the index of the next Smarandache–Wellin prime (if one exists) is greater than 18272.[6]

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa019518
[2] Pomerance, Carl B.; Crandall, Richard E. (2001). *Prime Numbers: a computational perspective*. Springer. pp. 78 Ex 1.86. ISBN 0387252827.
[3] http://en.wikipedia.org/wiki/Oeis%3Aa046284
[4] http://en.wikipedia.org/wiki/Oeis%3Aa046035
[5] Rivera, Carlos, Primes by Listing (http://www.primepuzzles.net/puzzles/puzz_008.htm)
[6] Weisstein, Eric W., " Integer Sequence Primes (http://mathworld.wolfram.com/IntegerSequencePrimes.html)" from MathWorld.

- Weisstein, Eric W., " Smarandache–Wellin Number (http://mathworld.wolfram.com/Smarandache-WellinNumber.html)" from MathWorld.
- Smarandache-Wellin number (http://planetmath.org/?op=getobj&from=objects&id=7921) on PlanetMath
- List of first 54 Smarandache–Wellin numbers with factorisations (http://www.gallup.unm.edu/~smarandache/SmConPri.txt)
- Smarandache–Wellin primes at *The Prime Glossary* (http://primes.utm.edu/glossary/page.php?sort=SmarandacheWellin)
- Smith, S. "A Set of Conjectures on Smarandache Sequences." Bull. Pure Appl. Sci. 15E, 101–107, 1996.

Solinas prime

In mathematics, a **Solinas prime,** named after Jerome Solinas, is a prime number of the form $2^a \pm 2^b \pm 1$, where $0 < b < a$.

For example, the first five pairs of twin primes are also Solinas primes.

The first few Solinas primes are

3, 5, 7, … (sequence A165255 [49] in OEIS).

External links

- Jerome A. Solinas, "Generalized Mersenne Numbers [1]" (pdf)

References

[1] http://www.cacr.math.uwaterloo.ca/techreports/1999/corr99-39.pdf

Sophie Germain prime

In number theory, a prime number p is a **Sophie Germain prime** if $2p + 1$ is also prime. For example, 23 is a Sophie Germain prime because it is a prime and $2 \times 23 + 1 = 47$, also prime. These numbers are named after French mathematician Marie-Sophie Germain.

A Sophie Germain prime $p > 3$ is of the form $6k-1$ or, equivalently, $p \equiv 5 \pmod 6$ — as is its matching safe prime $2p+1$. We note that the other form for a prime $p > 3$ is $6k + 1$ or, equivalently, $p \equiv 1 \pmod 6$, and that $3|(2p + 1)$ — thus excluding such p from the Sophie Germain prime domain. This is trivially proven using modular arithmetic.

It is conjectured that there are infinitely many Sophie Germain primes, but like the twin prime conjecture, this has not been proven.

The first few Sophie Germain primes are:

2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, ….. (sequence A005384 [50] in OEIS).

The largest known Sophie Germain prime as of March 2010 is $183027 \times 2^{265440}-1$. It has 79911 decimal digits and was found in March 2010 by Tom Wu using the program LLR.[1] Before that the two largest were $648621027630345 \times 2^{253824}-1$ and $620366307356565 \times 2^{253824}-1$. They both have 76424 decimal digits and were found in November 2009 by Zoltán Járai, Gabor Farkas, Timea Csajbok, János Kasza and Antal Járai.[2] [3] The previous record was set 6 weeks earlier, $607095 \times 2^{176311}-1$ with 53081 digits, found by Tom Wu.[4] Before that the record was $48047305725 \times 2^{172403}-1$ with 51910 digits, found by David Underbakke in January 2007 using the programs TwinGen and LLR.[5] And before that, the record was held by the same team as the November 2009 records, $137211941292195 \times 2^{171960}-1$ with 51780 digits, found in May 2006.[6] As of March 2010 the above are still the six largest known Sophie Germain primes.

A heuristic estimate (due to G. H. Hardy and J. E. Littlewood) for the number of Sophie Germain primes less than n is $2C_2\, n / (\ln n)^2$ where C_2 is the twin prime constant, approximately 0.660161. For $n = 10^4$, this estimate predicts 156 Sophie Germain primes, which has a 20% error compared to the exact value of 190. For $n = 10^7$, the estimate predicts 50822, which is still 10% off from the exact value of 56032.

A sequence $\{p, 2p + 1, 2(2p + 1) + 1, ...\}$ of 1 or more Sophie Germain primes, ending with a prime which does not have to be a Sophie Germain, is called a Cunningham chain of the first kind. Every term of such a sequence except the first and last is both a Sophie Germain prime and a safe prime.

If a Sophie Germain prime p is congruent to 3 (mod 4), then its matching safe prime $2p + 1$ will be a divisor of the Mersenne number $2^p - 1$.

Sophie Germain primes were mentioned in the stage play *Proof* and the subsequent film.

Application in (pseudo-)random number generation

Sophie Germain primes have a practical application in the generation of pseudo-random numbers. The decimal expansion of $1/q$ will produce a stream of $q - 1$ pseudo-random digits, if q is the safe prime of a Sophie Germain prime p, with p congruent to 3, 9, or 11 (mod 20). Thus "suitable" prime numbers q are 7, 23, 47, 59, 167, 179, etc. (corresponding to $p =$ 3, 11, 23, 29, 83, 89, etc.). The result is a stream of length $q - 1$ digits (including leading zeros); for more see OEIS sequence A000355 [7]. So, for example, using $q = 23$ generates the pseudo-random digits 0, 4, 3, 4, 7, 8, 2, 6, 0, 8, 6, 9, 5, 6, 5, 2, 1, 7, 3, 9, 1, 3. Note that these digits are not appropriate for cryptographic purposes, as the value of each can be derived from its predecessor in the digit-stream.

See also

- PrimeGrid – search for Sophie Germain primes
- Twin Prime Search – includes search for Sophie Germain primes

References

[1] The Prime Database: 183027*2^265440-1 (http://primes.utm.edu/primes/page.php?id=92222). From The Prime Pages.
[2] The Prime Database: 648621027630345*2^253824-1 (http://primes.utm.edu/primes/page.php?id=90907).
[3] The Prime Database: 620366307356565*2^253824-1 (http://primes.utm.edu/primes/page.php?id=90711)
[4] The Prime Database: 607095*2^176311-1 (http://primes.utm.edu/primes/page.php?id=89999).
[5] The Prime Database: 48047305725*2^172403-1 (http://primes.utm.edu/primes/page.php?id=79261).
[6] The Prime Database: 137211941292195*2^171960-1 (http://primes.utm.edu/primes/page.php?id=77705).
[7] http://en.wikipedia.org/wiki/Oeis%3Aa000355

Further reading

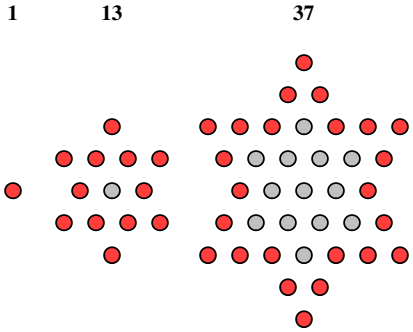
- Matthews, R. A. J. (1992), "Maximally Periodic Reciprocals", *Bulletin of the Institute of Mathematics and its Applications* **28**: 147–148

External links

- The Top Twenty Sophie Germain Primes (http://primes.utm.edu/top20/page.php?id=2) — from the Prime Pages.

Star number

A **star number** is a centered figurate number that represents a centered hexagram, such as the one that Chinese checkers is played on.



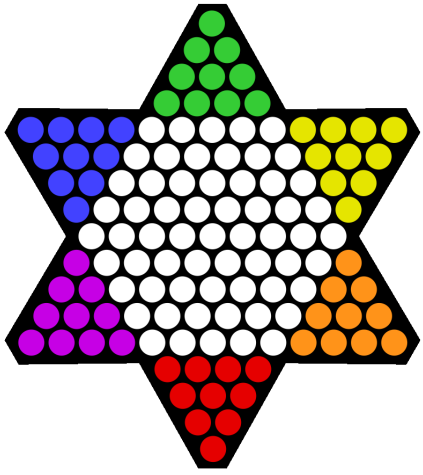
The *n*th star number is given by the formula 6*n*(*n* - 1) + 1. The first 43 star numbers are

1, 13, 37, 73, 121, 181, 253, 337, 433, 541, 661, 793, 937, 1093, 1261, 1441, 1633, 1837, 2053, 2281, 2521, 2773, 3037, 3313, 3601, 3901, 4213, 4537, 4873, 5221, 5581, 5953, 6337, 6733, 7141, 7561, 7993, 8437, 8893, 9361, 9841, 10333, 10837 (sequence A003154 [1] in OEIS).

Geometrically, the *n*th star number is made up of a central point and 12 copies of the (*n*-1)th triangular number — making it numerically equal to the *n*th centered dodecagonal number, but differently arranged.

The digital root of a star number is always 1 or 4. The last two digits of a star number in base 10 are always 01, 13, 21, 33, 37, 41, 53, 61, 73, 81, or 93.

Not many star numbers are also triangular numbers. 1 and 253 are the only two such numbers in the list given above, corresponding to n=1 and n=7. There are infinitely many with the next two correspond to n=91 and n=1261 (sequence A003154 [1] in OEIS). These are the values n=(x+2)/4 with x an even solution of the Diophantine equation $x^2 = 3y^2 + 1$.



Chinese checkers board has 121 holes.

Not many star numbers are also square. 1 and 121 are the only two such numbers in the list given above, corresponding to n=1 and n=5. There are infinitely many with the next two being n=45 and n=441 (sequence A054318 [2] in OEIS). These n values are n=(y+1)/2 from the Diophantine equation $2x^2 + 1 = 3y^2$.

The term "star number" or "stellate number" is occasionally used to refer to octagonal numbers.

A **star prime** is a star number that is prime. The first few star primes (sequence A083577 [51] in OEIS) are

13, 37, 73, 181, 337, 433, 541, 661, 937.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa003154
[2] http://en.wikipedia.org/wiki/Oeis%3Aa054318

Stern prime

A **Stern prime**, named for Moritz Abraham Stern, is a prime number that is not the sum of a smaller prime and twice the square of a nonzero integer. Or, to put it algebraically, if for a prime q there is no smaller prime p and nonzero integer b such that $q = p + 2b^2$, then q is a Stern prime. The known Stern primes are

2, 3, 17, 137, 227, 977, 1187, 1493 (sequence A042978 [52] in OEIS).

So, for example, if we try subtracting from 137 the first few squares doubled in order, we get {135, 129, 119, 105, 87, 65, 39, 9}, none of which are prime. That means that 137 is a Stern prime. On the other hand, 139 is not a Stern prime, since we can express it as $137 + 2(1^2)$, or $131 + 2(2^2)$, etc.

In fact, many primes have more than one representation of this sort. Given a twin prime, the larger prime of the pair has, if nothing else, a Goldbach representation of $p + 2(1^2)$. And if that prime is the largest of a prime quadruplet, $p + 8$, then $p + 2(2^2)$ is also available. Sloane's A007697 [1] lists odd numbers with at least n Goldbach representations. Leonhard Euler observed that as the numbers get larger, they get more representations of the form $p + 2b^2$, suggesting that there might be a largest number with zero such representations.

Therefore, the above list of Stern primes might be not only finite, but also complete. According to Jud McCranie, these are the only Stern primes from among the first 100000 primes. All the known Stern primes have more efficient Waring representations than their Goldbach representations would suggest.

Christian Goldbach conjectured in a letter to Leonhard Euler that every odd integer is of the form $p + 2b^2$ with b allowed to be any integer, including zero. Laurent Hodges believes that Stern became interested in the problem after reading a book of Goldbach's correspondence. Because in Stern's time, 1 was considered a prime, 3 was not a Stern prime because it could be represented as $1 + 2(1^2)$. The rest of the list remains the same.

References

- Laurent Hodges, A lesser-known Goldbach conjecture [2]

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa007697
[2] http://www.lacim.uqam.ca/~plouffe/OEIS/archive_in_pdf/mm-1.pdf

Strobogrammatic prime

A **strobogrammatic prime** is a prime number that, given a base and given a set of glyphs, appears the same whether viewed normally or upside down. In base 10, given a set of glyphs where 0, 1 and 8 are symmetrical around the horizontal axis, and 6 and 9 are the same as each other upside down, (such as the digit characters in ASCII using the font Stylus BT, or on the seven-segment display of a calculator), the first few strobogrammatic primes are:

11, 101, 181, 619, 16091, 18181 (sequence A007597 [1] in OEIS)

Although amateur aficionados of mathematics are quite interested in this concept, professional mathematicians generally are not. Like the concept of repunit primes and palindromic primes, the concept of strobogrammatic primes is base-dependent. But the concept of strobogrammatic primes is not neatly expressible algebraically, the way that the concept of repunit primes is, or even the concept of palindromic primes.

There are sets of glyphs for writing numbers in base 10, such as the Devanagari and Gurmukhi of India in which the primes listed above are not strobogrammatic at all.

In binary, given a glyph for 1 consisting of a single line without hooks or serifs, all Mersenne primes are strobogrammatic. Palindromic primes in binary are also strobogrammatic.

Dihedral primes that don't use 2 or 5 are also strobogrammatic primes.

See also

- Strobogrammatic number

External links

- The Prime Glossary: Strobogrammatic [2]

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa007597
[2] http://primes.utm.edu/glossary/page.php?sort=Strobogrammatic

Strong prime

In mathematics, a **strong prime** is a prime number with certain special properties. The definitions of strong primes are different in cryptography and number theory.

Definition in cryptography

In cryptography, a prime number p is *strong* if the following conditions are satisfied[1] .

1. p is large.
2. $p-1$ has large prime factors. That is, $p = a_1 q_1 + 1$ for some integer a_1 and large prime q_1 .
3. $q_1 - 1$ has large prime factors. That is, $q_1 = a_2 q_2 + 1$ for some integer a_2 and large prime q_2 .
4. $p+1$ has large prime factors. That is, $p = a_3 q_3 - 1$ for some integer a_3 and large prime q_3 .

Sometimes a prime that satisfies a subset of the above conditions is also called *strong*. In some cases, some additional conditions may be included. For example, $a_1 = 2$, or $a_2 = 2$, etc.

Definition in number theory

In number theory, a **strong prime** is a prime number that is greater than the arithmetic mean of the nearest prime above and below (in other words, it's closer to the following than to the preceding prime). Or to put it algebraically, given a prime number p_n, where *n* is its index in the ordered set of prime numbers, $p_n > \frac{p_{n-1} + p_{n+1}}{2}$. The first few strong primes are

> 11, 17, 29, 37, 41, 59, 67, 71, 79, 97, 101, 107, 127, 137, 149, 163, 179, 191, 197, 223, 227, 239, 251, 269, 277, 281, 307, 311, 331, 347, 367, 379, 397, 419, 431, 439, 457, 461, 479, 487, 499 (sequence A051634 [2] in OEIS).

For example, 17 is the seventh prime. The sixth and eighth primes, 13 and 19, add up to 32, and half that is 16. That is less than 17, thus 17 is a strong prime.

In a twin prime pair (p, p + 2) with $p > 5$, p is always a strong prime, since 3 must divide $p - 2$ which cannot be prime.

It is possible for a prime to be a strong prime both in the cryptographic sense and the number theoretic sense. For the sake of illustration, 439351292910452432574786963588089477522344331 is a strong prime in the number theoretic sense because the arithmetic mean of its two neighboring primes is 62 less. Without the aid of a computer, this number would be a strong prime in the cryptographic sense because 439351292910452432574786963588089477522344330 has the large prime factor 1747822896920092227343 (and in turn the number one less than that has the large prime factor 1683837087591611009), 439351292910452432574786963588089477522344332 has the large prime factor 864608136454559457049 (and in turn the number one less than that has the large prime factor 105646155480762397). Even using algorithms more advanced than trial by division, these numbers would be difficult to factor by hand. For a modern computer algebra system, these numbers can be factored almost instantaneously. A cryptographically strong prime has to be much larger than this example.

Application of strong primes in cryptography

Factoring-based cryptosystems

Some people suggest that in the key generation process in RSA cryptosystems, the modulus n should be chosen as the product of two strong primes. This makes the factorization of $n = pq$ using Pollard's $p - 1$ algorithm computationally infeasible. For this reason, strong primes are required by the ANSI X9.31 standard for use in generating RSA keys for digital signatures. However, strong primes do not protect against modulus factorisation using newer algorithms such as Lenstra elliptic curve factorization and Number Field Sieve algorithm. Given the additional cost of generating strong primes RSA Security do not currently recommend their use in key generation. Similar (and more technical) argument is also given by Rivest and Silverman [1] .

Discrete-logarithm-based cryptosystems

It is shown by Stephen Pohlig and Martin Hellman in 1978 that if all the factors of *p-1* are less than $log^c p$, then the problem of solving discrete logarithm modulo *p* is in P. Therefore, for cryptosystems based on discrete logarithm, such as DSA, it is required that *p-1* has at least one large prime factor.

References

[1] Ron Rivest and Robert Silverman, *Are 'Strong' Primes Needed for RSA?*, Cryptology ePrint Archive: Report 2001/007. http://eprint.iacr.org/2001/007

[2] http://en.wikipedia.org/wiki/Oeis%3Aa051634

External links

- Guide to Cryptography and Standards (http://www.isg.rhul.ac.uk/ugcs/Companion_v1.21.pdf)
- RSA Lab's explanation on strong vs weak primes (http://www.rsa.com/rsalabs/node.asp?id=2217)

Super-prime

Super-prime numbers are the subsequence of prime numbers that occupy prime-numbered positions within the sequence of all prime numbers. The subsequence begins

3, 5, 11, 17, 31, 41, 59, 67, 83, 109, 127, 157, … (sequence A006450 [53] in OEIS).

That is, if $p(i)$ denotes the ith prime number, the numbers in this sequence are those of the form $p(p(i))$. Dressler & Parker (1975) used a computer-aided proof (based on calculations involving the subset sum problem) to show that every integer greater than 96 may be represented as a sum of distinct super-prime numbers. Their proof relies on a result resembling Bertrand's postulate, stating that (after the larger gap between super-primes 5 and 11) each super-prime number is less than twice its predecessor in the sequence.

Broughan and Barnett[1] show that there are

$$\frac{x}{(\log x)^2} + O\left(\frac{x \log\log x}{(\log x)^3}\right)$$

super-primes up to x.

One can also define "higher-order" primeness much the same way, and obtain analogous sequences of primes. Fernandez (1999)

A variation on this theme is the sequence of prime numbers with palindromic indices, beginning with

3, 5, 11, 17, 31, 547, 739, 877, 1087, 1153, 2081, 2381, … (sequence A124173 [2] in OEIS).

References

[1] Kevin A. Broughan and A. Ross Barnett, On the Subsequence of Primes Having Prime Subscripts (http://www.cs.uwaterloo.ca/journals/JIS/VOL12/Broughan/broughan16.html), *Journal of Integer Sequences* **12** (2009), article 09.2.3.

[2] http://en.wikipedia.org/wiki/Oeis%3Aa124173

- Dressler, Robert E.; Parker, S. Thomas (1975), "Primes with a prime subscript", *Journal of the ACM* **22** (3): 380–381, doi:10.1145/321892.321900, MR0376599.
- Fernandez, Neil (1999), *An order of primeness, F(p)* (http://borve.org/primeness/FOP.html).

External links

- A Russian programming contest problem related to the work of Dressler and Parker (http://acm.sgu.ru/problem.php?contest=0&problem=116)

Supersingular prime (moonshine theory)

In the mathematical branch of moonshine theory, a **supersingular prime** is a certain type of prime number. Namely, a **supersingular prime** is a prime divisor of the order of the Monster group *M*, the largest of the sporadic simple groups. There are precisely 15 supersingular primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, and 71.

This definition is related to the notion of supersingular elliptic curves as follows. For a prime number *p*, the following are equivalent:

1. The modular curve $X_0^+(p) = X_0(p) / w_p$, where w_p is the Fricke involution of $X_0(p)$, has genus zero.
2. Every supersingular elliptic curve in characteristic *p* can be defined over the prime subfield $\mathbf{F}_p$.
3. The order of the Monster group is divisible by *p*.

The equivalence is due to Andrew Ogg. More precisely, in 1975 Ogg showed that the primes satisfying the first condition are exactly the 15 primes 2,...,71 listed above and shortly thereafter learned of the (then conjectural) existence of a sporadic simple group having exactly these primes as prime divisors. This strange coincidence was the beginning of the theory of Monstrous Moonshine.

References

- Weisstein, Eric W., "Supersingular Prime [1]" from MathWorld.
- Ogg, A. P. "Modular Functions." In The Santa Cruz Conference on Finite Groups. Held at the University of California, Santa Cruz, Calif., June 25-July 20, 1979 (Ed. B. Cooperstein and G. Mason). Providence, RI: Amer. Math. Soc., pp. 521-532, 1980.

References

[1] http://mathworld.wolfram.com/SupersingularPrime.html

Thabit number

In number theory, a **Thabit number**, **Thâbit ibn Kurrah number**, or **321 number** is an integer of the form $3 \cdot 2^n - 1$ for a non-negative integer n. The first few Thabit numbers are:

2, 5, 11, 23, 47, 95, 191, 383, 767, 1535, 3071, 6143, 12287, 24575, 49151, 98303, 196607, 393215, 786431, 1572863, ... (sequence A055010 [1] in OEIS)

The binary representation of the Thabit number $3 \cdot 2^n - 1$ is $n+2$ digits long, consisting of "10" followed by n 1s.

The first few Thabit numbers that are prime (also known as **321 primes**):

2, 5, 11, 23, 47, 191, 383, 6143, 786431, 51539607551, 824633720831, ... (sequence A007505 [55] in OEIS)

As of April 2008, the known n values which give prime Thabit numbers are:[2] [3]

0, 1, 2, 3, 4, 6, 7, 11, 18, 34, 38, 43, 55, 64, 76, 94, 103, 143, 206, 216, 306, 324, 391, 458, 470, 827, 1274, 3276, 4204, 5134, 7559, 12676, 14898, 18123, 18819, 25690, 26459, 41628, 51387, 71783, 80330, 85687, 88171, 97063, 123630, 155930, 164987, 234760, 414840, 584995, 702038, 727699, 992700, 1201046, 1232255, 2312734, 3136255, 4235414 (sequence A002235 [4] in OEIS)

The primes for $n \geq 234760$ were found by the distributed computing project **321 search**.[5] The largest of these, $3 \cdot 2^{4235414} - 1$, has 1274988 digits and was found by Dylan Bennett in April 2008. The former record was $3 \cdot 2^{3136255} - 1$ with 944108 digits, found by Paul Underwood in March 2007.

Amicable numbers

When both n and n-1 yield prime Thabit numbers, and $9 \cdot 2^{2n-1} - 1$ is also prime, a pair of amicable numbers can be calculated as follows:

$$2^n(3 \cdot 2^{n-1} - 1)(3 \cdot 2^n - 1) \text{ and } 2^n(9 \cdot 2^{2n-1} - 1).$$

So, for example, n=2 gives the Thabit number 11, and n=1 gives the Thabit number 5, and our third term is 71. Then, 2^2=4, multiplied by 5 and 11 results in 220, whose divisors add up to 284, and 4 times 71 is 284, whose divisors add up to 220.

The only known n satisfying these conditions are 2, 4 and 7, corresponding to the Thabit numbers 11, 47 and 383.

The 9th Century astronomer Thābit ibn Qurra is credited as the first to study these numbers and their relation to amicable numbers.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa055010
[2] (http://www.mersenneforum.org/321search/How many digits these primes have.html)
[3] (http://primes.utm.edu/primes/page.php?id=84769)
[4] http://en.wikipedia.org/wiki/Oeis%3Aa002235
[5] (http://www.mersenneforum.org/321search/The status of the search.html)

- Weisstein, Eric W., " Thâbit ibn Kurrah Number (http://mathworld.wolfram.com/ThabitibnKurrahNumber.html)" from MathWorld.

Truncatable prime

In number theory, a **left-truncatable prime** is a prime number which, in a given base, contains no 0, and if the leading ("left") digit is successively removed, then all resulting numbers are prime. For example 9137, since 9137, 137, 37 and 7 are all prime. Decimal representation is often assumed and always used in this article.

A **right-truncatable prime** is a prime which remains prime when the last ("right") digit is successively removed. For example 7393, since 7393, 739, 73, 7 are all prime.

There are exactly 4260 decimal left-truncatable primes:

> 2, 3, 5, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 113, 137, 167, 173, 197, 223, 283, 313, 317, 337, 347, 353, 367, 373, 383, 397, 443, 467, 523, 547, 613, 617, 643, 647, 653, 673, 683, 743, 773, 797, 823, 853, 883, 937, 947, 953, 967, 983, 997, 1223, 1283, 1367 ... (sequence A024785 [16] in OEIS)

The largest is the 24-digit 357686312646216567629137.

There are 83 right-truncatable primes. The complete list:

> 2, 3, 5, 7, 23, 29, 31, 37, 53, 59, 71, 73, 79, 233, 239, 293, 311, 313, 317, 373, 379, 593, 599, 719, 733, 739, 797, 2333, 2339, 2393, 2399, 2939, 3119, 3137, 3733, 3739, 3793, 3797, 5939, 7193, 7331, 7333, 7393, 23333, 23339, 23399, 23993, 29399, 31193, 31379, 37337, 37339, 37397, 59393, 59399, 71933, 73331, 73939, 233993, 239933, 293999, 373379, 373393, 593933, 593993, 719333, 739391, 739393, 739397, 739399, 2339933, 2399333, 2939999, 3733799, 5939333, 7393913, 7393931, 7393933, 23399339, 29399999, 37337999, 59393339, 73939133 (sequence A024770 [43] in OEIS)

The largest is the 8-digit 73939133. All primes above 5 end with digit 1, 3, 7 or 9, so a right-truncatable prime can only contain those digits after the leading digit.

There are 15 primes which are both left-truncatable and right-truncatable. They have been called **two-sided primes**. The complete list:

> 2, 3, 5, 7, 23, 37, 53, 73, 313, 317, 373, 797, 3137, 3797, 739397 (A020994 [61])

While the primality of a number does not depend on the numeral system used, truncatable primes are defined only in relation with a given base. A variation involves removing 2 or more decimal digits at a time. This is mathematically equivalent to using base 100 or a larger power of 10, with the restriction that base 10^n digits must be at least 10^{n-1}, in order to match a decimal n-digit number with no leading 0.

References

- Weisstein, Eric W., "Truncatable Prime [1]" from MathWorld.
- Caldwell, Chris, *left-truncatable prime* [2] and *right-truncatable primes* [3], at the Prime Pages glossary.
- Rivera, Carlos, Problems & Puzzles: Puzzle 2.- Prime strings [4]

References

[1] http://mathworld.wolfram.com/TruncatablePrime.html
[2] http://primes.utm.edu/glossary/page.php?sort=LeftTruncatablePrime
[3] http://primes.utm.edu/glossary/page.php?sort=RightTruncatablePrime
[4] http://www.primepuzzles.net/puzzles/puzz_002.htm

Twin prime

A **twin prime** is a prime number that differs from another prime number by two. Except for the pair (2, 3), this is the smallest possible difference between two primes. Some examples of twin prime pairs are (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), ... (821, 823), etc. Sometimes the term *twin prime* is used for a pair of twin primes; an alternative name for this is **prime twin**.

History

The question of whether there exist infinitely many twin primes has been one of the great open questions in number theory for many years. This is the content of the **twin prime conjecture**, which states *There are infinitely many primes p such that p + 2 is also prime.* In 1849 de Polignac made the more general conjecture that for every natural number k, there are infinitely many prime pairs p and p' such that $p' - p = 2k$. The case $k = 1$ is the twin prime conjecture.

A stronger form of the twin prime conjecture, the Hardy–Littlewood conjecture, postulates a distribution law for twin primes akin to the prime number theorem.

Brun's theorem

In 1915, Viggo Brun showed that the sum of reciprocals of the twin primes was convergent. This famous result, called Brun's theorem, was the first use of the Brun sieve and helped initiate the development of modern sieve theory. The modern version of Brun's argument can be used to show that the number of twin primes less than N does not exceed

$$\frac{CN}{\log^2 N}$$

for some absolute constant $C > 0$.

In 1940, Paul Erdős showed that there is a constant $c < 1$ and infinitely many primes p such that $(p' - p) < (c \ln p)$ where p' denotes the next prime after p. This result was successively improved; in 1986 Helmut Maier showed that a constant $c < 0.25$ can be used. In 2004 Daniel Goldston and Cem Yıldırım showed that the constant could be improved further to $c = 0.085786\ldots$ In 2005, Goldston, János Pintz and Yıldırım established that c can be chosen to be arbitrarily small[1] [2]

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

In fact, by assuming the Elliott–Halberstam conjecture or a slightly weaker version, they were able to show that there are infinitely many n such that at least two of n, $n + 2$, $n + 6$, $n + 8$, $n + 12$, $n + 18$, or $n + 20$ are prime. Under a stronger hypothesis they showed that at least two of n, $n + 2$, $n + 4$, and $n + 6$ are prime.

Every twin prime pair except (3, 5) is of the form $(6n - 1, 6n + 1)$ for some natural number n, and with the exception of n = 1, n must end in 0, 2, 3, 5, 7, or 8.

It has been proved that the pair $(m, m+2)$ is a twin prime if and only if

$$4((m-1)! + 1) \equiv -m \pmod{m(m+2)}.$$

If $m - 4$ or $m + 6$ is also prime then the 3 primes are called a prime triplet.

Largest known twin prime

On January 15, 2007 two distributed computing projects, Twin Prime Search and PrimeGrid found the largest known twin primes, $2003663613 \cdot 2^{195000} \pm 1$. The numbers have 58711 decimal digits. Their discoverer was Eric Vautier of France.

On August 6, 2009 those same two projects announced that a new record twin prime had been found.[3] It is $65516468355 \cdot 2^{333333} \pm 1$.[4] The numbers have 100355 decimal digits.

An empirical analysis of all prime pairs up to $4.35 \cdot 10^{15}$ shows that if the number of such pairs less than x is $f(x) \cdot x/(\log x)^2$ then f(x) is about 1.7 for small x and decreases towards about 1.3 as x tends to infinity.

There are 808,675,888,577,436 twin prime pairs below 10^{18}.[5]

The limiting value of f(x) is conjectured to equal twice the twin prime constant (not to be confused with Brun's constant)

$$2 \prod_{\substack{p \text{ prime} \\ p \geq 3}} \left(1 - \frac{1}{(p-1)^2}\right) = 1.3203236\ldots;$$

(sequence A114907 [6] in OEIS) this conjecture would imply the twin prime conjecture, but remains unresolved.

The twin prime conjecture would give a better approximation, as with the prime counting function, by

$$\pi_2(x) \approx 2C_2 \operatorname{li}_2(x) = 2C_2 \int_2^x \frac{dt}{(\log_e t)^2}.$$

The first 35 twin prime pairs

There are 35 twin prime pairs below 1000, given in the following list:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), (227, 229), (239, 241), (269, 271), (281, 283), (311, 313), (347, 349), (419, 421), (431, 433), (461, 463), (521, 523), (569, 571), (599, 601), (617, 619), (641, 643), (659, 661), (809, 811), (821, 823), (827, 829), (857, 859), (881, 883).

Since every third odd number is divisible by 3, no three successive odd numbers can be prime unless one of them is 3, thus 5 is the only prime which is part of two pairs. Also, along the same lines, other than the first pair, the number centered between the twin primes must always be divisible by 6. The lower member of a pair is by definition a Chen prime.

First Hardy–Littlewood conjecture

The **Hardy–Littlewood conjecture** (after G. H. Hardy and John Littlewood) is a generalization of the twin prime conjecture. It is concerned with the distribution of prime constellations, including twin primes, in analogy to the prime number theorem. Let $\pi_2(x)$ denote the number of primes $p \leq x$ such that $p + 2$ is also prime. Define the **twin prime constant** C_2 as[7]

$$C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \approx 0.660161815846869573927812110014\ldots$$

(sequence A005597 [8] in OEIS) (here the product extends over all prime numbers $p \geq 3$). Then the conjecture is that

$$\pi_2(n) \sim 2C_2 \frac{n}{(\ln n)^2} \sim 2C_2 \int_2^n \frac{dt}{(\ln t)^2}$$

in the sense that the quotient of the two expressions tends to 1 as n approaches infinity. (The second ~ is not part of the conjecture and is proved by integration by parts.)

This conjecture can be justified (but not proven) by assuming that 1 / ln t describes the density function of the prime distribution, an assumption suggested by the prime number theorem.

Polignac's conjecture

Polignac's conjecture from 1849 states that for every even natural number k, there are infinitely many prime pairs p and p' such that $p - p' = k$. The case $k = 2$ is the twin prime conjecture. The case $k = 4$ corresponds to cousin primes and the case $k = 6$ to sexy primes. The conjecture has not been proved or disproved for any value of k.

References

[1] "Small gaps between primes exist" (http://www.arxiv.org/abs/math.NT/0505300). 2007. . Retrieved 2007-06-20.
[2] "Small gaps between primes or almost primes" (http://www.arxiv.org/abs/math.NT/0506067). 2007. . Retrieved 2007-06-20.
[3] "News Archive" (http://www.primegrid.com/all_news.php#188). *PrimeGrid*. 6 August 2009. . Retrieved 2009-08-07.
[4] "The Prime Database: 65516468355*2^333333-1" (http://primes.utm.edu/primes/page.php?id=89650). *Prime Pages*. 13 August 2009. . Retrieved 2009-08-14.
[5] Tomás Oliveira e Silva (7 April 2008). "Tables of values of pi(x) and of pi2(x)" (http://www.ieeta.pt/~tos/primes.html). Aveiro University. . Retrieved 7 January 2011.
[6] http://en.wikipedia.org/wiki/Oeis%3Aa114907
[7] "A page of number theoretical constants" (http://oeis.org/classic/a001692.shtml). 2007. . Retrieved 2007-06-20.
[8] http://en.wikipedia.org/wiki/Oeis%3Aa005597

External links

- Top-20 Twin Primes (http://primes.utm.edu/top20/page.php?id=1) at Chris Caldwell's Prime Pages.
- Xavier Gourdon, Pascal Sebah: *Introduction to Twin Primes and Brun's Constant* (http://numbers.computation.free.fr/Constants/Primes/twin.html)
- "Official press release" (http://mersenneforum.org/showpost.php?p=96237&postcount=51) of 58711-digit twin prime record.
- Weisstein, Eric W., " Twin Primes (http://mathworld.wolfram.com/TwinPrimes.html)" from MathWorld.
- The 20 000 first twin primes (http://arnflo.se/~site_files/Other/twinprimes)

Two-sided prime

In number theory, a **left-truncatable prime** is a prime number which, in a given base, contains no 0, and if the leading ("left") digit is successively removed, then all resulting numbers are prime. For example 9137, since 9137, 137, 37 and 7 are all prime. Decimal representation is often assumed and always used in this article.

A **right-truncatable prime** is a prime which remains prime when the last ("right") digit is successively removed. For example 7393, since 7393, 739, 73, 7 are all prime.

There are exactly 4260 decimal left-truncatable primes:

> 2, 3, 5, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 113, 137, 167, 173, 197, 223, 283, 313, 317, 337, 347, 353, 367, 373, 383, 397, 443, 467, 523, 547, 613, 617, 643, 647, 653, 673, 683, 743, 773, 797, 823, 853, 883, 937, 947, 953, 967, 983, 997, 1223, 1283, 1367 ... (sequence A024785 [16] in OEIS)

The largest is the 24-digit 357686312646216567629137.

There are 83 right-truncatable primes. The complete list:

> 2, 3, 5, 7, 23, 29, 31, 37, 53, 59, 71, 73, 79, 233, 239, 293, 311, 313, 317, 373, 379, 593, 599, 719, 733, 739, 797, 2333, 2339, 2393, 2399, 2939, 3119, 3137, 3733, 3739, 3793, 3797, 5939, 7193, 7331, 7333, 7393, 23333, 23339, 23399, 23993, 29399, 31193, 31379, 37337, 37339, 37397, 59393, 59399, 71933, 73331, 73939, 233993, 239933, 293999, 373379, 373393, 593933, 593993, 719333, 739391, 739393, 739397, 739399, 2339933, 2399333, 2939999, 3733799, 5939333, 7393913, 7393931, 7393933, 23399339, 29399999, 37337999, 59393339, 73939133 (sequence A024770 [43] in OEIS)

The largest is the 8-digit 73939133. All primes above 5 end with digit 1, 3, 7 or 9, so a right-truncatable prime can only contain those digits after the leading digit.

There are 15 primes which are both left-truncatable and right-truncatable. They have been called **two-sided primes**. The complete list:

> 2, 3, 5, 7, 23, 37, 53, 73, 313, 317, 373, 797, 3137, 3797, 739397 (A020994 [61])

While the primality of a number does not depend on the numeral system used, truncatable primes are defined only in relation with a given base. A variation involves removing 2 or more decimal digits at a time. This is mathematically equivalent to using base 100 or a larger power of 10, with the restriction that base 10^n digits must be at least 10^{n-1}, in order to match a decimal n-digit number with no leading 0.

References

- Weisstein, Eric W., "Truncatable Prime [1]" from MathWorld.
- Caldwell, Chris, *left-truncatable prime* [2] and *right-truncatable primes* [3], at the Prime Pages glossary.
- Rivera, Carlos, Problems & Puzzles: Puzzle 2.- Prime strings [4]

Ulam number

An **Ulam number** is a member of an integer sequence devised by and named after Stanislaw Ulam, who introduced it in 1964.[1] The standard Ulam sequence (the (1, 2)-Ulam sequence) starts with $U_1 = 1$ and $U_2 = 2$. Then for $n > 2$, U_n is defined to be the smallest integer that is the sum of two distinct earlier terms in exactly one way.

Examples

By the definition, 3 = 1 + 2 is an Ulam number; and 4 = 1 + 3 is an Ulam number (The sum 4 = 2 + 2 doesn't count because the previous terms must be distinct.) The integer 5 is not an Ulam number because 5 = 1 + 4 = 2 + 3. The first few terms are

> 1, 2, 3, 4, 6, 8, 11, 13, 16, 18, 26, 28, 36, 38, 47, 48, 53, 57, 62, 69, 72, 77, 82, 87, 97, 99 (sequence A002858 [2] in OEIS).

The first Ulam numbers that are also prime numbers are

> 2, 3, 11, 13, 47, 53, 97, 131, 197, 241, 409, 431, 607, 673, 739, 751, 983, 991, 1103, 1433, 1489 (A068820 [62]).

Infinite sequence

There are infinitely many Ulam numbers. For, after the first n numbers in the sequence have already been determined, it is always possible to extend the sequence by one more element: $U_{n-1} + U_n$ is uniquely represented as a sum of two of the first n numbers, and there may be other smaller numbers that are also uniquely represented in this way, so the next element can be chosen as the smallest of these uniquely representable numbers.[3]

Ulam is said to have conjectured that the numbers have zero density,[4] but they seem to have a density of approximately 0.07396.[5]

Generalizations

The idea can be generalized as (u, v)-Ulam numbers by selecting different starting values (u, v). A sequence of (u, v)-Ulam numbers is *regular* if the sequence of differences between consecutive numbers in the sequence is eventually periodic. When v is an odd number greater than three, the (2, v)-Ulam numbers are regular. When v is congruent to 1 (mod 4) and at least five, the (4, v)-Ulam numbers are again regular. However, the Ulam numbers themselves do not appear to be regular.[6]

A sequence of numbers is said to be s-additive if each number in the sequence, after the initial $2s$ terms of the sequence, has exactly s representations as a sum of two previous numbers. Thus, the Ulam numbers and the (u, v)-Ulam numbers are 1-additive sequences.[7]

If one forms a sequence by appending the largest number with a unique representation as a sum of two earlier numbers, instead of appending the smallest uniquely representable number, then the resulting sequence is the sequence of Fibonacci numbers.[8]

Notes

[1] Ulam (1964a, 1964b).

[2] http://en.wikipedia.org/wiki/Oeis%3Aa002858

[3] Recaman (1973) gives a similar argument, phrased as a proof by contradiction. He states that, if there were finitely many Ulam numbers, then the sum of the last two would also be an Ulam number, a contradiction. However, although the sum of the last two numbers would in this case have a unique representation as a sum of two Ulam numbers, it would not necessarily be the smallest number with a unique representation.

[4] The statement that Ulam made this conjecture is in OEIS A002858 (http://en.wikipedia.org/wiki/Oeis:a002858), but Ulam does not address the density of this sequence in Ulam (1964a), and in Ulam (1964b) he poses the question of determining its density without conjecturing a value for it. Recaman (1973) repeats the question from Ulam (1964b) of the density of this sequence, again without conjecturing a value for it.

[5] OEIS A002858 (http://en.wikipedia.org/wiki/Oeis:a002858)

[6] Queneau (1972) first observed the regularity of the sequences for $u = 2$ and $v = 7$ and $v = 9$. Finch (1992) conjectured the extension of this result to all odd v greater than three, and this conjecture was proven by Schmerl & Spiegel (1994). The regularity of the (4, v)-Ulam numbers was proven by Cassaigne & Finch (1995).

[7] Queneau (1972).

[8] Finch (1992).

References

- Cassaigne, Julien; Finch, Steven R. (1995), "A class of 1-additive sequences and quadratic recurrences" (http://www.emis.ams.org/journals/EM/restricted/4/4.1/finch.ps), *Experimental Mathematics* **4** (1): 49–60.
- Finch, Steven R. (1992), "On the regularity of certain 1-additive sequences", *Journal of Combinatorial Theory, Series A* **60** (1): 123–130, doi:10.1016/0097-3165(92)90042-S.
- Guy, Richard (2004), *Unsolved Problems in Number Theory* (3rd ed.), Springer-Verlag, pp. 166–167, ISBN 0-387-20860-7.
- Queneau, Raymond (1972), "Sur les suites *s*-additives" (in French), *Journal of Combinatorial Theory, Series A* **12** (1): 31–71, doi:10.1016/0097-3165(72)90083-0.
- Recaman, Bernardo (1973), "Questions on a sequence of Ulam" (http://www.jstor.org/stable/2319404), *American Mathematical Monthly* **80** (8): 919–920.
- Schmerl, James; Spiegel, Eugene (1994), "The regularity of some 1-additive sequences", *Journal of Combinatorial Theory, Series A* **66** (1): 172–175, doi:10.1016/0097-3165(94)90058-2.
- Ulam, Stanislaw (1964a), "Combinatorial analysis in infinite sets and some physical theories" (http://www.jstor.org/stable/2027963), *SIAM Review*: 343–355.
- Ulam, Stanislaw (1964b), *Problems in Modern Mathematics*, Wiley-Interscience, p. xi.

External links

- Ulam Sequence from MathWorld (http://mathworld.wolfram.com/UlamSequence.html)

Unique prime

In number theory, a **unique prime** is a certain kind of prime number. A prime $p \neq 2, 5$ is called **unique** if there is no other prime q such that the period length of the decimal expansion of its reciprocal, $1 / p$, is equivalent to the period length of the reciprocal of q, $1 / q$. Unique primes were first described by Samuel Yates in 1980.

It can be shown that a prime p is of unique period n if and only if there exists a natural number c such that

$$\frac{\Phi_n(10)}{\gcd(\Phi_n(10), n)} = p^c$$

where $\Phi_n(x)$ is the n-th cyclotomic polynomial. At present, more than fifty unique primes or probable primes are known. However, there are only twenty-three unique primes below 10^{100}. The following table gives an overview of all 23 unique primes below 10^{100} (sequence A040017 [63] in OEIS) and their periods (sequence A051627 [1] in OEIS):

Period length	Prime
1	3
2	11
3	37
4	101
10	9,091
12	9,901
9	333,667
14	909,091
24	99,990,001
36	999,999,000,001
48	9,999,999,900,000,001
38	909,090,909,090,909,091
19	1,111,111,111,111,111,111
23	11,111,111,111,111,111,111,111
39	900,900,900,900,990,990,990,991
62	909,090,909,090,909,090,909,090,909,091
120	100,009,999,999,899,989,999,000,000,010,001
150	10,000,099,999,999,989,999,899,999,000,000,000,100,001
106	9,090,909,090,909,090,909,090,909,090,909,090,909,090,909,090,909,091
93	900,900,900,900,900,900,900,900,900,900,990,990,990,990,990,990,990,990,990,991
134	909,090,909,090,909,090,909,090,909,090,909,090,909,090,909,090,909,090,909,090,909,091
294	142,857,157,142,857,142,856,999,999,985,714,285,714,285,857,142,857,142,855,714,285,571,428,571,428,572,857,143
196	999,999,999,999,990,000,000,000,000,099,999,999,999,999,000,000,000,000,009,999,999,999,999,900,000,000,000,001

The prime with period length 294 is similar to the reciprocal of 7 (0.142857142857142857...)

Just after the table, the twenty-fourth unique prime has 128 digits and period length 320. It can be written as $(9_{32}0_{32})_2 + 1$, where a subscript number n indicates n consecutive copies of the digit or group of digits before the subscript.

Though they are rare, based on the occurrence of repunit primes and probable primes, it is conjectured strongly that there are infinitely many unique primes. (Any repunit prime is unique.)

As of 2010 the repunit $(10^{270343}-1)/9$ is the largest known probable unique prime.[2]

In 1996 the largest *proven* unique prime was $(10^{1132} + 1)/10001$ or, using the notation above, $(99990000)_{141}+ 1$. Its reciprocal period is 2264. The record has been improved many times since then. As of 2010 the largest proven unique prime has 10,081 digits.[3]

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa051627

[2] PRP Records: Probable Primes Top 10000 (http://www.primenumbers.net/prptop/prptop.php)

[3] *The Top Twenty Unique*; Chris Caldwell (http://primes.utm.edu/top20/page.php?id=62)

External links

- The Prime Glossary: Unique prime (http://primes.utm.edu/glossary/page.php?sort=UniquePrime)
- Prime Top Tens (http://primes.utm.edu/lists/top_ten/topten.pdf)
- Unique Period Primes (http://www.utm.edu/staff/caldwell/preprints/unique.pdf)
- Factorization of 11...11 (Repunit) (http://homepage2.nifty.com/m_kamada/math/11111.htm)

Wagstaff prime

Publication year	1989[Note 1]
Author of publication	Bateman, P. T., Selfridge, J. L., Wagstaff Jr., S. S.
Number of known cases	30
OEIS index and link	A000979 [64]

In number theory, a **Wagstaff prime** is a prime number p of the form

$$p = \frac{2^q + 1}{3}$$

where q is another prime. Wagstaff primes are named after the mathematician Samuel S. Wagstaff Jr.; the prime pages credit François Morain for naming them in a lecture at the Eurocrypt 1990 conference. Wagstaff primes are related to the New Mersenne conjecture and have applications in cryptology.

The first three Wagstaff primes are 3, 11, and 43 because

$$3 = \frac{2^3 + 1}{3},$$
$$11 = \frac{2^5 + 1}{3},$$
$$43 = \frac{2^7 + 1}{3}.$$

The first few Wagstaff primes are:

> 3, 11, 43, 683, 2731, 43691, 174763, 2796203, 715827883, 2932031007403, … (sequence A000979 [64] in OEIS)

The first exponents q which produce Wagstaff primes or probable primes are:

> 3, 5, 7, 11, 13, 17, 19, 23, 31, 43, 61, 79, 101, 127, 167, 191, 199, 313, 347, 701, 1709, 2617, 3539, 5807, 10501, 10691, 11279, 12391, 14479, 42737, 83339, 95369, 117239, 127031, 138937, 141079, 267017, 269987, 374321, 986191, 4031399, … (sequence A000978 [65] in OEIS)

These numbers are proven to be prime for the values of q up to 42737. Those with $q > 42737$ are probable primes as of February 2010. The primality proof for $q = 42737$ was performed by François Morain in 2007 with a distributed ECPP implementation running on several networks of workstations for 743 GHz-days on an Opteron processor.[1] It is the fourth largest primality proof by ECPP as of 2010.[2]

The largest currently known probable Wagstaff prime

$$\frac{2^{4031399} + 1}{3}$$

was found by Tony Reix in February 2010.[3] It has 1,213,572 digits and it is the 3rd biggest PRP ever found at this date.

Currently, the fastest algorithm for proving the primality of Wagstaff numbers is ECPP.

Notes

1.^ Wagstaff primes were first described in Bateman, P. T., Selfridge, J. L., Wagstaff Jr., S. S. (1989). The New Mersenne Conjecture [4] *Amer. Math. Monthly* **96** 125-128

References

[1] Comment by François Morain, The Prime Database: $(2^{42737} + 1)/3$ (http://primes.utm.edu/primes/page.php?id=82071#comments) at The Prime Pages.

[2] Caldwell, Chris, "The Top Twenty: Elliptic Curve Primality Proof" (http://primes.utm.edu/top20/page.php?id=27), *The Prime Pages*,

[3] PRP Records (http://www.primenumbers.net/prptop/prptop.php)

[4] http://www.jstor.org/pss/2323195

External links

- John Renze and Eric W. Weisstein, " Wagstaff prime (http://mathworld.wolfram.com/WagstaffPrime.html)" from MathWorld.
- Chris Caldwell, *The Top Twenty: Wagstaff* (http://primes.utm.edu/top20/page.php?id=67) at The Prime Pages.
- Renaud Lifchitz, "An efficient probable prime test for numbers of the form $(2^p + 1)/3$" (http://ourworld.compuserve.com/homepages/hlifchitz/Documents/TestNP.zip).
- Tony Reix, "Three conjectures about primality testing for Mersenne, Wagstaff and Fermat numbers based on cycles of the Digraph under $x^2 - 2$ modulo a prime" (http://tony.reix.free.fr/Mersenne/SummaryOfThe3Conjectures.pdf).

Wall-Sun-Sun prime

In number theory, a **Wall–Sun–Sun prime** or **Fibonacci–Wieferich prime** is a certain kind of prime number which is conjectured to exist although none are known. A prime $p > 5$ is called a Wall–Sun–Sun prime if p^2 divides the Fibonacci number $F_{p-\left(\frac{p}{5}\right)}$, where the Legendre symbol $\left(\frac{p}{5}\right)$ is defined as

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5 \\ -1 & \text{if } p \equiv \pm 2 \pmod 5 \end{cases}$$

Wall–Sun–Sun primes are named after D. D. Wall,[1] Zhi Hong Sun and Zhi Wei Sun; Z. H. Sun and Z. W. Sun showed in 1992 that if the first case of Fermat's last theorem was false for a certain prime p, then p would have to be a Wall–Sun–Sun prime.[2] As a result, prior to Andrew Wiles' proof of Fermat's last theorem, the search for Wall–Sun–Sun primes was also the search for a counterexample to this centuries-old conjecture.

No Wall–Sun–Sun primes are known as of October 2010. In 2007, Richard J. McIntosh and Eric L. Roettger showed that if any exist, they must be $> 2\times10^{14}$.[3] It has been conjectured that there are infinitely many Wall–Sun–Sun primes.[4] The search for Wall-Sun-Sun primes has since then been extended to 9.7×10^{14} without finding such a prime.[5]

See also

- Wieferich prime
- Wilson prime
- Wolstenholme prime

References

[1] Wall, D. D. (1960), "Fibonacci Series Modulo m", *American Mathematical Monthly* **67** (6): 525–532, doi:10.2307/2309169

[2] Sun, Zhi-Hong; Sun, Zhi-Wei (1992), "Fibonacci numbers and Fermat's last theorem" (http://matwbn.icm.edu.pl/ksiazki/aa/aa60/aa6046.pdf), *Acta Arithmetica* **60** (4): 371–388,

[3] McIntosh, R. J.; Roettger, E. L. (2007), "A search for Fibonacci–Wieferich and Wolstenholme primes" (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.9393&rep=rep1&type=pdf), *Mathematics of Computation* **76** (260): 2087–2094, doi:10.1090/S0025-5718-07-01955-2,

[4] Klaška, Jiří (2007), "Short remark on Fibonacci–Wieferich primes" (http://dml.cz/dmlcz/137492), *Acta Mathematica Universitatis Ostraviensis* **15** (1): 21–25, .

[5] Dorais F. G., Klyve D. W. Near Wieferich primes up to 6.7 x 10^{15} (http://www-personal.umich.edu/~dorais/docs/wieferich.pdf)

Further reading

- Crandall, Richard E.; Pomerance, Carl (2001), *Prime Numbers: A Computational Perspective*, Springer, p. 29, ISBN 0387947779

External links

- Chris Caldwell, The Prime Glossary: Wall–Sun–Sun prime (http://primes.utm.edu/glossary/page.php?sort=WallSunSunPrime) at the Prime Pages.
- Weisstein, Eric W., " Wall–Sun–Sun prime (http://mathworld.wolfram.com/Wall-Sun-SunPrime.html)" from MathWorld.
- Richard McIntosh, Status of the search for Wall–Sun–Sun primes (October 2003) (http://www.loria.fr/~zimmerma/records/Wieferich.status)

Wedderburn-Etherington number

In graph theory, the **Wedderburn–Etherington numbers**, named for Ivor Malcolm Haddon Etherington and Joseph Wedderburn, count how many weak binary trees can be constructed: that is, the number of trees for which each graph vertex (not counting the root) is adjacent to no more than three other such vertices, for a given number of nodes. The first few Wedderburn–Etherington numbers are

1, 1, 1, 2, 3, 6, 11, 23, 46, 98, 207, 451, 983, 2179, 4850, 10905, 24631, 56011, 127912, 293547, 676157, 1563372, 3626149, 8436379, 19680277, 46026618, 107890609, 253450711, 596572387, 1406818759, 3323236238, 7862958391,... (sequence A001190 [66] in OEIS)

References

- S. J. Cyvin et al., "Enumeration of constitutional isomers of polyenes," *J. Molec. Structure (Theochem)* **357** (1995): 255–261
- I. M. H. Etherington, "Non-associate powers and a functional equation," *Math. Gaz.* **21** (1937): 36–39, 153
- I. M. H. Etherington, "On non-associative combinations," *Proc. Royal Soc. Edinburgh*, **59** 2 (1939): 153–162.
- S. R. Finch, *Mathematical Constants*. Cambridge: Cambridge University Press (2003): 295–316
- F. Murtagh, "Counting dendrograms: a survey," *Discrete Applied Mathematics* **7** (1984): 191–199
- J. H. M. Wedderburn, "The functional equation $g(x^2) = 2ax + [g(x)]^2$" *Ann. Math.* **24** (1923): 121–140

Wieferich pair

In mathematics, a **Wieferich pair** is a pair of prime numbers p and q that satisfy

$$p^{q-1} \equiv 1 \pmod{q^2} \text{ and } q^{p-1} \equiv 1 \pmod{p^2}$$

Wieferich pairs are named after German mathematician Arthur Wieferich.

There are only six Wieferich pairs known:[1]

(2, 1093), (3, 1006003), (5, 1645333507), (83, 4871), (911, 318917), and (2903, 18787) (sequence A124121 [2] and A124122 [3] in OEIS)

Wieferich pairs play an important role in Preda Mihăilescu's 2002 proof[4] of Mihăilescu's theorem (formerly known as Catalan's conjecture).[5]

References

[1] Weisstein, Eric W., " Double Wieferich Prime Pair (http://mathworld.wolfram.com/DoubleWieferichPrimePair.html)" from MathWorld.

[2] http://en.wikipedia.org/wiki/Oeis%3Aa124121

[3] http://en.wikipedia.org/wiki/Oeis%3Aa124122

[4] Preda Mihăilescu (2004). "Primary Cyclotomic Units and a Proof of Catalan's Conjecture". *J. Reine Angew. Math.* **572**: 167–195. MR2076124.

[5] Jeanine Daems A Cyclotomic Proof of Catalan's Conjecture (http://www.math.leidenuniv.nl/~jdaems/scriptie/Catalan.pdf).

Further reading

- Yuri Bilu (2004). "Catalan's conjecture (after Mihăilescu)". *Astérisque* **294**: vii, 1 – 26.
- R. Ernvall; T. Metsänkylä (1997). "On the *p*-divisibility of Fermat quotients" (http://www.ams.org/mcom/1997-66-219/S0025-5718-97-00843-0/home.html). *Math. Comp.* **66** (219): 1353–1365. doi:10.1090/S0025-5718-97-00843-0.

- Ray Steiner (1998). "Class number bounds and Catalan's equation" (http://www.ams.org/mcom/1998-67-223/S0025-5718-98-00966-1/home.html). *Math. Comp.* **67** (213): 1317–1322. doi:10.1090/S0025-5718-98-00966-1.

Wieferich prime

Publication year	1909
Author of publication	Wieferich, A.
Number of known cases	2
OEIS index and link	A001220 [67]

In number theory, a **Wieferich prime** is defined as a prime number p such that p^2 divides $2^{p-1} - 1$,[1] therefore connecting these primes with Fermat's little theorem, which states that every odd prime p divides $2^{p-1} - 1$. Wieferich primes were first described by Arthur Wieferich in 1909 in works pertaining to Fermat's last theorem, at which time both of Fermat's theorems had already been well known to mathematicians.[2] [3]

The search for Wieferich primes

The only known Wieferich primes are 1093 and 3511 (sequence A001220 [67] in OEIS), found by W. Meissner in 1913 and N. G. W. H. Beeger in 1922, respectively. If any other Wieferich primes exist, they must be greater than 6.7×10^{15}.[4] It has been conjectured that only finitely many Wieferich primes exist.[1] It has also been conjectured (as for Wilson primes) that infinitely many Wieferich primes exist, and that the number of Wieferich primes below x is approximately $\log \log x$, which is the heuristic result followed from a plausible assumption that for a prime p, the (p-1)-th degree roots of unity modulo p^2 are uniformly distributed in the multiplicative group of integers modulo p^2.

Although all available numerical evidence suggests that there are very few Wieferich primes, it is still an open problem to prove that there are infinitely many primes that are *not* Wieferich primes.

The search for new Wieferich primes is currently performed by the distributed computing project Wieferich@Home.

Properties of Wieferich primes

- It is known that the nth Mersenne number $M_n = 2^n - 1$ is prime only if n is prime. Fermat's little theorem implies that if $p > 2$ is prime, then M_{p-1} ($= 2^{p-1} - 1$) is always divisible by p. Since Mersenne numbers of prime indices M_p and M_q are co-prime,

  A prime divisor p of M_q, where q is prime, is a Wieferich prime if and only if p^2 divides M_q.[5]

  Thus, a Mersenne prime cannot also be a Wieferich prime. A notable open problem is to determine whether or not all Mersenne numbers of prime index are square-free. If a Mersenne number M_q is *not* square-free, i.e., there exists a prime p for which p^2 divides M_q, then p is a Wieferich prime. Therefore, if there are only finitely many Wieferich primes, then there will be at most finitely many Mersenne numbers that are not square-free.
- Similarly, if p is prime and p^2 divides some Fermat number $F_n = 2^{2^n} + 1$, then p must be a Wieferich prime.[6]
- Johnson observed[7] that the two known Wieferich primes are one greater than numbers with periodic binary expansions ($1092 = 010001000100_2$; $3510 = 110110110110_2$). The Wieferich@Home project searches for Wieferich primes by testing numbers that are one greater than a number with a periodic binary expansion, but up to a total binary expansion length of 3500 and up to a period length of 24 it has not found a new Wieferich prime.[8]

- If p is a Wieferich prime, then $2^{p^2} = 2 \pmod{p^2}$.

Wieferich primes and Fermat's last theorem

The following theorem connecting Wieferich primes and Fermat's last theorem was proven by Wieferich in 1909:

> Let p be prime, and let x, y, z be integers such that $x^p + y^p + z^p = 0$. Furthermore, assume that p does not divide the product xyz. Then p is a Wieferich prime.

In 1910, Mirimanoff was able to expand the theorem by showing that, if the preconditions of the theorem hold true for some prime p, then p^2 must also divide $3^{p-1} - 1$.

Generalizations

- A prime p satisfying the congruence $2^{(p-1)/2} \equiv \pm 1 + Ap \pmod{p^2}$ with small $|A|$ is commonly called a *near-Wieferich prime*.[9] [10] Near-Wieferich primes with $A = 0$ represent Wieferich primes. Recent searches, in addition to their primary search for Wieferich primes, also tried to find near-Wieferich primes.[4] [11] The following table lists all near-Wieferich primes with $|A| < 100$ up to 3×10^{15}.
- Dorais and Klyve came up with a new definition of a Near-Wieferich prime.[4] Let the Fermat quotient of n mod p be $\omega(p) = \frac{2^{p-1} - 1}{p}$. The following table lists all primes p with small $\left|\frac{\omega(p)}{p}\right|$ up to 6.7×10^{15}
- A *Wieferich prime base a* is a prime p that satisfies

  $a^{p-1} \equiv 1 \pmod{p^2}$.[12]

  Such a prime cannot divide a, since then it would also divide 1. For the known Wieferich primes base a with small prime values of a, see Fermat quotient.
- A Wieferich pair is a pair of primes p and q that satisfy

  $p^{q-1} \equiv 1 \pmod{q^2}$ and $q^{p-1} \equiv 1 \pmod{p^2}$

  so that a Wieferich prime p which is $\equiv 1 \pmod 4$ will form such a pair $(p, 2)$: the only known instance in this case is $p = 1093$. There are 6 known Wieferich pairs.[13]
- For a cyclotomic generalisation of the Wieferich property:$(n^p - 1)/(n - 1)$ divisible by q^2, there are solutions like

  $(3^5 - 1)/(3 - 1) = 11^2$

  and even with exponents higher than 2, like in

  $(19^6 - 1)/(19 - 1) \equiv 0 \pmod{7^3}$.

See also

- Wilson prime
- Wall-Sun-Sun prime
- Wolstenholme prime
- Taro Morishima
- Double Mersenne number
- Fermat quotient

References

[1] *The Prime Glossary: Wieferich prime* (http://primes.utm.edu/glossary/xpage/WieferichPrime.html),

[2] Israel Kleiner (2000), "From Fermat to Wiles: Fermat's Last Theorem Becomes a Theorem" (http://math.stanford.edu/~lekheng/flt/kleiner.pdf), *Elem. Math.* **55**: 21, .

[3] Leonhard Euler (1736), "Theorematum quorundam ad numeros primos spectantium demonstratio" (http://math.dartmouth.edu/~euler/pages/E054.html), *Novi Comm. Acad. Sci. Petropol.* **8**: 33–37, .

[4] F. G. Dorais and D. W. Klyve Near Wieferich primes up to 6.7×10^{15} (http://www-personal.umich.edu/~dorais/docs/wieferich.pdf)

[5] *Mersenne Primes: Conjectures and Unsolved Problems* (http://primes.utm.edu/mersenne/index.html#unknown),

[6] Ribenboim, Paulo (1991), *The little book of big primes* (http://books.google.com/?id=zUCK7FT4xgAC&pg=PA64), New York: Springer, p. 64, ISBN 038797508X,

[7] Wells Johnson (1977), "On the nonvanishing of Fermat quotients (mod p)" (http://www.digizeitschriften.de/index.php?id=resolveppn&PPN=GDZPPN002193698), *J. reine angew. Math.* **292**: 196–200,

[8] Jan Dobeš; Miroslav Kureš (2010), "Search for Wieferich primes through the use of periodic binary strings", *Serdica Journal of Computing* **4**: 293–300

[9] Crandall, Dilcher and Pomerance A search for Wieferich and Wilson primes (http://www.math.dartmouth.edu/~carlp/PDF/paper111.pdf)

[10] Joshua Knauer; Jörg Richstein (2005), "The continuing search for Wieferich primes" (http://www.ams.org/journals/mcom/2005-74-251/S0025-5718-05-01723-0/S0025-5718-05-01723-0.pdf), *Math. Comp.* **74**: 1559–1563, doi:10.1090/S0025-5718-05-01723-0, .

[11] About project Wieferich@Home (http://www.elmath.org/index.php?id=main)

[12] Wilfrid Keller; Jörg Richstein (2005), "Solutions of the congruence $a^{p-1}\equiv1 \pmod{p^r}$" (http://www.ams.org/journals/mcom/2005-74-250/S0025-5718-04-01666-7/S0025-5718-04-01666-7.pdf), *Math. Comp.* **74**: 927–936, doi:10.1090/S0025-5718-04-01666-7, .

[13] Weisstein, Eric W., " Double Wieferich Prime Pair (http://mathworld.wolfram.com/DoubleWieferichPrimePair.html)" from MathWorld.

Further reading

- Wieferich, A. (1909), "Zum letzten Fermat'schen Theorem" (http://gdz.sub.uni-goettingen.de/dms/resolveppn/?PPN=GDZPPN002166968), *Journal für die reine und angewandte Mathematik* **136**: 293–302
- Mirimanoff, D. (1910), "Sur le dernier théorème de Fermat", *Comptes rendus hebdomadaires des séances de l'Académie des Sciences* **150**: 293–206
- Beeger, N. G. W. H. (1922), "On a new case of the congruence $2^{p-1} \equiv 1 \ (p^2)$" (http://ia301527.us.archive.org/1/items/messengerofmathe5051cambuoft/messengerofmathe5051cambuoft.pdf), *Messenger of Mathematics* **51**: 149–150
- Meissner, W. (1913), "Über die Teilbarkeit von $2p^p - 2$ durch das Quadrat der Primzahl p=1093", *Sitzungsber. Akad. D. Wiss. Berlin*: 663–667
- Silverman, J. H. (1988), "Wieferich's criterion and the abc-conjecture", *Journal of Number Theory* **30** (2): 226–237, doi:10.1016/0022-314X(88)90019-4
- Morishima, T. (1935), "Ueber die Fermatsche Vermutung. XI" (in German), *Jap. J. Math.* **11**: 241–252
- Ribenboim, P. (1979), *Thirteen lectures on Fermat's Last Theorem*, Springer-Verlag, pp. 139, 151, ISBN 0-387-90432-8
- Crandall, Richard E.; Dilcher, Karl; Pomerance, Carl (1997), "A search for Wieferich and Wilson primes" (http://gauss.dartmouth.edu/~carlp/PDF/paper111.pdf), *Math. Comput.* **66** (217): 433–449, doi:10.1090/S0025-5718-97-00791-6
- Guy, Richard K. (2004), *Unsolved Problems in Number Theory* (3rd ed.), Springer Verlag, p. 14, ISBN 0387208607.

External links

- Weisstein, Eric W., " Wieferich prime (http://mathworld.wolfram.com/WieferichPrime.html)" from MathWorld.
- Fermat-/Euler-quotients $(a^{p-1}-1)/p^k$ with arbitrary k (http://go.helms-net.de/math/expdioph/fermatquotients.pdf)
- A note on the two known Wieferich primes (http://cybrary.uwinnipeg.ca/people/dobson/mathematics/Wieferich_primes.html)

Wilson prime

Publication year	1938[Note 1]
Author of publication	Lehmer, E.
Number of known cases	3
OEIS index and link	A007540 [68]

A **Wilson prime**, named after John Wilson, is a prime number p such that p^2 divides $(p - 1)! + 1$, where "!" denotes the factorial function; compare this with Wilson's theorem, which states that every prime p divides $(p - 1)! + 1$.

The only known Wilson primes are 5, 13, and 563 (sequence A007540 [68] in OEIS); if any others exist, they must be greater than 5×10^8.[1] It has been conjectured that infinitely many Wilson primes exist, and that the number of Wilson primes in an interval $[x, y]$ is about $\log(\log(y) / \log(x))$.[2]

Generalizations

- A prime p satisfying the congruence $(p - 1)! \equiv \pm1 + Bp \pmod{p^2}$ with small $|B|$ can be called a **near-Wilson prime**. Near-Wilson primes with B=0 represent Wilson primes. The following table lists all such primes with |B| <= 100 up to 6 x 10^9 (Based on information by Richard Crandall, Karl Dilcher and Carl Pomerance as well as Richard McIntosh and Mark Rodenkirch):

See also

- Wieferich prime
- Wall-Sun-Sun prime
- Wolstenholme prime

Notes

1.^ Wilson primes were first described by Lehmer, E. On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson [3], Ann. of. Math. **39**(1938), 350-360.

[1] Status of the search for Wilson primes (http://www.loria.fr/~zimmerma/records/Wieferich.status), also see Crandall et. al. 1997

[2] The Prime Glossary: Wilson prime (http://primes.utm.edu/glossary/page.php?sort=WilsonPrime)

[3] http://www.google.de/url?sa=t&source=web&cd=10&ved=0CGgQFjAJ&url=http%3A%2F%2Fgradelle.educanet2.ch%2Fchristian.aebi%2F.ws_gen%2F14%2FEmma_Lehmer_1938.pdf&rct=j&q=lehmer%20on%20congruences%20involving%20bernoulli%20numbers%20and%20the%20quotients%20of%20fermat%20and%20wilson&ei=QVHcTK2iAZDysgae9o2iBA&usg=AFQjCNGuZ93z06kDmxXutGU8S_ADA6FgZw&cad=rja

References

- N. G. W. H. Beeger (1913-1914). "Quelques remarques sur les congruences $r^{p-1} \equiv 1 \pmod{p^2}$ et $(p-1)! \equiv -1 \pmod{p^2}$". *The Messenger of Mathematics* **43**: 72-84.
- Karl Goldberg (1953). "A table of Wilson quotients and the third Wilson prime". *J. Lond. Math. Soc.* **28**: 252–256. doi:10.1112/jlms/s1-28.2.252.
- Paulo Ribenboim (1996). *The new book of prime number records*. Springer-Verlag. pp. 346. ISBN 0-387-94457-5.
- Richard E. Crandall; Karl Dilcher, Carl Pomerance (1997). "A search for Wieferich and Wilson primes". *Math. Comput.* **66** (217): 433–449. doi:10.1090/S0025-5718-97-00791-6.

- Richard E. Crandall; Carl Pomerance (2001). *Prime Numbers: A Computational Perspective*. Springer-Verlag. p. 29. ISBN 0-387-94777-9.
- Takashi Agoh; Karl Dilcher, Ladislav Skula (1998). "Wilson quotients for composite moduli" (http://en.wikipedia.org/w/index.php?title=Wilson_prime&action=edit&section=4). *Math. Comput.* **67** (222): 843-861.
- Erna H. Pearson (1963). "On the Congruences (p-1)! ≡ -1 and $2^{p-1} \equiv 1 \pmod{p^2}$" (http://www.ams.org/journals/mcom/1963-17-082/S0025-5718-1963-0159780-0/S0025-5718-1963-0159780-0.pdf). *Math. Comput.* **17**: 194-195.

External links

- The Prime Glossary: Wilson prime (http://primes.utm.edu/glossary/page.php?sort=WilsonPrime)
- Weisstein, Eric W., " Wilson prime (http://mathworld.wolfram.com/WilsonPrime.html)" from MathWorld.
- Status of the search for Wilson primes (http://www.loria.fr/~zimmerma/records/Wieferich.status)
- Wilson Quotients for composite moduli (http://www.google.de/url?sa=t&source=web&cd=3&ved=0CC4QFjAC&url=http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.6544&rep=rep1&type=pdf&rct=j&q=a table of wilson quotients and the third wilson prime&ei=nk_cTPjcJMv4sgaLn4yiBA&usg=AFQjCNHrvGLzlN26fFSUfC1sh5keBqvpWA&cad=rja)
- On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson (http://www.google.de/url?sa=t&source=web&cd=10&ved=0CGgQFjAJ&url=http://gradelle.educanet2.ch/christian.aebi/.ws_gen/14/Emma_Lehmer_1938.pdf&rct=j&q=lehmer on congruences involving bernoulli numbers and the quotients of fermat and wilson&ei=QVHcTK2iAZDysgae9o2iBA&usg=AFQjCNGuZ93z06kDmxXutGU8S_ADA6FgZw&cad=rja)

Wolstenholme prime

In mathematics, **Wolstenholme's theorem** states that for a prime number $p > 3$, the congruence

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$$

holds, where the parentheses denote a binomial coefficient. For example, with $p = 7$, this says that 1716 is one more than a multiple of 343. An equivalent formulation is the congruence

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}.$$

The theorem was first proved by Joseph Wolstenholme in 1862. In 1819, Charles Babbage showed the same congruence modulo p^2, which holds for all primes p (for p=2 only in the second formulation). The second formulation of Wolstenholme's theorem is due to J. W. L. Glaisher and is inspired by Lucas' theorem.

No known composite numbers satisfy Wolstenholme's theorem and it is conjectured that there are none (see below). A prime that satisfies the congruence modulo p^4 is called a **Wolstenholme prime** (see below).

As Wolstenholme himself established, his theorem can also be expressed as a pair of congruences for (generalized) harmonic numbers:

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} \equiv 0 \pmod{p^2}, \text{ and}$$
$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p}.$$

(Congruences with fractions make sense, provided that the denominators are coprime to the modulus.) For example, with p=7, the first of these says that the numerator of 49/20 is a multiple of 49, while the second says the numerator

of 5369/3600 is a multiple of 7.

Wolstenholme primes

A prime *p* is called a Wolstenholme prime iff the following condition holds:

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}.$$

If *p* is a Wolstenholme prime, then Glaisher's theorem holds modulo p^4. The only known Wolstenholme primes so far are 16843 and 2124679 (sequence A088164 [69] in OEIS); any other Wolstenholme prime must be greater than 10^9.[1] This result is consistent with the heuristic argument that the residue modulo p^4 is a pseudo-random multiple of p^3. This heuristic predicts that the number of Wolstenholme primes between *K* and *N* is roughly *ln ln N - ln ln K*. The Wolstenholme condition has been checked up to 10^9, and the heuristic says that there should be roughly one Wolstenholme prime between 10^9 and 10^{24}. A similar heuristic predicts that there are no "doubly Wolstenholme" primes, meaning that the congruence holds modulo p^5.

A proof of the theorem

There is more than one way to prove Wolstenholme's theorem. Here is a proof that directly establishes Glaisher's version using both combinatorics and algebra.

For the moment let *p* be any prime, and let *a* and *b* be any non-negative integers. Then a set *A* with *ap* elements can be divided into *a* rings of length *p*, and the rings can be rotated separately. Thus, the group $C_p{}^a$ acts on the set *A*, and by extension it acts on the set of subsets of size *bp*. Every orbit of this group action has p^k elements, where *k* is the number of incomplete rings, i.e., if there are *k* rings that only partly intersect a subset *B* in the orbit. There are $\binom{a}{b}$ orbits of size 1 and there are no orbits of size *p*. Thus we first obtain Babbage's theorem

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^2}.$$

Examining the orbits of size p^2, we also obtain

$$\binom{ap}{bp} \equiv \binom{a}{b} + \binom{a}{2}\left(\binom{2p}{p} - 2\right)\binom{a-2}{b-1} \pmod{p^3}.$$

Among other consequences, this equation tells us that the case *a=2* and *b=1* implies the general case of the second form of Wolstenholme's theorem.

Switching from combinatorics to algebra, both sides of this congruence are polynomials in *a* for each fixed value of *b*. The congruence therefore holds when *a* is any integer, positive or negative, provided that *b* is a fixed positive integer. In particular, if *a=-1* and *b=1*, the congruence becomes

$$\binom{-p}{p} \equiv \binom{-1}{1} + \binom{-1}{2}\left(\binom{2p}{p} - 2\right) \pmod{p^3}.$$

This congruence becomes an equation for $\binom{2p}{p}$ using the relation

$$\binom{-p}{p} = \frac{(-1)^p}{2}\binom{2p}{p}.$$

When *p* is odd, the relation is

$$3\binom{2p}{p} \equiv 6 \pmod{p^3}.$$

When $p \neq 3$, we can divide both sides by 3 to complete the argument.

A similar derivation modulo p^4 establishes that

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^4}$$

for all positive *a* and *b* if and only if it holds when *a=2* and *b=1*, i.e., if and only if *p* is a Wolstenholme prime.

The converse as a conjecture

It is conjectured that if

$$\binom{2n-1}{n-1} \equiv 1 \pmod{n^k},$$

when *k=3*, then *n* is prime. The conjecture can be understood by considering $k = 1$ and 2 as well as 3. When $k = 1$, Babbage's theorem implies that it holds for $n = p^2$ for p an odd prime, while Wolstenholme's theorem implies that it holds for $n = p^3$ for $p > 3$. When $k = 2$, it holds for $n = p^2$ if p is a Wolstenholme prime. Only a few other composite values of n are known when $k = 1$, and none are known when $k = 2$, much less $k = 3$. Thus the conjecture is considered likely because Wolstenholme's congruence seems over-constrained and artificial for composite numbers. Moreover, if the congruence does hold for any particular n other than a prime or prime power, and any particular k, it does not imply that

$$\binom{an}{bn} \equiv \binom{a}{b} \pmod{n^k}.$$

See also

- Fermat's little theorem
- Wilson's theorem
- Wieferich prime
- Wilson prime
- Wall-Sun-Sun prime
- List of special classes of prime numbers

References

[1] McIntosh, R. J.; Roettger, E. L. (2007), "A search for Fibonacci–Wieferich and Wolstenholme primes" (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.9393&rep=rep1&type=pdf), *Mathematics of Computation* **76** (260): 2087–2094, doi:10.1090/S0025-5718-07-01955-2,

- Babbage, C. (1819), "Demonstration of a theorem relating to prime numbers" (http://books.google.de/books?id=KrA-AAAAYAAJ&pg=PA46), *The Edinburgh philosophical journal* **1**: 46–49.
- Wolstenholme, J. (1862), "On certain properties of prime numbers" (http://books.google.com/books?id=vL0KAAAAIAAJ&pg=PA35), *The Quarterly Journal of Pure and Applied Mathematics* **5**: 35–39.
- McIntosh, R. J. (1995), "On the converse of Wolstenholme's theorem" (http://matwbn.icm.edu.pl/ksiazki/aa/aa71/aa7144.pdf), *Acta Arithmetica* **71** (4): 381–389.

External links

- The Prime Glossary: Wolstenholme prime (http://primes.utm.edu/glossary/page.php?sort=Wolstenholme)
- Status of the search for Wolstenholme primes (http://www.loria.fr/~zimmerma/records/Wieferich.status)

Woodall number

In number theory, a **Woodall number** (W_n) is any natural number of the form

$$W_n = n \times 2^n - 1$$

for some natural number n. The first few Woodall numbers are:

1, 7, 23, 63, 159, 383, 895, … (sequence A003261 [1] in OEIS).

Woodall numbers were first studied by Allan J. C. Cunningham and H. J. Woodall in 1917, inspired by James Cullen's earlier study of the similarly-defined Cullen numbers. Woodall numbers curiously arise in Goodstein's theorem.

Woodall numbers that are also prime numbers are called **Woodall primes**; the first few exponents n for which the corresponding Woodall numbers W_n are prime are 2, 3, 6, 30, 75, 81, 115, 123, 249, 362, 384, … (sequence A002234 [2] in OEIS); the Woodall primes themselves begin with 7, 23, 383, 32212254719, … (sequence A050918 [70] in OEIS).

In 1976 Christopher Hooley showed that almost all Cullen numbers are composite. Hooley's proof was reworked by Hiromi Suyama to show that it works for any sequence of numbers $n \cdot 2^{n+a} + b$ where a and b are integers, and in particular also for Woodall numbers. Nonetheless, it is conjectured that there are infinitely many Woodall primes. As of December 2007, the largest known Woodall prime is $3752948 \times 2^{3752948} - 1$.[3] It has 1,129,757 digits and was found by Matthew J. Thompson in 2007 in the distributed computing project PrimeGrid.

Like Cullen numbers, Woodall numbers have many divisibility properties. For example, if p is a prime number, then p divides

$W_{(p+1)/2}$ if the Jacobi symbol $\left(\frac{2}{p}\right)$ is +1 and

$W_{(3p-1)/2}$ if the Jacobi symbol $\left(\frac{2}{p}\right)$ is −1.

A **generalized Woodall number** is defined to be a number of the form $n \times b^n - 1$, where $n + 2 > b$; if a prime can be written in this form, it is then called a **generalized Woodall prime**.

References

[1] http://en.wikipedia.org/wiki/Oeis%3Aa003261

[2] http://en.wikipedia.org/wiki/Oeis%3Aa002234

[3] "The Prime Database: 938237*2^3752950-1" (http://primes.utm.edu/primes/page.php?id=83407), *Chris Caldwell's The Largest Known Primes Database*, , retrieved December 22, 2009

Further reading

- Guy, Richard K. (2004), *Unsolved Problems in Number Theory* (3rd ed.), New York: Springer Verlag, pp. section B20, ISBN 0387208607.
- Keller, Wilfrid (1995), "New Cullen Primes" (http://www.ams.org/mcom/1995-64-212/S0025-5718-1995-1308456-3/S0025-5718-1995-1308456-3.pdf), *Mathematics of Computation* **64** (212): 1733–1741.
- Caldwell, Chris, "The Top Twenty: Woodall Primes" (http://primes.utm.edu/top20/page.php?id=7), *The Prime Pages*, retrieved December 29, 2007.

External links

- Chris Caldwell, The Prime Glossary: Woodall number (http://primes.utm.edu/glossary/page.php?sort=WoodallNumber) at The Prime Pages.
- Weisstein, Eric W., " Woodall number (http://mathworld.wolfram.com/WoodallNumber.html)" from MathWorld.
- Steven Harvey, List of Generalized Woodall primes (http://harvey563.tripod.com/GeneralizedWoodallPrimes.txt).

Article Sources and Contributors

Prime number theorem *Source*: http://en.wikipedia.org/w/index.php?oldid=408122982 *Contributors*: AbcXyz, Alexjohnc3, Anonymous Dissident, Arcfrk, Arthur Rubin, AxelBoldt, Bab dz, Bbaumer, Bender235, Bernfarr, BeteNoir, Billymac00, Bryan Derksen, Bubba73, CRGreathouse, Charles Matthews, Charleswallingford, Chas zzz brown, Ck lostsword, Conversion script, DYLAN LENNON, Dahn, David Eppstein, DavidCBryant, Dbenbenn, Decrypt3, Dessources, Diza, Dmharvey, Dmr2, Doctormatt, Dysprosia, EmilJ, Endlessoblivion, Eric Ng, Fred Stober, Gandalf61, Giftlite, Gregbard, HappyCamper, Herbee, II MusLiM HyBRiD II, Inwind, JamesBWatson, JensG, JerryFriedman, Jitse Niesen, Jnestorius, John Vandenberg, JoshuaZ, Justin W Smith, KSmrq, Karl-H, Katsushi, Kidburla, Kompik, Linas, Looxix, Lupin, Maxal, Mcsee, Mdotley, Michael Hardy, Mon4, Motomuku, Myasuda, Nicolae Coman, Ninjagecko, Nono64, Nuesken, Olaf, Paul August, Pottermagic, PrBeacon, Primalbeing, PrimeHunter, Python eggs, R.e.b., RA0808, Rich Farmbrough, Roybb95, Salgueiro, ScottAlanHill, Scythe33, Skimaxpower, Sligocki, Sstrader, Statsone, TMC1221, TakuyaMurata, Tarotcards, Thomassteinke, Tobias Bergemann, Uncia, Viebel, Vincent Semeria, WAREL, Wellithy, Wereon, XJamRastafire, Xiong Chiamiov, Zooloo, 93 anonymous edits

Riemann hypothesis *Source*: http://en.wikipedia.org/w/index.php?oldid=408429291 *Contributors*: 345Kai, A-Doo, Aiden Fisher, Albert Einstein2011, Allmightyduck, Andrei Stroe, Anonymous Dissident, Antandrus, Anupam, Army1987, Arthur Rubin, Atlantia, AxelBoldt, Aydinkutlu, Baiji, Barticus88, Bender235, BigFatBuddha, Bkkbrad, Boing! said Zebedee, Bubba73, C S, CRGreathouse, Calton, Can't sleep, clown will eat me, Carnildo, Cedars, Cenarium, Charles Matthews, Chartguy, Ched Davis, Chinju, Chocolateboy, Chrisguidry, Cole Kitchen, Conscious, Conversion script, Cool Blue, Copedance, Corkgkagj, Crisófilax, DBrane, DYLAN LENNON, Daqu, David Eppstein, David Gerard, David Haslam, Deadbarnacle, DerHexer, Dicconb, DiceDiceBaby, Discospinster, Dmharvey, Dod1, Dominic, Doomed Rasher, Dr. Leibniz, Dr. Megadeth, Droog Andrey, Dto, Dysprosia, ERcheck, Egg, Einsteinino, Ekaratsuba, Emersoni, Emholvoet, EmilJ, Epbr123, Eric119, Ericamick, Erud, Estel, Evercat, F3et, Fournax, Fredrik, Frenchwhale, Freticat, Fullmetal2887, Fumblebruschi, GTBacchus, Gandalf61, Gary King, Gavia immer, Gene Ward Smith, Gershwinrb, Giftlite, Gika, Gingermint, GirasoleDE, Guardian of Light, Gurch, HaeB, Halo, Harleyjamesmunro, He Who Is, Helohe, Henry Delforn, Herbee, Hofingerandi, Hu, Hut 8.5, Iamunknown, IanOsgood, Ianmacm, Icairns, Ilyanep, InvertRect, IronSwallow, J.delanoy, JW1805, JackSchmidt, Jacobolus, Jakob.scholbach, Jeppesn, Jheald, Jijinmachina, Jitse Niesen, Joel.Gilmore, Jtwdog, Jujutacular, Julesd, Karl-H, Karl-Henner, Katsushi, Kdoto, Kh7, Kingdon, Klaus, KnowledgeOfSelf, Krea, LDH, LiDaobing, Linas, Loadmaster, Looxix, LouisWins, Lzur, Madmath789, Maha ts, MarkSutton, Marudubshinki, Mcarling, Mcsee, Meekohi, Michael Hardy, Million Little Gods, Mindmatrix, Mistamagic28, Mon4, Motomuku, Mpatel, Mpeisenbr, Mrhawley, Myasuda, NatusRoma, Neilc, Nicolasqueen, Numerao, Obradovic Goran, Ocolon, Ofap, Oleg Alexandrov, Olivier, Openshac, Opustylnikov, Oshanker, Overlord 77520, PL290, Pasky, Peterungar, Phil Boswell, Piet Delport, Pip2andahalf, Plastikspork, Pleasantville, PrimeHunter, Profstein, Pstudier, Pt, Qui1che, R.e.b., REGULAR-NORMAL, Raul654, Raulshc, Ravi12346, Rchamberlin, Reinyday, Revolver, Rgclegg, Rich Farmbrough, Ripe, Rivertorch, Rjwilmsi, RobHar, RobertG, Rodhullandemu, Ruakh, Rylann, STRANGELUV3, Saccerzd, Saga City, Salix alba, Sallypally, Sbjf, Schneelocke, Scythe33, Seglea, Seraphita, Sherbrooke, Shimgray, Shreevatsa, Sidis24, Slonzor, Snthdiueoa, Speight, Suruena, Svetovid, Symplectic Map, TakuyaMurata, Tarquin, Taxman, Teeesssyyy, The Anome, TheCustomOfLife, TheSeven, Thehotelambush, Timhoooey, Timothy Clemans, Tobias Bergemann, Tpbradbury, Travelbird, TravisAF, UkPaolo, Venona2007, Vinoo Cameron, Vipul, Voidxor, WAREL, Wafulz, Waprap, Wile E. Heresiarch, William Avery, Woseph, Wshun, Wwwolf, XJamRastafire, Yurakm, ZX81, Zaian, Zondor, 399 anonymous edits

Riemann zeta function *Source*: http://en.wikipedia.org/w/index.php?oldid=408649161 *Contributors*: 212.134.18.xxx, A. Pichler, AJRG, Alexf, Alffa, Ancheta Wis, Andrei Stroe, Anville, Arcette, Arcfrk, Arthur Rubin, Auclairde, AxelBoldt, Aymesq, Bdmy, Beanyk, Beck128, Boud, C S, CRGreathouse, Caekaert, Calvin 1998, Carbuncle, Carifio24, ChaosCon343, Conversion script, Cotterr2, Count Iblis, D.vegetali, DRLB, Dantheox, Daqu, Dauto, DaveFoster110@hotmail.com, DaveRusin, David Eppstein, DavidCBryant, DavidHouse, Dfeuer, Dml (usurped), Doctormatt, Doomed Rasher, Dysprosia, Dzordzm, EEMIV, Edsanville, Eequor, Egg, Ekaratsuba, EmilJ, Eric Kvaalen, Eric Olson, Fangz, FocalPoint, Fqqf, Fredrik, GTBacchus, Gandalf61, Gauge, Gauss, Gene Ward Smith, Georg Muntingh, Giftlite, Graham87, Haham hanuka, Hashar, He Who Is, Henning Makholm, Herbee, Hongooi, Horndude77, Hu, Ixfd64, JCSantos, JDPhD, Janek Kozicki, Jeppesn, JerroldPease-Atlanta, Jim.belk, JimmyPhysics, Jimothy 46, Jitse Niesen, Jleedev, Joachim Selke, JohnDavies, JonMcLoone, Jordi Burguet Castell, Josh Grosse, Joth, Jsondow, Julian Brown, KapilTagore, Karl-H, Karl-Henner, Keenan Pepper, Kier07, KittyKAY4, Lambiam, Ledrug, Liamdaly620, Light current, Linas, LittleDan, MathMartin, Matteo s, Mecanismo, Melchoir, Mfiorentino, Michael Hardy, Mirv, Mkehrt, Mon4, Mondkoncepto, Mpatel, Mssgill, Myriad, Nageh, Ncik, NewtonEin, Nuityens, Numerao, Oleg Alexandrov, Oshanker, Overlook1977, Phil Boswell, Pko, Plastikspork, Plato, Portalian, Pred, Protious, Pt, Pythagoras0, Qwfp, R.e.b., RMFan1, Revolver, Rhythm, Risk one, Rjanag, Rjwilmsi, Roadrunner, RobHar, Romanm, Rumping, SF007, Saga City, Sandrobt, Scythe33, Semistablesystem, Shadowjams, Shikaku13, Silly rabbit, Sligocki, Societelibre, Spiff, Sreds, Stux, Sverdrup, Sławomir Biały, TakuyaMurata, That Guy, From That Show!, The Anome, Thehotelambush, Thincat, Timwi, Tobias Bergemann, Tomchiukc, Vagodin, Vanish2, Vanished User 0001, Ventura, Virginia-American, Voorlandt, Vyznev Xnebara, Wakimball, William Ackerman, Winen, Wtmitchell, Wtuvell, XJamRastafire, Xaos, Xeno onex, Yecril, Yoctobarryc, Zaslav, Zundark, 174 anonymous edits

Balanced prime *Source*: http://en.wikipedia.org/w/index.php?oldid=328879516 *Contributors*: Anton Mravcek, CRGreathouse, Cristiano Toàn, Giftlite, Iffy, Matt Ryall, Matt me, Michael Hardy, N4nojohn, Numerao, PrimeFan, PrimeHunter, Rand0m011, Supernumerator, Tango, Whiteknox, Yulinwu, 4 anonymous edits

Bell number *Source*: http://en.wikipedia.org/w/index.php?oldid=396535732 *Contributors*: Amikake3, Ams80, AnonMoos, Betacommand, CBM, CRGreathouse, Charles Matthews, D6, David Eppstein, Dcoetzee, Dr. Universe, Druseltal2005, Eequor, F3et, Fredrik, Futurebird, Gian-2, Giftlite, Herbee, Ixionid, Jeffersonian123, Jks, Linas, Man pl, Maxal, Michael Hardy, Mirv, Numerao, Patrick, Pmanderson, PrimeHunter, Pyrop, R. J. Mathar, Rar, Remember the dot, Rich Farmbrough, Robinh, Salix alba, Samboy, Small potato, Texture, Tokenzero, Umeboshi, Wshun, Wzwz, XJamRastafire, Xanthoxyl, Zero0000, 43 anonymous edits

Carol number *Source*: http://en.wikipedia.org/w/index.php?oldid=392807961 *Contributors*: AgentPeppermint, Anton Mravcek, Astaroth628, B.Wind, Caribjustice, DataWraith, David Eppstein, Duncharris, Gandalf61, Giftlite, JackofOz, Jitse Niesen, Krenon, Mholland, N4nojohn, Numerao, OwenX, Pgk, PrimeFan, PrimeHunter, Richfife, Robertd, SoWhy, Tango, Updatehelper, 13 anonymous edits

Centered decagonal number *Source*: http://en.wikipedia.org/w/index.php?oldid=380641762 *Contributors*: Giftlite, Kammat, Merovingian, Mhaitham.shammaa, PrimeFan, PrimeHunter, Radiant!, Rocchini, Shyam, ZeroOne, 2 anonymous edits

Centered heptagonal number *Source*: http://en.wikipedia.org/w/index.php?oldid=268674964 *Contributors*: Charles Matthews, CompositeFan, GTBacchus, Giftlite, Herbee, Maksim-e, Mhaitham.shammaa, PrimeFan, Spooky, 白駒, 4 anonymous edits

Centered square number *Source*: http://en.wikipedia.org/w/index.php?oldid=403980111 *Contributors*: Anton Mravcek, Arbol01, Burn, FrozenPurpleCube, Georgia guy, Giftlite, Hadal, Henrygb, Ilmari Karonen, Karl Palmen, Linas, Maksim-e, Mhaitham.shammaa, Michael Hardy, Oleg Alexandrov, Patrick, PrimeFan, PrimeHunter, RSido, RobHar, Shyam, Sverdrup, Tabletop, Tedernst, 13 anonymous edits

Centered triangular number *Source*: http://en.wikipedia.org/w/index.php?oldid=249071700 *Contributors*: Anton Mravcek, Burn, David Andel, Eequor, FvdP, Giftlite, Hotdogjuicer, Karl Palmen, Kmhkmh, Mhaitham.shammaa, Nekura, Oleg Alexandrov, PrimeFan, PrimeHunter, Tabletop, WikiSlasher, 4 anonymous edits

Chen prime *Source*: http://en.wikipedia.org/w/index.php?oldid=398946553 *Contributors*: Anton Mravcek, Arbol01, Army1987, Arthur Rubin, BL14387, Backslash Forwardslash, Betacommand, CRGreathouse, Caturdayz, CompositeFan, DYLAN LENNON, David Eppstein, Elroch, Fak119, Giftlite, GregorB, Heder, Hv, Jacob grace, JamesBWatson, Jsondow, KOROSHI, LaForge, Liangent, Magioladitis, Matchups, Mendaliv, N4nojohn, Nburden, Neptune5000, Oleg Alexandrov, Pmanderson, PrimeFan, PrimeHunter, Schneelocke, Silverfish, Toshio Yamaguchi, WAREL, WATARU, Welsh, XJamRastafire, 33 anonymous edits

Circular prime *Source*: http://en.wikipedia.org/w/index.php?oldid=408716509 *Contributors*: Asmeurer, Julzes, Michael Hardy, PrimeHunter, Quickfoot, R0mai Exception, Toshio Yamaguchi

Cousin prime *Source*: http://en.wikipedia.org/w/index.php?oldid=387011351 *Contributors*: Anton Mravcek, CRGreathouse, Dmharvey, Dysprosia, Giftlite, Herbee, KenJDavis, Kimhyk, Linas, Maksim-e, Michael Hardy, PrimeHunter, Schneelocke, StoicalSoul, WAREL, 1 anonymous edits

Cuban prime *Source*: http://en.wikipedia.org/w/index.php?oldid=307850506 *Contributors*: 4pq1injbok, Army1987, CRGreathouse, Giftlite, MathImagics, Murtasa, Oleg Alexandrov, PrimeFan, PrimeHunter, Schneelocke, Shell Kinney, Stdazi, Tyomitch, XJamRastafire, 5 anonymous edits

Cullen number *Source*: http://en.wikipedia.org/w/index.php?oldid=403576462 *Contributors*: Adcoon, Bender235, Burn, Dedalus, Eric119, Falcon8765, Fredrik, Giftlite, GraemeMcRae, Herbee, Jnestorius, Maxal, Personline, Peter Kwok, PrimeHunter, Reyk, Schneelocke, Sir Dagon, Tbhotch, Thomassteinke, Vanish2, XJamRastafire, 11 anonymous edits

Dihedral prime *Source*: http://en.wikipedia.org/w/index.php?oldid=333253125 *Contributors*: BadWeather, CRGreathouse, David Eppstein, Giftlite, PrimeFan, PrimeHunter, Reinyday, Smjg, 1 anonymous edits

Dirichlet's theorem on arithmetic progressions *Source*: http://en.wikipedia.org/w/index.php?oldid=386789312 *Contributors*: Akriasas, Andy Smith, Arthur Rubin, AxelBoldt, Ayacop, Bender235, BeteNoir, Brion VIBBER, CRGreathouse, Charles Matthews, Chocolateboy, DYLAN LENNON, David Eppstein, Giftlite, Hanche, Hwttdz, IKIZAMA, JackSchmidt, Japanese Searobin, Jcobb, Jshadias, KittySaturn, Kwertii, Lhf, Looxix, MSGJ, Madmath789, Michael Hardy, Myasuda, Nk, Nono64, Oleg Alexandrov, Pleasantville, PrimeHunter, RobHar, Srbauer, TakuyaMurata, The goober, Tosha, Vanish2, XJamRastafire, Zundark, קאלדנב הנוי, 14 anonymous edits

Double factorial *Source*: http://en.wikipedia.org/w/index.php?oldid=110248189 *Contributors*: A. Pichler, Acer, Agricola44, Ahoerstemeier, Alexandre Vassalotti, Alparmarta, Altenmann, Andres, Anonymous Dissident, Anton Mravcek, Arabic Pilot, ArglebargleIV, Arneth, ArnoldReinhold, Arphibagon, Aruton, Audiovideo, Autopilot, AxelBoldt, Bdesham, Ben pcc, Blahm, Boltsman, Booyabazooka, BruceHodge, Bryan H Bell, Bubba73, Burgercat, CRGreathouse, Capitalist, Carlosguitar, CheekierMonkey, Chrispringle, Christian List, Ckatz, Colonies Chris, Connelly, Conversion script, Curlytop999, Darkmeerkat, David Eppstein, Db099221, Dcluett, Dcoetzee, Deathphoenix, Denelson83, Dhp1080, Dmcq, Dogah, Dominus, Domitori, Dragohunter, Dude1818, Dysprosia, Ec-, EdC, Emperorbma, Eras-mus, Eric119, Eridani, Ernest lk lam, Eumeme, Eutactic, Evil Monkey, Excirial, FallenAngel, FatalError, Fibonacci, Fishcorn, Fredericksgary, Fredrik, Frencheigh, Fritzpoll, Furrykef, Garoto burns, GeneralCheese, Gesslein, Giftlite, Glenn L, Godden46, Goldencako, Google Child, Gruntler, H3llbringer, Haein45, Hairy Dude, Hannes Eder, Happy-melon, Hassan210360, Henrygb, Herbee, Hyacinth, Iamunknown, Icek, Idbelange, ImperatorExercitus, Indeed123, IronGargoyle, Isopropyl, Ixfd64, JB82, JWSchmidt, JabberWok, Jagun, JebeddiahSpringfield, Jezzabr, Jgoulden, Jiel.B, Jim.belk, Jleedev, JohnBlackburne, Jonathunder, Jonik, Jordaan12, Jumbuck, Justin W Smith, Jwmcleod, Kaimiddleton, Karl Palmen, Kbrose, Keith111, Keithcc, Kevin Baas, Kier07, King Bee, Knutux, Koolman2, Korax1214, Lambiam, Lantonov, Lhf, MSGJ, Marc van Leeuwen, MarkSweep, Marquez, Mathacw, MattGiuca, Mattbuck, Matusz, Maximaximax, Mboverload, McKay, Mech Aaron, MegaSloth, Melchoir, Mets501, Michael Hardy, Michael Slone, Minesweeper, Misof, Mktos532, MoleculeUpload, Mon4, MrOllie, Mradam2008, Mrbowtie, Ms2ger, Nabla, Namaxwell, Necrid Master, NeonMerlin, NerdyScienceDude, Nicolas.Wu, Nikai, Nishantsah, Nitrolicious, Nitrxgen, Nniigeell, Nomet, Num Ref, Obradovic Goran, Octahedron80, Oldjackson, Oleg Alexandrov, PAR, Patrick, Paul August, Paul Niquette, Pde, Pek the Penguin, Piano non troppo, Pilover819, Pleasantville, Poor Yorick, Prari, PrimeFan, PrimeHunter, Qonnec, Quantling, Quaoar, Quest for Truth, Qwerty mac13, RaitisMath, Rhythm, Rich Farmbrough, Rob.derosa, Robo37, SGBailey, Sabbut, Salix alba, Saraghav, Schneelocke, Seb-Gibbs, Shawnhath, Shimgray, Silsor, Slady, Spyswimmer33, Stevenj, Stevey7788, Stuart Morrow, Super Spider, Super-Magician, Sushi Tax, Sverdrup, Svick, Swpb, THEN WHO WAS PHONE?, TXiKi, TakuyaMurata, Taxman, Tels, Thatoneguy, The Perfection, The Thing That Should Not Be, TheArcher, Thingg, ThinkEnemies, Tim1988, TomViza, Tommy2010, Tomruen, Trusilver, Usien6, Vorratt, Vvargoal, WFPM, Waggers, Wholmestu, Whywhenwhohow, Wik, Wile E. Heresiarch, Wirkstoff, Wperdue, WriterHound, Wrs1864, XJamRastafire, Xario, Xenoglossophobe, Yamamoto Ichiro, Yarvin, Youandme, ZICO, Zaslav, Zundark, Zzedar, Zzyzx11, Ævar Arnfjörð Bjarmason, יש דוד, 446 anonymous edits

Double Mersenne prime *Source*: http://en.wikipedia.org/w/index.php?oldid=259749579 *Contributors*: Anonymouspp, Bender235, CRGreathouse, David Eppstein, Georgia guy, Giftlite, Ixfd64, Jerzy, Justin W Smith, Leavemsg2, Linas, Maksim-e, MarSch, Maxal, Mholland, Oleg Alexandrov, Pakaran, PhiEaglesfan712, PrimeHunter, Pt, Rich Farmbrough, Ryan Cable, Scythe33, Silverfish, XJamRastafire, Zundark, 27 anonymous edits

Eisenstein prime *Source*: http://en.wikipedia.org/w/index.php?oldid=389654779 *Contributors*: 4pq1injbok, Alphabetathre3, Anton Mravcek, Bender235, CRGreathouse, Charles Matthews, Dugwiki, Fayenatic london, Fropuff, Giftlite, KnightRider, Knodeltheory, Ncik, OwenX, Pmanderson, PrimeFan, PrimeHunter, Supernumerator, WISo, WLior, 2 anonymous edits

Emirp *Source*: http://en.wikipedia.org/w/index.php?oldid=344854432 *Contributors*: Blotwell, CRGreathouse, Doctormatt, FrankTobia, Func, Giftlite, GregorB, Kaluppollo, Magnus Manske, Miaow Miaow, Michaelkourlas, Oleg Alexandrov, PV=nRT, PrimeHunter, Sikilai, Silverfish, Whitepaw, XJamRastafire, 18 anonymous edits

Euclid number *Source*: http://en.wikipedia.org/w/index.php?oldid=396802420 *Contributors*: Buenasdiaz, CRGreathouse, Cherry blossom tree, CompositeFan, Doctormatt, Giftlite, JPD, Jasonwu1197, Lambiam, Linas, MarSch, Michael Hardy, Nsaa, Oleg Alexandrov, Pearle, PrimeHunter, RJFJR, Reetep, Rugi, Satori, Scythe33, Timothy Clemans, VidGa, XJamRastafire, 28 anonymous edits

Even number *Source*: http://en.wikipedia.org/w/index.php?oldid=161012870 *Contributors*: .:Ajvol:., Afed, Ahoerstemeier, Angela, Angr, Arthur Rubin, AxelBoldt, Beowulf7120, BiT, Blotwell, Bm128, Brick Thrower, CRGreathouse, Calcyman, Charles Matthews, Cheeser1, ChemGardener, Chenxlee, Col tom, DGMorales, DRLB, David Eppstein, Demmy, Ellywa, Falsedef, Fishnet37222, GeordieMcBain, Gesslein, Giftlite, Gregwmay, HeikoEvermann, Henrygb, Iseeaboar, IslandHopper973, Ixfd64, JForget, Jhinman, Jonathan Webley, Josh Parris, Jshadias, Jumbuck, Justin W Smith, Kelisi, Kewp, Kpufferfish, LimoWreck, Linas, Logan, Lotans, Lucinos, MDCollins, MER-C, MK8, MacMed, Magister Mathematicae, Marc Venot, Maxal, Mcqxx, Melchoir, Mellum, Mets501, Mfc, Michael Angelkovich, Michael Hardy, Minesweeper, Mormegil, N2e, Nuno Tavares, Nuttycoconut, Oddity-, Oleg Alexandrov, Oliver Pereira, Oxymoron83, Paquitotrek, PhotoBox, PierreAbbat, Poor Yorick, Potatoswatter, Rhopkins8, Rhythm, Rodriguesds, Romanm, Rpresser, Ryulong, Salix alba, Snowdog, Starwiz, Stwalkerster, Synchronism, TXiKi, TakuyaMurata, Thaurisil, The Anome, The enemies of god, Thetorpedodog, Toby Bartels, Trainman jaime, Twri, Usien6, Vegaswikian, VictorAnyakin, Wbrenna36, Xario, Xcentaur, Zaslav, 175 anonymous edits

Factorial prime *Source*: http://en.wikipedia.org/w/index.php?oldid=402481040 *Contributors*: Angela, Burn, CRGreathouse, Dude1818, Eequor, Eje211, Fredrik, Giftlite, Hede2000, Ixfd64, Kieff, Koppapa, Linas, MIT Trekkie, Marc van Leeuwen, Michael Hardy, Nnh, PrimeFan, PrimeHunter, Robo37, Silverfish, Sl, TarSix, Utcursch, WikiGrrrl, YGingras, 8 anonymous edits

Fermat number *Source*: http://en.wikipedia.org/w/index.php?oldid=405687186 *Contributors*: A legend, Alpertron, Altenmann, Angela, AnthonyQBachler, Armanobalassi, Arthena, Asmeurer, AxelBoldt, Bender235, Blugill, Brim, Burn, CRGreathouse, Charles Matthews, Coolkid70, Cristiano Toàn, DSachan, David Eppstein, Derlay, Doctormatt, ESkog, Egil, EmilJ, Eric119, Etudiant, Fredrik, Georgia guy, Gfis, Giftlite, GraemeMcRae, GregorB, Gubbubu, Heatherpeather, Herbee, Hgrosser, Ideyal, Integralolrivative, Ixfd64, JaGa, Jaerik, Janek37, Jerzy, JidGom, John Reid, Jossi, Katsushi, Kompik, Kprateek88, Lipedia, Luokehao, Markhurd, Matikkapoika, Mav, Maxal, Mccrotch, Messagetolove, Mhaitham.shammaa, Michael Hardy, Moreschi, Motomuku, Mzamora2, N Shar, Obscurans, PFHLai, Pablo-flores, PhiEaglesfan712, Pmanderson, Portalian, PrimeHunter, Pwlfong, Qutezuce, RTC, Rajula, Rdawson, Redgolpe, Reedy, Rettetast, Revolver, Reyk, Rich Farmbrough, Richard L. Peterson, Robroot, Sabbut, Samuelsen, Shadowoftime, Shreevatsa, Soap, Spewin, Stochata, Stux, SunCreator, TELL ME that, Tarquin, The Anome, TheScurvyEye, Toph 1729, Unyoyega, Vanish2, Visionsofyou, Waltersimons, WojciechSwiderski, Wshun, XJamRastafire, ZICO, Zundark, 127 anonymous edits

Fibonacci prime *Source*: http://en.wikipedia.org/w/index.php?oldid=407945425 *Contributors*: Anton Mravcek, Bender235, CBM, CRGreathouse, Charles Matthews, Dcoetzee, Divineprime, Esprit15d, Fedor Chelnokov, Fredrik, Gandalf61, Gfis, Giftlite, GraemeMcRae, Ixfd64, Ligulem, Linas, Moyet, OverlordQ, Palica, PrimeFan, PrimeHunter, Raoul NK, Reyk, Robomojo, Ronhjones, Silverfish, Singularity, Smjg, Tanner Swett, UnitedStatesian, 20 anonymous edits

Fortunate prime *Source*: http://en.wikipedia.org/w/index.php?oldid=259739735 *Contributors*: Anton Mravcek, CRGreathouse, Chris19910, CompositeFan, David Eppstein, Giftlite, GraemeMcRae, Intersofia, Leontolstoy2, Manticore, Michael Hardy, Oleg Alexandrov, PrimeFan, PrimeHunter, 5 anonymous edits

Full reptend prime *Source*: http://en.wikipedia.org/w/index.php?oldid=306356791 *Contributors*: A math-wiki, Anton Mravcek, CRGreathouse, Charles Matthews, Eli the Bearded, Giftlite, Luokehao, Murfas, Numerao, PrimeFan, PrimeHunter, Supernumerator, 5 anonymous edits

Gaussian integer *Source*: http://en.wikipedia.org/w/index.php?oldid=402447427 *Contributors*: Albmont, Altenmann, AxelBoldt, Burn, CRGreathouse, Charles Matthews, Color40, Crocogator, Daran, DavidHouse, Dmharvey, Dogah, Dominus, Dranorter, Dysprosia, Fafredverda, Fredrik, Giftlite, GromXXVII, Herbee, JoergenB, Joriki, KHamsun, Karl E. V. Palmen, Knodeltheory, Kompik, LGB, Lave, Linas, Macrakis, Madmath789, Majopius, Maksim-e, Michael Hardy, Mschlindwein, Msh210, NawlinWiki, Ntmatter, Numbo3, PierreAbbat, R. J. Mathar, Rjwilmsi, Run54, Salvatore Ingala, Scythe33, Setitup, TakuyaMurata, Teapeat, Telewatho, Tiphareth, Truejackster, Virginia-American, Wmahan, XJamRastafire, Zundark, יבצ לאינ, 40 anonymous edits

Genocchi number *Source*: http://en.wikipedia.org/w/index.php?oldid=336890372 *Contributors*: Almit39, Charles Matthews, Gandalf61, Giftlite, Kilom691, Michael Hardy, Reyk

Goldbach's conjecture *Source*: http://en.wikipedia.org/w/index.php?oldid=408343683 *Contributors*: 171.64.38.xxx, 212.130.12.xxx, A. S. Aulakh, AND198724764, Ac44ck, Adpete, Ahoerstemeier, Alfrodull, Andrew Robertson, AndrewWTaylor, ArglebargleIV, Aswarp, AxelBoldt, AzaToth, Azuredu, Ben-Zin, Benbovee, Bender235, Billymac00, Bogdangiusca, Bollinger, Borgx, CRGreathouse, Caleb Rookwood, Charles Matthews, Chinmin, Chocolateboy, Cngoulimis, Cole Kitchen, Conversion script, Corvus cornix, Cícero, DAJF, DJ Clayworth, DStoykov, DYLAN LENNON, Daveblack, David Eppstein, David Haslam, DavidCary, DavidWBrooks, Dbenbenn, Dcoetzee, Derek Ross, Dfeuer, Digby Tantrum, DiscoStuMan, Doug, Drmies, Dtrebbien, Duke Dudley, Dysprosia, EddEdmondson, Elektron, Epbr123, Esb, Excirial, Exteray, Eyebum, Fadereu, Funky Fantom, Furrykef, Gadoev, Gail, Gandalf61, Gareth Owen, GaryW, GeeZee, Gene Ward Smith, Giftlite, Ginsengbomb, Goatasaur, GraemeMcRae, Graham87, GregorB, Gslin, Gulliveig, Gurch, Gzornenplatz, HaboFreakNumber2, Haham hanuka, Helohe, Herbee, Histrion, Ianmacm, Ideyal, Imran, Indon, Isaacl, J.delanoy, JAF1970, JackSchmidt, JamesBWatson, Jamesedwardsmith, Jed 20012, Jeffq, Jkelly, JoshuaZ, Jrtayloriv, Jushi, Justin W Smith, Karam.Anthony.K, Karl-Henner, Keenan Pepper, Keith Edkins, Kieff, Klaus, Kope, Korg, Lambiam, Lowellian, Luqui, Lykantrop, MSGJ, Magioladitis, Maniac18, MarkSweep, MarnetteD, Marquez, MathMan64, Mcsee, Michael Hardy, Mintguy, Mon4, Motomuku, Mrityunjay tripathi, Mstftsm, Mwalimu59, NatusRoma, NewEnglandYankee, Nobrook, Noosfractal, NubKnacker, Oboeboy, Oldiexian, Oleg Alexandrov, Olin, Olivier, Onorem, OwenX, PageWizard, Pakaran, Paul August, PaulTaylor, Peruvianllama, PhiEaglesfan712, Philip Trueman, Pigsonthewing, Plaudite, Pleasantville, Pmanderson, Pony99CA, Porcher, Positronium, Pred, Premeditated Chaos, PrimeFan, PrimeHunter, Pt, Python eggs, Qdxinyu, Ravi12346, Rbarreira, Reddish, Reinyday, Robertpadian, Rotem Dan, Roviury, Rydel, Sabbut, Sander123, Santyno, Sgeo, Shaunwhim2, Simplicityinstinct, Sir Isaac, Sligocki, Smurrayinchester, Snoyes, Someonefrommars, Soulouri, Spireguy, Ssimsekler, StaticGull, Steamroller Assault, Stefan64, Stevenoostdijk, Superm401, Surv1v4l1st, Susvolans, Sverdrup, Swarm, Syndrome, THEN WHO WAS PHONE?, Tarquin, Teorth, TeunSpaans, The Anome, The JPS, The Rogue Penguin, Thevelho, Tosha, Triksox, Uncia, Vcelloho, Victor Scientist, Viriditas, Vreddy92, Wapcaplet, Wclark, Wereon, Whodunit, Wile E. Heresiarch, WriterHound, Wzhao553, XJamRastafire, Yacht, Youandme, Yulracso, Zander, 284 anonymous edits

Good prime *Source*: http://en.wikipedia.org/w/index.php?oldid=375514347 *Contributors*: Evatutin, PrimeHunter, Reinyday, 2 anonymous edits

Happy number *Source*: http://en.wikipedia.org/w/index.php?oldid=403522912 *Contributors*: 4meter4, A Real Kaiser, A.R., ACredibleLie, Acm, Adishem, Ahugenerd, Ajd, Alasdair, Angmering, AppleMacReporter, Basketballtim, Beano, BinaryFrog, Blotwell, Bubba73, CRGreathouse, ColinHorne, Cristiano Toàn, Darksun, DataWraith, DavidWBrooks, Dbenbenn, Dhartung, Doctormatt, Dogah, Dysprosia, Emurphy42, Er Komandante, Evatutin, Evilmoo, Fmansfeld, FrostyBytes, Gabrielbijleveld, Giftlite, Hohum, Hughcharlesparker, Hypnosadist, Ian Pitchford, Ismakefire, JYi, Justin W Smith, KeithS, Kelly Martin, LPH, Linas, Lucas Brown, MFH, MarkSweep, MathMan64, Matt.whitby, Melchoir, Mgenuth, Moe1234567890000, Mrmrbeaniepiece, Murkee, Mytchill, Nealmcb, Oleg Alexandrov, Oliphaunt, OwenX, Peak Freak, Pearle, PhiJ, Philip Trueman, Phoenix79, Pichu826, Pmanderson, PrimeHunter, R. S. Shaw, R27182818,

Radon210, Rick21784, Rikimaru, Serein (renamed because of SUL), Silverfish, Smjg, Snorbaard, Squad51, Stephenb, TJ09, TWSummer, Telemath, Thehelpfulone, TonyW, Waldir, Wikipeterproject, XJamRastafire, Zaslav, ZeroOne, 141 anonymous edits

Higgs prime *Source*: http://en.wikipedia.org/w/index.php?oldid=195278181 *Contributors*: Alakniranjan, CRGreathouse, Michael Hardy, PrimeFan, PrimeHunter, XJamRastafire, 1 anonymous edits

Highly cototient number *Source*: http://en.wikipedia.org/w/index.php?oldid=277395549 *Contributors*: Am2t, Anonymous Dissident, Anton Mravcek, Bubba73, Charles Matthews, Frencheigh, Giftlite, Gurch, Linas, Loud neighbors, NBS525, Oleg Alexandrov, Pne, PrimeFan, PrimeHunter, Reinyday, ST47, Silverfish, 2 anonymous edits

Illegal prime *Source*: http://en.wikipedia.org/w/index.php?oldid=393621069 *Contributors*: .mau., 1812ahill, 4pq1injbok, Alansohn, Angela, Ansell, ArnoldReinhold, Arvindn, Bdesham, Bobblewik, CBM, CRGreathouse, Cerejota, Chris Wood, Cyde, DMacks, Danski14, Dantheman531, David Gerard, DavidWBrooks, Denelson83, Dreftymac, Dtobias, Dweller, ESkog, Easyas12c, Ed g2s, Eldacan, Eloquence, Epeefleche, Favonian, Frencheigh, Giftlite, GregorB, Head, Heron, Iffy, Imjustmatthew, JWSchmidt, Jdavidb, Jengod, Kylemcinnes, Lupin, MarSch, Math1337, Matt Crypto, MeltBanana, Michiexile, Miserlou, Misza13, Moep, Natalie Erin, Pathoschild, Penwhale, Phlip, PrimeHunter, Psychonaut, Puckly, Quadell, Radagast83, Raggmopp614, Realchallange, Reinyday, Rich Farmbrough, RobertG, Schneelocke, Sfacets, Shaddack, Shogun, SirSam972, Smyth, Snowynight, Thumperward, Tijfo098, Tingrin87, Tregoweth, TreyHarris, Tripps, Tritium6, Trivialist, Unloud, VeryVerily, W guice, Wapcaplet, Washod, WikiSlasher, Ww, 69 anonymous edits

Irregular prime *Source*: http://en.wikipedia.org/w/index.php?oldid=259751284 *Contributors*: Boemanneke, CRGreathouse, Charles Matthews, Cristiano Toàn, Cybercobra, DRLB, David Shay, Fredrik, Giftlite, Gwaihir, Henrygb, Herbee, Iffy, LilHelpa, MathMartin, Peter Kwok, Pouya, PrimeFan, PrimeHunter, R.e.b., Reyk, RobHar, Safek, Schneelocke, Throwawayhack, Vanish2, XJamRastafire, 10 anonymous edits

Kynea number *Source*: http://en.wikipedia.org/w/index.php?oldid=364314597 *Contributors*: Anton Mravcek, Charles Matthews, David Eppstein, Giftlite, GregorB, Jitse Niesen, Nico92400, PrimeFan, PrimeHunter, Reinyday, Rich Farmbrough, Rjwilmsi, Sjorford, 6 anonymous edits

Leyland number *Source*: http://en.wikipedia.org/w/index.php?oldid=402685572 *Contributors*: Carl Turner, David Eppstein, Doctormatt, Droog Andrey, Giftlite, Infrangible, Insider, Katharineamy, PrimeFan, PrimeHunter, Rich Farmbrough, WolfWings, 6 anonymous edits

List of prime numbers *Source*: http://en.wikipedia.org/w/index.php?oldid=408702306 *Contributors*: 2D, 4pq1injbok, 97rs24, 99of9, AdjustShift, Alansohn, Alex12 3, Alexius08, Ali K, Alpha Quadrant (alt), Amorim Parga, Anaxial, Andrushkkutza, Angela, AnthonyQBachler, Anton Mravcek, Arakunem, Arcfrk, ArglebargleIV, Arhughes, Asmeurer, Atif.t2, AtiwH, Banaticus, Barneca, Bduke, Bender235, Bento00, Billymac00, Bizza4Prezident, Bobbu9876, Boing! said Zebedee, BoomerAB, Brighterorange, CBM, CRGreathouse, Calmypal, Calton, Calvin 1998, Chardish, Chinni26, Christophenstein, Chuunen Baka, Cje, Closedmouth, CompositeFan, Connormah, Craig Mayhew, Cyclonenim, D8880, Daqu, Darkfelinanova, Darth Panda, Dawn Bard, Deadcorpse, Delicious carbuncle, Deor, DerHexer, Dmitri Yuriev, Doctormatt, Docu, Download, DragonflySixtyseven, Drmies, Duncancumming, Easyas12c, Echuck215, Egmontaz, Ehheh, Elassint, Epbr123, Evatutin, Favonian, Fennec, Flagboy, Frank Lofaro Jr., Fredrik, Fyyer, Garkbit, Gazimoff, Gfoley4, Giftlite, Gjd001, Glane23, Glass Sword, Goudzovski, Gowrb05, Gtstricky, HJ Mitchell, HalfShadow, Happypal, Helder.wiki, HexaChord, Hubertsimson, Hv, Icarus3, Igoldste, Inferno, Lord of Penguins, Ixfd64, J-t-m, J.delanoy, JackofOz, JamesAM, Jamesday, Jhalkompwdr, Jj137, JustUser, Jwissick, Jwoodger, Jwrosenzweig, K1Bond007, KFP, Kartano, KerryVeenstra, Kevinkor2, Kingturtle, Kiore, Kjoonlee, Kopaka649, Kotiwalo, Kristen Eriksen, Leafyplant, Leatherbelly, LeaveSleaves, Linas, Ljr180, Lowellian, Luk, Luna Santin, M00npirate, MATThematical, Magister Mathematicae, Marek69, MarkSutton, Martin451, Maxime.Debosschere, Melissa.holtcamp, Mets501, Michael Hardy, Mike Rosoft, MikeLynch, Mini-Geek, MrOllie, MrWikiMiki, My76Strat, Mygerardromance, NTK, Nakon, Nateguimondart, Nico92400, NuclearWarfare, Numerao, Odie5533, Omerfc1, Onevalefan, Orange Suede Sofa, Oscarfan, Owen, OwenX, PL290, Paul-L, Pdcook, Petiatil, Phantomsteve, PhiEaglesfan712, Piano non troppo, Pinethicket, Pizza1512, Portalian, Poulpy, PrimeFan, PrimeHunter, Psylocibe, Quirkasaurus, QuirkyQuark, Qxz, R. J. Mathar, RJaguar3, Radagast3, Radiant!, RadicalPi, Recognizance, Reconsider the static, Redgolpe, Redrocketboy, Reinyday, Res2216firestar, RexNL, Rgrg, Rich.lewis, Rickterp, RobertG, Roentgenium111, Romanm, RoyBoy, RxS, Ryan Postlethwaite, SC979, SGBailey, Salvio giuliano, SchfiftyThree, Seth Ilys, Shyam, Skalman, Skralg, Slord, Smjg, SpLoT, Spiritia, Splodgenry, Stay Dead, Stickee, Struds, Suffusion of Yellow, Texas44, The Cave Troll, The Thing That Should Not Be, TheRealFennShysa, Tide rolls, Timrem, Tompagenet, Trusilver, Two2Naach, Tyomitch, Ulric1313, UnitedStatesian, Us441, UserDoe, Veinor, Vlad4599, Waldir, WatermelonPotion, WikHead, WikiDao, Wroscel, Xmlizer, Zoicon5, Zzuuzz, לובי לב, 820 anonymous edits

Lucas number *Source*: http://en.wikipedia.org/w/index.php?oldid=405987823 *Contributors*: Andy M. Wang, Anton Mravcek, Arbol01, BL Lacertae, Blackskilled, CRGreathouse, Carrionluggage, Charles Matthews, Danielklein, Dina, DiscX, Fantusta, Fredrik, Fropuff, Gaius Cornelius, Gandalf61, GatesPlusPlus, Giftlite, Insanity Incarnate, J04n, JRSpriggs, Jed 20012, Kanguole, Maxal, Mikez23, Netsnipe, Nffy212, PV=nRT, Patrick, Plenilune, PrimeHunter, Razorflame, Sawbeit, Shadowx88, Sligocki, Stux, Vijilant, Wasell, Wik, Wild Lion, Wutchamacallit27, Xiutwel, ZeroOne, 33 anonymous edits

Lucky number *Source*: http://en.wikipedia.org/w/index.php?oldid=404494551 *Contributors*: Algebraist, Antonio Lopez, Arthur Rubin, Blotwell, Buck O'Nollege, CRGreathouse, CapitalSasha, Carlosguitar, Cawas, Celtic Minstrel, Computer97, DXL, Dominus, Dysprosia, Enochlau, Fredrik, Giftlite, Haham hanuka, Isnow, JerryFriedman, Jshadias, King Mir, Linas, Message From Xenu, Mr. Billion, Nakon, Ninetyone, Oleg Alexandrov, Olivier, Pleasantville, Pred, PrimeHunter, Rikimaru, Sbhuvans, Sottolacqua, Tanyakh, Tommy2010, Wtmitchell, XJamRastafire, 46 anonymous edits

Markov number *Source*: http://en.wikipedia.org/w/index.php?oldid=370861187 *Contributors*: Aaron Schulz, Anton Mravcek, Burn, Charles Matthews, Giftlite, Jitse Niesen, Knodeltheory, KurtSchwitters, Maxal, Michael Hardy, Pmanderson, PrimeFan, Silverfish, The DQN,macbeth, Timrem, XJamRastafire, 15 anonymous edits

Mersenne prime *Source*: http://en.wikipedia.org/w/index.php?oldid=402682917 *Contributors*: (, .:Ajvol:., 10metreh, Acroterion, Adamd1008, Alcuin, Alpha Beta Epsilon, Alpt, Andi47, Anomalocaris, AnonMoos, Anonymouspp, AnteaterZot, Arcfrk, Arthena, Arthur Rubin, Arvindn, Ashwath.rabindranath, AxelBoldt, Bawolff, Bcnelson, Bedivere, Bender235, Bensin, Berteun, Billymac00, Blackbird2150, Bobblewik, Borgx, Bryan Derksen, Bubba73, C.R.Selvakumar, CRGreathouse, CecilBlade, Chaosdruid, Christian List, Cimon Avaro, Ciphers, Cleroth, CobaltBlue, Conversion script, Cordell, Cstaffa, Cxxl, Dantheox, Derlay, Dissident, DropDeadGorgias, Duncan, Ekrumme, EmilJ, Eplant, Eric119, FancyMouse, Favonian, Fivemack, Fredrik, Fresheneesz, Fulvius, FvdP, Fæ, Gap9551, Gene Ward Smith, Georgia guy, Ghewgill, Giftlite, Glenn L, GngstrMNKY, Gowen, GraemeMcRae, Graham87, GregorB, Haham hanuka, Hakeem.gadi, Herbee, Heryu, Hut 8.5, IanOsgood, Ideyal, Intelati, Isarl, Ixfd64, JackofOz, Jao, Jarekadam, Jeff8765, Jennavecia, Jeronimo, JerryLaGrou, Jiang, Jmalc, Joblack, Johantheghost, Johnblythedobson, JoshuaZ, Jsvaidya, Jumbuck, Jushi, Karada, Kerry Lander, Kigali1, Kingoomieiii, Knutux, Lambiam, Landon Curt Noll, Laplacian, Linas, Loadmaster, Looxix, Lowellian, Lumidek, Lzur, Majestic27, Malcolm Farmer, MartinGugino, Materialscientist, Matsonb, Matt Kurz, Maxal, Meredyth, Michael Hardy, Mikez, Mini-Geek, Minipie8, Mormegil, Motomuku, N.Nahber, NickelKnowledge, NuclearWarfare, Numerao, Olivier, Optim, Otets, Pakaran, Pascal666, Pgan002, PhiEaglesfan712, Pilover819, Ponder, Pred, PrimeFan, PrimeHunter, PrometheusX303, Prumpf, Pt, Qutezuce, R00723r0, Radagast3, Ranjithsutari, Raryel, Rbonvall, Rbraunwa, Remote009, Res2216firestar, Rhnet, Rhythm, Rich Farmbrough, Richard L. Peterson, Robo37, Robomojo, Roentgenium111, Romanm, Ross Fraser, Rossami, Rziff, Sabbut, Salgueiro, Salix alba, Schneelocke, Shabda, Shanes, Shawnc, Shovonma17, Sohale, Sry85, SummerPhD, Tambora1815, Tarandeep1983, Tengai, The Anome, Tim Starling, Tirkfl, Tjfulopp, Tommy2010, Tooto, Toshio Yamaguchi, UU, Uncwilly, UtherSRG, VHF, Vic93, Vobis132, Watsonwatt, Wiwaxia, XJamRastafire, Yann, Zaphod Beeblebrox, Zigger, Zubaz, Zundark, 273 anonymous edits

Mills' constant *Source*: http://en.wikipedia.org/w/index.php?oldid=395373952 *Contributors*: Andypar, Asmeurer, CBM, CRGreathouse, Carifio24, Charles Matthews, Cy1387, David Eppstein, Dicklyon, Dogah, Gfis, Giftlite, Hannes Eder, Ixfd64, Kieff, Lowellian, Mike Rosoft, Oleg Alexandrov, Omnipaedista, PV=nRT, PrimeFan, PrimeHunter, RandomP, Reyk, Rich Farmbrough, Robo37, Tamfang, TeunSpaans, 16 anonymous edits

Minimal prime (recreational mathematics) *Source*: http://en.wikipedia.org/w/index.php?oldid=341529461 *Contributors*: 4pq1injbok, Arcfrk, CRGreathouse, CompositeFan, Giftlite, PrimeFan, PrimeHunter, Supernumerator

Motzkin number *Source*: http://en.wikipedia.org/w/index.php?oldid=358848883 *Contributors*: Bab dz, Cacycle, David Eppstein, Eequor, Fredrik, Giftlite, Holimion, JocK, Lantonov, Linas, Mhym, Michael Hardy, Numerao, OwenX, PrimeFan, PrimeHunter, Robertd, Schneelocke, Stephen B Streater, 6 anonymous edits

Newman–Shanks–Williams prime *Source*: http://en.wikipedia.org/w/index.php?oldid=378106260 *Contributors*: Anton Mravcek, Bender235, Burn, CRGreathouse, Dogah, Fredrik, FvdP, Gandalf61, Giftlite, Herbee, Jotomicron, Linas, Michael Hardy, PrimeFan, Reinyday, Rikimaru, Schneelocke, Supernumerator, Uncia, 5 anonymous edits

Odd number *Source*: http://en.wikipedia.org/w/index.php?oldid=161012912 *Contributors*: .:Ajvol:., Afed, Ahoerstemeier, Angela, Angr, Arthur Rubin, AxelBoldt, Beowulf7120, BiT, Blotwell, Bm128, Brick Thrower, CRGreathouse, Calcyman, Charles Matthews, Cheeser1, ChemGardener, Chenxlee, Col tom, DGMorales, DRLB, David Eppstein, Demmy, Ellywa, Falsedef, Fishnet37222, GeordieMcBain, Gesslein, Giftlite, Gregwmay, HeikoEvermann, Henrygb, Iseeaboar, IslandHopper973, Ixfd64, JForget, Jhinman, Jonathan Webley, Josh Parris, Jshadias, Jumbuck, Justin W Smith, Kelisi, Kewp, Kpufferfish, LimoWreck, Linas, Logan, Lotans, Lucinos, MDCollins, MER-C, MK8, MacMed, Magister Mathematicae, Marc Venot, Maxal, Mcqxx, Melchoir, Mellum, Mets501, Mfc, Michael Angelkovich, Michael Hardy, Minesweeper, Mormegil, N2e, Nuno Tavares, Nuttycoconut, Oddity-, Oleg Alexandrov, Oliver Pereira, Oxymoron83, Paquitotrek, PhotoBox, PierreAbbat, Poor Yorick, Potatoswatter, Rhopkins8, Rhythm, Rodriguesds, Romanm, Rpresser, Ryulong, Salix alba, Snowdog, Starwiz, Stwalkerster, Synchronism, TXiKi, TakuyaMurata, Thaurisil, The Anome, The enemies of god, Thetorpedodog, Toby Bartels, Trainman jaime, Twri, Usien6, Vegaswikian, VictorAnyakin, Wbrenna36, Xario, Xcentaur, Zaslav, 175 anonymous edits

Padovan sequence *Source*: http://en.wikipedia.org/w/index.php?oldid=389040662 *Contributors*: Amber388, Burn, CRGreathouse, Charles Matthews, Fnorp, FvdP, Gandalf61, Gentlemath, Gfis, Giftlite, Hyperdivision, Jtlien, Knodeltheory, Michael Hardy, Oleg Alexandrov, Plenilune, Pmanderson, PrimeFan, Txomin, 13 anonymous edits

Palindromic prime *Source*: http://en.wikipedia.org/w/index.php?oldid=393495860 *Contributors*: Angela, Arthur Rubin, Blotwell, CBM, CRGreathouse, Chasingsol, Computician, Dfarmer, Flamingantichimp, Gandalf61, Georgia guy, Giftlite, GraemeMcRae, GregorB, Herbee, Infovarius, Jayamohan, Johnmoyer, PV=nRT, PhiEaglesfan712, PrimeFan, PrimeHunter, Redgolpe, Reinyday, Reyk, Ronhjones, Schneelocke, Shell Kinney, Teratornis, XJamRastafire, 12 anonymous edits

Partition (number theory) *Source*: http://en.wikipedia.org/w/index.php?oldid=404257680 *Contributors*: 4pq1injbok, Almit39, Anomalocaris, Arch dude, Bluebusy, Burn, CRGreathouse, Charles Matthews, David Eppstein, El C, Eliasen, FractalFusion, GTBacchus, Gandalf61, Giftlite, GromXXVII, Hannes Eder, Henrygb, Hillman, HorsePunchKid, Ilmari Karonen, Ixfd64, JNLII, JRSpriggs, Jason Quinn, Jed 20012, JoaquinFerrero, Joriki, Justin W Smith, Jwmcleod, Kevin Forsyth, Khunglongcon, Kku, Krishnachandranvn, Lambiam, Lantonov, Linas, Loopology, Macrakis, Marc van Leeuwen, Mathman99, Maxal, Merovingian, Mhym, Miaers, Michael Hardy, Michael Slone, Milogardner, Nonenmac, Oleg Alexandrov, Philip Trueman, Phys, Pwlfong, Redgolpe, Richard L. Peterson, Robinh, Robo37, Shoeofdeath, Simetrical, Stevertigo, Tarquin, Tetracube, Thehebrewhammer, Timothy Clemans, Timrem, Wang ty87916, Wshun, Ylloh, Zdaugherty, מענובא, 白駒, 61 anonymous edits

Pell number *Source*: http://en.wikipedia.org/w/index.php?oldid=404206001 *Contributors*: Amikake3, Ask123, CRGreathouse, David Eppstein, Dbg144, Fountainofignorance, Fredrik, Gentlemath, Giftlite, Glenn L, Haseldon, Incnis Mrsi, Jacques Antoine, Jshadias, Michael Hardy, Mofo67, PV=nRT, Paul August, Pmanderson, Pomte, PrimeFan, PrimeHunter, Salvatore Ingala, Silverfish, Uncia, Varnesavant, YixilTesiphon, 14 anonymous edits

Permutable prime *Source*: http://en.wikipedia.org/w/index.php?oldid=399077043 *Contributors*: ABCD, Anban k, Anton Mravcek, Bojan Basic, CRGreathouse, Charles Matthews, Decagon, Giftlite, Michael Hardy, Oleg Alexandrov, PrimeFan, PrimeHunter, Reyk, Shell Kinney, Sohale, Uncia, 11 anonymous edits

Perrin number *Source*: http://en.wikipedia.org/w/index.php?oldid=402249507 *Contributors*: 4pq1injbok, Anton Mravcek, Burn, Charles Matthews, Daniel5Ko, David Eppstein, Eraserhead, Fivemack, Giftlite, J1729, Johnbibby, MarSch, Maxal, Mu, Oxnard27, PrimeHunter, Sjorford, Splee, 19 anonymous edits

Pierpont prime *Source*: http://en.wikipedia.org/w/index.php?oldid=349320580 *Contributors*: Anton Mravcek, Bender235, CRGreathouse, Charles Matthews, CompositeFan, Fivemack, Giftlite, Hv, Jitse Niesen, Michael Hardy, Numerao, Oleg Alexandrov, PrimeFan, PrimeHunter, Quuxplusone, Reyk, Sohale, Supernumerator, Walter Nissen, 6 anonymous edits

Pillai prime *Source*: http://en.wikipedia.org/w/index.php?oldid=388089162 *Contributors*: Anton Mravcek, Army1987, Bender235, CRGreathouse, CompositeFan, David Eppstein, Gandalf61, Giftlite, Numerao, PrimeFan, PrimeHunter, Sohale

Prime gap *Source*: http://en.wikipedia.org/w/index.php?oldid=396737746 *Contributors*: CRGreathouse, Charles Matthews, Chenxlee, DataWraith, EmilJ, Gap9551, Giftlite, Goldenart, Graham87, GregorB, Hairhorn, Jitse Niesen, Jsondow, Kope, Luokehao, Madmath789, Michael Hardy, Mon4, Octahedron80, Oleg Alexandrov, Olivemountain, PrimeHunter, Terra Xin, Timothy Clemans, XJamRastafire, 48 anonymous edits

Prime quadruplet *Source*: http://en.wikipedia.org/w/index.php?oldid=403883780 *Contributors*: Almit39, AnonUser, Anton Mravcek, Bedivere, CRGreathouse, DYLAN LENNON, Discospinster, Dougweller, DrScienceAstronaut, Epastore, Giftlite, Giggy, Gwaihir, Linas, Lzur, Matchups, Mwalimu59, Oleg Alexandrov, PhiEaglesfan712, PrimeFan, PrimeHunter, Rich Farmbrough, Scythe33, Sicherlich, 13 anonymous edits

Prime triplet *Source*: http://en.wikipedia.org/w/index.php?oldid=404665558 *Contributors*: Gandalf61, Giftlite, Lord of Illusions, MFH, Michael Hardy, PhiEaglesfan712, PrimeHunter, 白駒, 2 anonymous edits

Prime-counting function *Source*: http://en.wikipedia.org/w/index.php?oldid=406099511 *Contributors*: Abc135246, AbcXyz, Almit39, Alodyne, Arthur Rubin, AxelBoldt, Ben-Arba, Billymac00, Bubba73, CRGreathouse, Charles Matthews, Crisófilax, Dantheox, Dmharvey, Doshell, Droog Andrey, EmilJ, Eric119, EulerGamma, Gandalf61, Gene Ward Smith, Giftlite, GregorB, Haseldon, Ixfd64, JCSantos, James Harris, JamesHoadley, Jimothy 46, Joerite, Karl-H, Katsushi, Madmath789, Magioladitis, Michael Hardy, Mikewarbz, Motomuku, Mwboyer, Numerao, Oleg Alexandrov, PV=nRT, Paul August, Philip Trueman, PittBill, Portalian, PrimeHunter, R.e.b., Rich.lewis, RobertG, Salgueiro, Scythe33, Superm401, Tchoř, That Guy, From That Show!, Tobias Bergemann, Tos, Werner D. Sand, XJamRastafire, Xario, Xenonice, 75 anonymous edits

Primeval prime *Source*: http://en.wikipedia.org/w/index.php?oldid=193722064 *Contributors*: Anton Mravcek, CRGreathouse, Charles Matthews, Ekpyrotic Architect, Fredrik, Giftlite, Herbee, Interlingua, Linas, Mysid, Oleg Alexandrov, PrimeHunter, Schneelocke, 3 anonymous edits

Primorial prime *Source*: http://en.wikipedia.org/w/index.php?oldid=404048004 *Contributors*: Army1987, CRGreathouse, Giftlite, GregorB, Josh Cherry, Koppapa, Michael Hardy, Oleg Alexandrov, Pakaran, PrimeFan, PrimeHunter, RJHall, Robo37, Silverfish, Superm401, Supernumerator, Thinking of England, Triona, 18 anonymous edits

Probable prime *Source*: http://en.wikipedia.org/w/index.php?oldid=407322482 *Contributors*: Ams80, Arvindn, AxelBoldt, CBorges, Charles Matthews, Dcoetzee, Dude1818, Elektron, EmilJ, Fredrik, Ixfd64, Linas, Maxal, Michael Hardy, Neko-chan, Oleg Alexandrov, QuantumEngineer, Redgolpe, Zvika, 4 anonymous edits

Proth number *Source*: http://en.wikipedia.org/w/index.php?oldid=406129079 *Contributors*: Bender235, CRGreathouse, Charles Matthews, Giftlite, Infovarius, Ixfd64, Ken g6, Leavemsg2, Michael Hardy, Oleg Alexandrov, OwenX, PV=nRT, PrimeHunter, Puuropyssy, Qutezuce, R.e.b., Redgolpe, Rikimaru, Vernanimalcula, Visée, XJamRastafire, 4 anonymous edits

Pseudoprime *Source*: http://en.wikipedia.org/w/index.php?oldid=404383341 *Contributors*: Julzes, Maxal, PrimeHunter

Pythagorean prime *Source*: http://en.wikipedia.org/w/index.php?oldid=405667696 *Contributors*: 4pq1injbok, CRGreathouse, David Eppstein, Disavian, Giftlite, Hede2000, Jitse Niesen, JoergenB, Michael Hardy, PrimeFan, XJamRastafire, 1 anonymous edits

Ramanujan prime *Source*: http://en.wikipedia.org/w/index.php?oldid=399107570 *Contributors*: Avraham, Bender235, CBM, CRGreathouse, CiaPan, Gandalf61, Giftlite, Groovybill, Haonhien, Jsondow, Michael Hardy, Nishkid64, PrimeHunter, R. S. Shaw, Reddwarf2956, Salvatore Ingala, Stephen B Streater, Stephenchou0722, The Anome, Toohool, Topbanana, XJamRastafire, ZooFari, 16 anonymous edits

Regular prime *Source*: http://en.wikipedia.org/w/index.php?oldid=386831909 *Contributors*: Boemanneke, CRGreathouse, Charles Matthews, Cristiano Toàn, Cybercobra, DRLB, David Shay, Fredrik, Giftlite, Gwaihir, Henrygb, Herbee, Iffy, LilHelpa, MathMartin, Peter Kwok, Pouya, PrimeFan, PrimeHunter, R.e.b., Reyk, RobHar, Safek, Schneelocke, Throwawayhack, Vanish2, XJamRastafire, 10 anonymous edits

Repunit *Source*: http://en.wikipedia.org/w/index.php?oldid=408603015 *Contributors*: ABCD, Alfio, Arthur Rubin, B.d.mills, Blotwell, Burn, CRGreathouse, CompositeFan, Cristiano Toàn, David Eppstein, Delirium, Dwheeler, Fibonacci, Fivemack, Fuenfundachtzig, GUllman, Gandalf61, Giftlite, Glenn L, GregorB, Gwaihir, Herbee, Jacquerie27, Laurentius, Lazugod, Luokehao, Maxal, Mholland, Michael Hardy, Netsabes, Oleg Alexandrov, Oyd11, Pmanderson, PrimeFan, PrimeHunter, R. J. Mathar, Rar42, Redgolpe, Reinyday, Rich Farmbrough, Rjwilmsi, Sligocki, Srain, Sugarfish, Suslin, Tomlee2060, Toshio Yamaguchi, Vanish2, WATARU, XJamRastafire, Xanthoxyl, ZeroOne, 34 anonymous edits

Safe prime *Source*: http://en.wikipedia.org/w/index.php?oldid=380697172 *Contributors*: A Nobody, Anton Mravcek, Aononemoose, ArnoldReinhold, BigChicken, CBM, CRGreathouse, Colonies Chris, David Schwein, Duke Dudley, Fgrieu, Fredrik, Giftlite, Heryu, HisSpaceResearch, Jafet, Mangojuice, Michael Hardy, Numerao, OwenX, PrimeFan, PrimeHunter, Pyrop, R. S. Shaw, Robma, Soylentgreen47, Starwiz, Wildtornado, 16 anonymous edits

Self number *Source*: http://en.wikipedia.org/w/index.php?oldid=391452853 *Contributors*: Anton Mravcek, Blotwell, CRGreathouse, Chinju, Corti, Daniel,levine, Darkskiez, Fibonacci, Giftlite, Heryu, J'raxis, JackofOz, Joffan, Karl Palmen, Kevin Murray, Linas, Major Danby, Maxal, Michael Hardy, NByz, Noe, Number 0, Numerao, Oleg Alexandrov, Pinkgothic, PrimeFan, PrimeHunter, Pvrantz, Reyk, Rvinjamuri, Sam Korn, Shanes, Vlad, XJamRastafire, Zahlentheorie, 20 anonymous edits

Sexy prime *Source*: http://en.wikipedia.org/w/index.php?oldid=406829717 *Contributors*: Alansohn, Anakata, C.R.Selvakumar, CRGreathouse, CanisRufus, Condem, Crumwell, DragonflySixtyseven, Dysprosia, Emurphy42, FarzanehSarafraz, Gate28, Giftlite, Gurch, Haikz, Herbee, Ideal gas equation, Im.a.lumberjack, JForget, Jwing421, KenJDavis, Lendorien, Linas, Marek69, Mechanical digger, Mike Schwartz, Mwalimu59, Mwoolf, Mysdaao, Neptune5000, Ngebendi, NotAnonymous0, Pengo, PhiEaglesfan712, PrimeHunter, Rebent, Schneelocke, Spondoolicks, Stifle, Suruena, Svick, Tacoblast Legacy, W8TVI, WirelessMaven, Wroscel, Yuefairchild, 70 anonymous edits

Smarandache–Wellin number *Source*: http://en.wikipedia.org/w/index.php?oldid=296374758 *Contributors*: Altenmann, Anton Mravcek, Arvindn, Blotwell, David Eppstein, Fiveless, Fredrik, Gandalf61, Harrypotter, Herbee, Herostratus, Hillman, Hu12, Hutschi, Linas, Lowellian, Michael Hardy, NBeale, NathanBeach, Numerao, Oleg Alexandrov, PrimeFan, PrimeHunter, Pt, ROFLimeditinghistory, Schneelocke, Silverfish, Suisui, Tobias Bergemann, TutterMouse, 4 anonymous edits

Solinas prime *Source*: http://en.wikipedia.org/w/index.php?oldid=318382081 *Contributors*: Drbreznjev, Déjà Vu, Giftlite, Jim.belk, Michael Hardy

Sophie Germain prime *Source*: http://en.wikipedia.org/w/index.php?oldid=408605006 *Contributors*: Advuser14, Angela, Anton Mravcek, Arcadian, Ashmoo, Bender235, Bexalain, Burn, C.R.Selvakumar, CRGreathouse, Ctx13, DYLAN LENNON, Duke Dudley, Dysprosia, Eisnel, EmilJ, Fredrik, Gfis, Giftlite, Hapsiainen, Herbee, Ivan Štambuk, JamesBWatson, K.C. Tang, Linas, Lowellian, Mav, Meni Rosenfeld, Mentifisto, Michael Hardy, Mmxbass, Numerao, Pavel Stanley, PrimeFan, PrimeHunter, Robma, Sabbut, Salix alba, Schneelocke, Silverfish, Slon02, Stevenj, The Anome, The wub, Tide rolls, Tom harrison, Unit 739, Unyoyega, X1cygnus, XJamRastafire, Zoicon5, 霧木諒二, 51 anonymous edits

Star number *Source*: http://en.wikipedia.org/w/index.php?oldid=400616752 *Contributors*: A2569875, CZeke, Caltas, Gentlemath, Giftlite, Karl Palmen, Linas, Mhaitham.shammaa, Numbo3, PrimeFan, PrimeHunter, Qwyrxian, 10 anonymous edits

Stern prime *Source*: http://en.wikipedia.org/w/index.php?oldid=340066505 *Contributors*: Anton Mravcek, CRGreathouse, Cdc, Giftlite, Maproom, Mojomama, Mon4, Nico92400, PrimeFan, PrimeHunter, Simongorbaty, Supernumerator, That Guy, From That Show!, 2 anonymous edits

Strobogrammatic prime *Source*: http://en.wikipedia.org/w/index.php?oldid=389042433 *Contributors*: Angela, Anton Mravcek, CRGreathouse, David Eppstein, FF2010, Giftlite, GrahamN, HollyAm, OwenX, Pengo, PrimeFan, Shell Kinney, Simple Thomas, Squash, Supernumerator, Who, Willy²

Strong prime *Source*: http://en.wikipedia.org/w/index.php?oldid=388951524 *Contributors*: AgentPeppermint, ArnoldReinhold, CRGreathouse, Cristiano Toàn, David Eppstein, David Musgrove, Edward, Eng2007, Giftlite, Iffy, Izzycat, Madmath789, Mangojuice, Michael Hardy, Numerao, PrimeFan, PrimeHunter, Soap, Taggard, 5 anonymous edits

Super-prime *Source*: http://en.wikipedia.org/w/index.php?oldid=405188436 *Contributors*: CRGreathouse, David Eppstein, Hut 8.5, JHunterJ, Ken g6, Lol5916, Magioladitis, Michael Hardy, Pmanderson, PrimeHunter, The Thing That Should Not Be, Turgidson, 2 anonymous edits

Supersingular prime (moonshine theory) *Source*: http://en.wikipedia.org/w/index.php?oldid=311280377 *Contributors*: Doetoe, Roentgenium111, 1 anonymous edits

Thabit number *Source*: http://en.wikipedia.org/w/index.php?oldid=404371861 *Contributors*: Anton Mravcek, DataWraith, Dcoetzee, Giftlite, Linas, Maxal, PrimeFan, PrimeHunter, Silverfish, Zzyzx11, 2 anonymous edits

Truncatable prime *Source*: http://en.wikipedia.org/w/index.php?oldid=321116355 *Contributors*: Arthur Rubin, CRGreathouse, Fredrik, Numerao, PrimeHunter, Sopoforic, Suruena

Twin prime *Source*: http://en.wikipedia.org/w/index.php?oldid=406838275 *Contributors*: AS, Aiden Fisher, Akriasas, Al Pereira, Amos153, AndriuZ, Arthur Rubin, AxelBoldt, Bedivere, C.R.Selvakumar, CRGreathouse, Cimon Avaro, DYLAN LENNON, David Eppstein, Dmharvey, Dysprosia, El Snubbe, EmilJ, Epbr123, Eric119, Fredrik, Giftlite, Gurch, Hakeem.gadi, Heder, Hofoen, Iridescent, Ixfd64, J.delanoy, JForget, JamesBWatson, Jim.belk, Jonathunder, Jonel, Jsondow, Justincoslor, Kingturtle, Kyle Barbour, Lambiam, LavosBacons, Liberty4u, Linas, Loren.wilton, Lumian.world, Lumos3, Lzur, MFH, Marlkiy, Matthew0028, Mav, Maxim Razin, Michael Hardy, Mini-Geek, Mwalimu59, Nickyus, Nicola.fragnito, Numbo3, Oliver Pereira, Paul August, Persian Poet Gal, PhiEaglesfan712, PrimeHunter, R. J. Mathar, Radagast3, Random rings, Rbonvall, Rotem Dan, Rumping, Sabbut, Salgueiro, Seav, Sophus Bie, Spacepotato, Starx, Stephen B Streater, Svick, Teorth, The Nut, Trovatore, XJamRastafire, 129 anonymous edits

Two-sided prime *Source*: http://en.wikipedia.org/w/index.php?oldid=113565750 *Contributors*: Arthur Rubin, CRGreathouse, Fredrik, Numerao, PrimeHunter, Sopoforic, Suruena

Ulam number *Source*: http://en.wikipedia.org/w/index.php?oldid=396975513 *Contributors*: Anthony Appleyard, Arun.ramachandran, Bubba73, Burn, Cairnarvon, David Eppstein, Jonka364, Michael Hardy, NumberTheorist, PrimeHunter, Rjwilmsi, Timeroot, XJamRastafire, 14 anonymous edits

Unique prime *Source*: http://en.wikipedia.org/w/index.php?oldid=349372368 *Contributors*: CRGreathouse, David Eppstein, Emurphy42, Falsifian, Fredrik, Georgia guy, Giftlite, Herbee, Jleedev, JoshWimble, Oleg Alexandrov, PrimeFan, PrimeHunter, Schneelocke, XJamRastafire, 3 anonymous edits

Wagstaff prime *Source*: http://en.wikipedia.org/w/index.php?oldid=407444079 *Contributors*: AndrewWTaylor, AquaRooster, Bender235, Burn, CRGreathouse, Charles Matthews, Essap, Fredrik, Giftlite, Ixfd64, Kaldosh, Linas, Maxal, Michael Hardy, PrimeFan, PrimeHunter, Rikimaru, Schneelocke, Silverfish, Toshio Yamaguchi, WereSpielChequers, 10 anonymous edits

Wall-Sun-Sun prime *Source*: http://en.wikipedia.org/w/index.php?oldid=381534866 *Contributors*: Algebraist, Bender235, Bubba73, Burn, CRGreathouse, Charles Matthews, DragonflySixtyseven, Giftlite, KevinPeter, Linas, Lowellian, Maxal, Michael Hardy, PrimeHunter, Rikimaru, Rspeer, Schneelocke, Smjg, Toshio Yamaguchi, Vanish2, Wasawa, WhiteCrane, XJamRastafire, 12 anonymous edits

Wedderburn-Etherington number *Source*: http://en.wikipedia.org/w/index.php?oldid=348985880 *Contributors*: Andreas Kaufmann, Charles Matthews, Cobi, David Eppstein, Giftlite, Jengelh, Kl4m, Matchups, Michael Hardy, Pmanderson, PrimeFan, PrimeHunter, R.e.b., Radiant!, TheParanoidOne, Twri, Vanish2, 2 anonymous edits

Wieferich pair *Source*: http://en.wikipedia.org/w/index.php?oldid=343046771 *Contributors*: Bender235, Gandalf61, Giftlite, Maxal, Mon4, PrimeHunter, Vanish2

Wieferich prime *Source*: http://en.wikipedia.org/w/index.php?oldid=405792593 *Contributors*: Arthur Rubin, Bender235, Burn, CRGreathouse, Druseltal2005, FractalFusion, Fredrik, FvdP, Gandalf61, Giftlite, Herbee, Ixfd64, Johnblythedobson, Johnny Vogler, JosephSilverman, Jsondow, Katsushi, KnightRider, Linas, MACHIDA, Maxal, Michael Hardy, Oleg Alexandrov, Pavel Vozenilek, Pmanderson, PrimeHunter, Schneelocke, Snowdog, Sohale, Stratusmccloud, TANAKA, Toshio Yamaguchi, Tsemii, Vanish2, Vgy7ujm, 25 anonymous edits

Wilson prime *Source*: http://en.wikipedia.org/w/index.php?oldid=406518550 *Contributors*: Anton Mravcek, Bardofcornish, Bender235, Burn, CRGreathouse, David Eppstein, Dupz, Essap, Fredrik, Giftlite, Herbee, Ixfd64, Linas, Mysid, PrimeHunter, Rikimaru, Schneelocke, Shreevatsa, Silverfish, Toshio Yamaguchi, Vanish2, 6 anonymous edits

Wolstenholme prime *Source*: http://en.wikipedia.org/w/index.php?oldid=255134677 *Contributors*: Bender235, BeteNoir, CRGreathouse, Charles Matthews, Giftlite, Greg Kuperberg, Gwaihir, Henrygb, Linas, Maksim-e, Maxal, Pontus, RekishiEJ, Shirifan, Txomin, User24, 6 anonymous edits

Woodall number *Source*: http://en.wikipedia.org/w/index.php?oldid=403576541 *Contributors*: Adcoon, Bender235, Billymac00, Burn, CRGreathouse, Charles Matthews, DataWraith, Ebyabe, Fredrik, Giftlite, Herbee, Hippolyte, Jnestorius, Lambyte, Michael Hardy, Okki, Personline, Peter Kwok, Ppntori, PrimeFan, PrimeHunter, Rich Farmbrough, Schneelocke, Sligocki, Spangineer, Tbhotch, Tesseran, Tromp, Vanish2, XJamRastafire, 15 anonymous edits

Image Sources, Licenses and Contributors

Image:PrimeNumberTheorem.png *Source*: http://en.wikipedia.org/w/index.php?title=File:PrimeNumberTheorem.png *License*: Public Domain *Contributors*: User:FredStober

Image:Primes - distribution - up to 19 primorial.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Primes_-_distribution_-_up_to_19_primorial.png *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: User:Endlessoblivion

File:RiemannCriticalLine.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:RiemannCriticalLine.svg *License*: Public Domain *Contributors*: User:Slonzor

File:Riemann zeta function absolute value.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Riemann_zeta_function_absolute_value.png *License*: Creative Commons Attribution-Sharealike 2.5 *Contributors*: Conscious, Kilom691

File:Zeta polar.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Zeta_polar.svg *License*: GNU Free Documentation License *Contributors*: User:Geek3, User:Linas

Image:Complex zeta.jpg *Source*: http://en.wikipedia.org/w/index.php?title=File:Complex_zeta.jpg *License*: Public Domain *Contributors*: Jan Homann

Image:zeta.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Zeta.png *License*: GNU Free Documentation License *Contributors*: Anarkman, Brf, EugeneZelenko, Kilom691, WhiteTimberwolf, 1 anonymous edits

Image:Zeta polar.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Zeta_polar.svg *License*: GNU Free Documentation License *Contributors*: User:Geek3, User:Linas

File:Genji chapter symbols groupings of 5 elements.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Genji_chapter_symbols_groupings_of_5_elements.svg *License*: Public Domain *Contributors*: AnonMoos

Image:BellNumberAnimated.gif *Source*: http://en.wikipedia.org/w/index.php?title=File:BellNumberAnimated.gif *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: User:Xanthoxyl

Image:Centered decagonal number.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Centered_decagonal_number.svg *License*: Creative Commons Attribution 2.5 *Contributors*: Claudio Rocchini

Image:Centered heptagonal number.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Centered_heptagonal_number.svg *License*: Creative Commons Attribution 2.5 *Contributors*: Claudio Rocchini

Image:GrayDot.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:GrayDot.svg *License*: Public Domain *Contributors*: Ilmari Karonen

Image:RedDot.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:RedDot.svg *License*: Public Domain *Contributors*: Ilmari Karonen, Pfctdayelise, 1 anonymous edits

Image:MissingDot.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:MissingDot.svg *License*: Public Domain *Contributors*: Ilmari Karonen

Image:BlackDot.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:BlackDot.svg *License*: Public Domain *Contributors*: Ilmari Karonen, Matthias M.

Image:Construct-nombres-tri-centres.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Construct-nombres-tri-centres.png *License*: Public Domain *Contributors*: Burn, Ma-Lik

Image:Seven segment display-animated.gif *Source*: http://en.wikipedia.org/w/index.php?title=File:Seven_segment_display-animated.gif *License*: GNU Free Documentation License *Contributors*: D-Kuru, Guam, Ilse@, Juiced lemon, Mattes, Origamiemensch, Wutsje, 9 anonymous edits

Image:Log-factorial.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Log-factorial.svg *License*: Public Domain *Contributors*: Original uploader was Ec- at en.wikipedia

Image:Factorial plot.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Factorial_plot.png *License*: Public Domain *Contributors*: User:Mathacw

Image:Factorial05.jpg *Source*: http://en.wikipedia.org/w/index.php?title=File:Factorial05.jpg *License*: Attribution *Contributors*: User:Domitori

Image:EisensteinPrimes-01.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:EisensteinPrimes-01.svg *License*: Public Domain *Contributors*: User:Fropuff

Image:Rubiks revenge solved.jpg *Source*: http://en.wikipedia.org/w/index.php?title=File:Rubiks_revenge_solved.jpg *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: User:TheCoffee

Image:Solid white.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Solid_white.svg *License*: Public Domain *Contributors*: User:Fibonacci

Image:Gaussian integer lattice.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Gaussian_integer_lattice.png *License*: GNU Free Documentation License *Contributors*: user:gunther

Image:gauss-primes-768x768.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Gauss-primes-768x768.png *License*: Public Domain *Contributors*: User:Truejackster

Image:GoldbachConjecture.gif *Source*: http://en.wikipedia.org/w/index.php?title=File:GoldbachConjecture.gif *License*: GNU Free Documentation License *Contributors*: Original uploader was Oleg Alexandrov at en.wikipedia

Image:Goldbach-1000.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Goldbach-1000.png *License*: GNU Free Documentation License *Contributors*: Original uploader was Reddish at en.wikipedia

Image:Goldbach-1000000.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Goldbach-1000000.png *License*: GNU Free Documentation License *Contributors*: Original uploader was Reddish at en.wikipedia

Image:DeCSS.PNG *Source*: http://en.wikipedia.org/w/index.php?title=File:DeCSS.PNG *License*: GNU Free Documentation License *Contributors*: Conscious, Matt Crypto, Sissssou, Wondigoma, 1 anonymous edits

Image:LuckySieve.gif *Source*: http://en.wikipedia.org/w/index.php?title=File:LuckySieve.gif *License*: Public Domain *Contributors*: Celtic Minstrel at en.wikipedia

Image:MarkoffNumberTree.png *Source*: http://en.wikipedia.org/w/index.php?title=File:MarkoffNumberTree.png *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: User:KurtSchwitters

Image:primes.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Primes.png *License*: GNU Free Documentation License *Contributors*: Ixfd64, Juiced lemon, Liftarn, Maksim

Image:MotzkinChords4.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:MotzkinChords4.svg *License*: Creative Commons Attribution 3.0 *Contributors*: Original uploader was Robertd at en.wikipedia

Image:MotzkinChords5.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:MotzkinChords5.svg *License*: Creative Commons Attribution 3.0 *Contributors*: Original uploader was Robertd at en.wikipedia

Image:Motzkin4.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Motzkin4.svg *License*: Creative Commons Attribution 3.0 *Contributors*: Original uploader was Robertd at en.wikipedia

Image:Padovan_triangles.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Padovan_triangles.png *License*: unknown *Contributors*: User:Gandalf61

File:Ferrer partitioning diagrams.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Ferrer_partitioning_diagrams.svg *License*: GNU Free Documentation License *Contributors*: User:nonenmac

File:GrayDot.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:GrayDot.svg *License*: Public Domain *Contributors*: Ilmari Karonen

File:RedDot.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:RedDot.svg *License*: Public Domain *Contributors*: Ilmari Karonen, Pfctdayelise, 1 anonymous edits

File:BlackDot.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:BlackDot.svg *License*: Public Domain *Contributors*: Ilmari Karonen, Matthias M.

Image:Pell octagons.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Pell_octagons.svg *License*: Public Domain *Contributors*: Original uploader was David Eppstein at en.wikipedia

Image:Pell right triangles.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Pell_right_triangles.svg *License*: Public Domain *Contributors*: Original uploader was David Eppstein at en.wikipedia

Image:Pierpont_exponent_distribution.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Pierpont_exponent_distribution.png *License*: Public Domain *Contributors*: Fivemack

Image:PrimePi.PNG *Source*: http://en.wikipedia.org/w/index.php?title=File:PrimePi.PNG *License*: Public Domain *Contributors*: Kilom691, Tos, Zeimusu, 1 anonymous edits

Image:PlotDelta.gif *Source*: http://en.wikipedia.org/w/index.php?title=File:PlotDelta.gif *License*: Public Domain *Contributors*: User:Droog_Andrey

Image:RedDotX.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:RedDotX.svg *License*: Public Domain *Contributors*: Ilmari Karonen

Image:GrayDotX.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:GrayDotX.svg *License*: Public Domain *Contributors*: Ilmari Karonen

Image:Chinese checkers start.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Chinese_checkers_start.svg *License*: GNU Free Documentation License *Contributors*: w:en:User:FritzleinFritzlein at English Wikipedia Vectors by w:User:MysidMysid

License