Diszkrét matematika II., 9. előadás

Dr. Takách Géza
NyME FMK Informatikai Intézet
takach@inf.nyme.hu
http://inf.nyme.hu/~takach

2004. április 5

Kongruenciák

Definíció. Legyen $a, b \in \mathbf{Z}$ és $m \in \mathbf{N}$. Ekkor a kongruens b-vel modulo m, ha $m|a-b$. Jelölés: $a \equiv b \,(\mathrm{mod}\ m)$, vagy röviden $a \equiv b \,(m)$.

Tétel.

1. *A modulo m kongruencia ekvivalenciareláció* $\mathbf{Z}$*-n.*
2. *Ha $a \equiv b \,(\mathrm{mod}\ m)$ és $c \equiv d \,(\mathrm{mod}\ m)$, akkor $a + c \equiv b + d \,(\mathrm{mod}\ m)$, $a - c \equiv b - d \,(\mathrm{mod}\ m)$ és $ac \equiv bd \,(\mathrm{mod}\ m)$.*

Bizonyítás. Mintaként: trazitivitás: tfh. $a \equiv b \,(\mathrm{mod}\ m)$ és $b \equiv c \,(\mathrm{mod}\ m)$, belátjuk, hogy $a \equiv c \,(\mathrm{mod}\ m)$.

$$m|b-a \wedge m|c-b \quad \Rightarrow \quad m|(b-a)+(c-b) \quad \Rightarrow \quad m|c-a$$

Utolsó összefüggés: tfh. $a \equiv b \,(\mathrm{mod}\ m)$ és $c \equiv d \,(\mathrm{mod}\ m)$, belátjuk, hogy $ac \equiv bd \,(\mathrm{mod}\ m)$ azaz

$$m|ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d),$$

a feltétel szerint pedig $m|a-b$ és $m|c-d$, tehát ez teljesül. ♢

A tétel speciális esete (ha $c = d$), hogy szabad egy kongruencia mindkét oldalához/ból/t ugyanazt/t/zal a számot/ot/al hozzáadni/kivonni/szorozni. Mi a helyzet az osztással?

$20 \equiv 80 \,(15)$, le szabad-e osztani 4-gyel, illetve 5-tel?

$5 \equiv 20 \,(15)$ teljesül? IGEN! $\qquad 4 \equiv 16 \,(15)$ teljesül? NEM!

Tétel. *Legyen $a, b, c \in \mathbf{Z}$ és $m, n \in \mathbf{N}$.*

1. *ha $ac \equiv bc \,(m)$, akkor $a \equiv b \,(\frac{m}{(c,m)})$*
2. *ha $ac \equiv bc \,(m)$, és $(m, c) = 1$, akkor $a \equiv b \,(m)$*
3. *ha $an \equiv bn \,(mn)$, akkor $a \equiv b \,(m)$*
4. *ha $a \equiv b \,(mn)$, akkor $a \equiv b \,(m)$*

Bizonyítás. (1): Legyen $d = (c, m), c = c_1 d, m = m_1 d$.

$$m = m_1 d | ac - bc = c(a-b) = c_1 d(a-b)$$

d-vel osztva: $m_1|c_1(a-b)$, de $(m_1, c_1) = 1$, tehát $m_1|a-b$. ♢

Lineáris kongruenciák

Feladat. Adottak $a, b \in \mathbf{Z}$ és $m \in N$, keressük azon $x \in \mathbf{Z}$ számokat, amelyekre

$$ax \equiv b \,(\mathrm{mod}\ m).$$

Példa. Oldjuk meg a $21x \equiv 12\,(39)$ kongruenciát!

Ekvivalens átalakításokat végzünk:

$$\begin{array}{rcll} 21x & \equiv & 12 & (39) \quad / : 3 \\ 7x & \equiv & 4 & (13) \\ 20x & \equiv & 4 & (13) \quad / : 4 \\ 5x & \equiv & 1 & (13) \\ 5x & \equiv & 40 & (13) \quad / : 5 \\ x & \equiv & 8 & (13) \end{array}$$

Tehát a megoldások: $8, 21, 34, 47, 60, \ldots$, illetve még: $-5, -18, \ldots$.
Ha modulo 39 számolunk, akkor $47 \equiv 8\,(39)$, $60 \equiv 21\,(39)$, ... Tehát a megoldás:

$$x \equiv 8, 21, 34\,(39).$$

Tétel. *Legyen $d = (a, m)$ és $m = m_1 d, a = a_1 d$.*

1. *A fenti kongruenciának pontosan akkor van megoldása, ha $d|b$.*
2. *Ha u egy megoldás, akkor az általános megoldás $x \equiv u\,(m_1)$, vagyis a megoldás modulo m_1 egyértelmű.*
3. *Ha van megoldás, akkor modulo m a megoldások száma d.*

Bizonyítás. 1. A kongruenciának pontosan akkor van megoldása, ha
$(\exists x)(m|ax - b)$, azaz
$(\exists x)(\exists y)(my = ax - b)$, azaz
$(\exists x)(\exists y)(b = ax - my)$, azaz
megoldható az $ax - my = c$ diofantoszi egyenlet, amiről tudjuk, hogy pontosan akkor teljesül, ha $d|b$.

2. a. Tfh. u megoldás és $v \equiv u\,(m_1)$, lássuk be, hogy v is megoldás!

Kell: $av \equiv b\,(m)$, de mivel $au \equiv b\,(m)$, ezért elég: $au \equiv av\,(m)$, ami azt jelenti, hogy $m|au - av$.

Számoljunk: $au - av = a(u - v) = a_1 d \cdot m_1 k = m \cdot a_1 k$.

2. b. Tfh. u és v is megoldás, lássuk be, hogy $u \equiv v\,(m_1)$.

$$\begin{array}{rcll} au & \equiv & b & (m) \\ av & \equiv & b & (m) \\ \hline a(u-v) & \equiv & 0 & (m) \\ u - v & \equiv & 0 & (m_1) \\ u & \equiv & v & (m_1) \end{array}$$

3. ld. a példát! ♢

Lineáris kongruencia-rendszerek

Feladat.

$$\begin{array}{rcll} a_1 x & \equiv & b_1 & (m_1) \\ & \vdots & & \\ a_k x & \equiv & b_k & (m_k) \end{array}$$

A megoldás szükséges feltétele, hogy külön-külön megoldhatóak legyenek a kongruenciák, azaz $(\forall i)((m_i, a_i)|b_i)$.

Tekintsünk most egy olyan rendszert, ahol egyesével már megoldottuk a kongruenciákat:

$$\begin{array}{rcll} x & \equiv & b_1 & (m_1) \\ & \vdots & & \\ x & \equiv & b_k & (m_k) \end{array}$$

Az egyszerűség kedvéért a $k = 2$ esetet vizsgáljuk, azt is egy konkrét példán:

$$\begin{array}{rcll} x & \equiv & 6 & (7) \\ x & \equiv & 2 & (5) \end{array}$$

Visszavezetés diofantoszi egyenletre

$$\begin{array}{rcll} x & \equiv & 6 & (7) \\ x & \equiv & 2 & (5) \end{array}$$

Ha konkrét megoldást keresünk akkor vezessük vissza a kongruenciákat diofantoszi egyenletekké:

$$\begin{array}{rcll} 7 & \mid & x-6 & \text{azaz} \quad x-6=7y \\ 5 & \mid & x-2 & \text{azaz} \quad x-2=5z \\ & & & \text{tehát} \quad 4=5z-7y \end{array}$$

Ez megoldható mert, $(5,7) = 1 | 4 = 6 - 2$. Egy megoldás: $z = 5, y = 3$.

Tehát $x = 7 \cdot 3 + 6 = 27$ egy megoldás.

Általános megoldás

$$\begin{array}{rcll} x & \equiv & 6 & (7) \\ x & \equiv & 2 & (5) \end{array}$$

$x = 7 \cdot 3 + 6 = 27$ egy megoldás. Mi az általános megoldás?

a) Ha u is megoldás, akkor

$$\begin{array}{rcll} u & \equiv & 6 & (7) \\ 27 & \equiv & 6 & (7) \\ \hline u-27 & \equiv & 0 & (7) \\ 7 & \mid & u-27 & \end{array} \qquad \begin{array}{rcll} u & \equiv & 2 & (5) \\ 27 & \equiv & 2 & (5) \\ \hline u-27 & \equiv & 0 & (5) \\ 5 & \mid & u-27 & \end{array}$$

$$[7,5] | u - 27$$

$$u \equiv 27 \quad ([7,5])$$

b) Ekvivalens átalakításokat használtunk, azaz ha $u \equiv 27\,([7,5])$, akkor $u \equiv 6\,(7)$ és $u \equiv 2\,(5)$. Tehát u is megoldás.

Összefoglalva:
Az általános megoldás $x \equiv 27\,([7,5])$, vagyis $x \equiv 27\,(35)$.

Ha kettőnél több kongruenciából áll a rendszer, akkor ezzel a módszerrel mindig eggyel lehet csökkenteni a kongruenciák számát a rendszerben.

Tétel. *Az*

$$x_i \equiv b_i \quad (i = 1, \ldots, k)$$

kongruenciarendszer pontosan akkor oldható meg, ha

$$(\forall i \neq j)((m_i, m_j) | b_i - b_j).$$

Speciálisan (Kínai maradéktétel): Ha

$$(\forall i \neq j)((m_i, m_j) = 1),$$

vagyis a modulusok páronként relatív prímek, akkor az

$$x_i \equiv b_i \quad (i = 1, \ldots, k)$$

kongruenciarendszernek van megoldása tetszőleges b_i *értékek esetén.*
A megoldás egyértelmű modulo $m_1 \cdot \ldots \cdot m_k$.

Maradékosztályok

Definíció. A modulo m kongruencia ekvivalenciaosztályait modulo m maradékosztályoknak nevezzük.

Jelölés. Az $a \in \mathbf{Z}$ szám osztályát $\overline{a}$ jelöli. $\mathbf{Z}_m$ jelöli a modulo m maradékosztályok halmazát.

Példa. A modulo 3 maradékosztályok:
$\overline{0} = \{0, 3, 6, \ldots, -3, -6, \ldots\}$,
$\overline{1} = \{1, 4, 7, \ldots, -2, -5 \ldots\}$,
$\overline{2} = \{2, 5, 8, \ldots, -1, -4, \ldots\}$.

Definíció. Két maradékosztály összege, különbsége, szorzata egy-egy reprezentánsuk összegének, különbségének, szorzatának osztálya. A tétel szerint ez a definíció "jó", tehát az eredmény tényleg független a reprezentánsok választásától.

Példa.
$\overline{2} \cdot \overline{2} = \overline{2 \cdot 2} = \overline{4} = \overline{1}$ illetve $\overline{5} \cdot \overline{-4} = \overline{5 \cdot (-4)} = \overline{-20} = \overline{1}$;
$\overline{1} - \overline{2} = \overline{1 - 2} = \overline{-1} = \overline{2}$ illetve $\overline{-2} - \overline{8} = \overline{-2 - 8} = \overline{-10} = \overline{2}$.
Ezzel $(\mathbf{Z}_m; +, -, \cdot)$ egy algebrai struktúra lett.

Redukált maradékosztályok

Definíció. Egy $\overline{a} \in \mathbf{Z}$ egy modulo m redukált maradékosztály, ha $(a, m) = 1$.

Ez tényleg a maradékosztály tulajdonsága, és nem a reprezentánsáé, hiszen ha $a \equiv b\,(m)$, akkor $a - b = km$, s így $(a, m) = (b, m)$.

Definíció. Tetszőleges $n \in \mathbf{N}$ számra jelölje $\varphi(n)$ a modulo n maradékosztályok számát. Másképpen: hány n-hez relatív prím szám van 1 és n között. Ez az Euler-féle φ függvény.

Jelölje $\mathbf{Z}_m^*$ a modulo m maradékosztályok halmazát. Ekkor $\mathbf{Z}_m^*$ zárt a szorzásra, mert ha $(a, m) = 1$ és $(b, m) = 1$, akkor $(ab, m) = 1$. Nem zárt viszont az összeadásra és a kivonásra, mert például $(5, 6) = 1$, $(1, 6) = 1$, de $(1 + 5, 6) \neq 1$.

$\varphi(m)$ kiszámítása

$\varphi(1) = 1$, mert $(1, 1) = 1$. Ha p prím, akkor $\varphi(p) = p - 1$, mert p relatív prím minden nála kisebb pozitív egészhez.

Ha $m = p^\alpha$, ahol p prím, akkor m pontosan p többszöröseihez nem relatív prím, ezek: $p, 2p, 3p, \ldots, p^\alpha = p^{\alpha-1} \cdot p$, ami $p^{\alpha-1}$ darab szám. Ezért

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

Belátható, hogy φ gyengén multiplikatív függvény, vagyis $(a,b)=1$ esetén $\varphi(ab)=\varphi(a)\cdot\varphi(b)$. Ezért ha m prímtényezős felbontása $m=p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$, akkor

$$\varphi(m)=\prod_{i=1}^{k}\left(p_i^{\alpha_i}-p_i^{\alpha_i-1}\right)=\prod_{i=1}^{k}p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right)=m\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).$$

Maradékrendszerek

Definíció. Ha a modulo m maradékosztályok mindegyikéből kiválasztunk egy-egy elemet, akkor egy modulo m teljes maradékrendszert kapunk.
Másképpen: m darab páronként inkongruens szám.
Ha csak a modulo m redukált maradékosztályok mindegyikéből választunk ki egy-egy elemet, akkor egy modulo m redukált maradékrendszert kapunk.
Másképpen: $\varphi(m)$ darab páronként inkongruens szám, amelyek m-hez is inkongruensek.

Állítás. *Ha $s=\varphi(m)$ és $r_1,r_2,\ldots,r_s$ egy modulo m redukált maradékrendszer, továbbá $(a,m)=1$, akkor $ar_1,ar_2,\ldots,ar_s$ is egy modulo m redukált maradékrendszer.*

Bizonyítás. 1. Mivel $(a,m)=1$ és $(r_i,m)=1$, ezért $(ar_i,m)=1$.
2. $ar_1,ar_2,\ldots,ar_s$ páronként inkongruensek:
Tegyük fel indirekt módon, hogy valamely $i\neq j$ esetén $ar_i\equiv ar_j\,(m)$. Mivel $(a,m)=1$, ezért minden további nélkül le lehet osztani a-val: $r_i\equiv r_j\,(m)$, ami lehetetlen, hiszen r_i és r_j különböző maradékosztályokból valóak. ♢

Euler-tétel

Tétel. *(Euler) Ha $a,m\in\mathbf{Z}$, $m\leq 1$ és $(a,m)=1$, akkor $a^{\varphi(m)}\equiv 1\,(m)$.*

Bizonyítás. Jelölje $s=\varphi(m)$, és legyen $r_1,r_2,\ldots,r_s$ egy modulo m redukált maradékrendszer. Ekkor $ar_1,ar_2,\ldots,ar_s$ is egy modulo m redukált maradékrendszer. A két maradékrendszer elemei párba állíthatóak úgy, hogy a párok kongruensek legyenek. A kongruenciák összeszorozhatóak:

$$\begin{array}{rcll} r_1r_2\ldots r_s & \equiv & ar_1\cdot ar_2\cdot\ldots\cdot ar_s & (m)\\ r_1r_2\ldots r_s & \equiv & a^s\cdot r_1r_2\ldots r_s & (m)\\ 1 & \equiv & a^s & (m)\end{array}$$

mert $(m,r_1r_2\ldots r_s)=1$. ♢

Következmény. *(Fermat) Ha p pozitív prím, $a\in\mathbf{Z}$ és $p\not|a$, akkor*
$a^{p-1}\equiv 1\,(p)$.

Következmény. *Ha p pozitív prím és $a\in\mathbf{Z}$, akkor $a^p\equiv a\,(p)$.*

Bizonyítás. Két eset: $p\not|a$ [Fermat] vagy $p|a$ [$a^p\equiv 0\equiv a\,(p)$].