Az érettségi vizsgára előkészülő tanulók figyelmébe!

Egyenletek és egyenletrendszerek megoldása a Z_n halmazon

Az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ egyenlet megoldása Z_n-ben

Mielőtt rátérnénk a jelzett egyenlet megoldására, azelőtt tanulságosnak és hasznosnak látjuk megvizsgálni az $a\cdot x+b\cdot y=c$ egyenlet megoldását rendre az R illetve a Z halmazon.

Az egyenletnek az R-en történő megoldásáról az $a\cdot b \neq 0$ feltétel mellett következőket emelnénk ki: az $a\cdot x+b\cdot y=c$ egyenletből bármelyik ismeretlen kifejezhető, így $y=\frac{c-ax}{b}$. Ezért, legyen $x=m$ tetszőleges valós szám, így $y=\frac{c-am}{b}$ vagyis az egyenlet összes megoldása $(m, \frac{c-am}{b})$ ahol $m\in R$ tetszőleges. Tehát az egyenletnek az R-en mindig végtelen sok megoldása van, és ezek mind az $a\cdot x+b\cdot y=c$ egyenletű egyenesen helyezkednek el.

Most vizsgáljuk meg az $a\cdot x+b\cdot y=c$ $(a,b,c\in Z)$ úgynevezett elsőfokú kétismeretlenes diofantikus egyenletnek a Z halmazon való megoldását. Legyen $d=(a,b)$ így $a=d\cdot a'$ *és* $b=d\cdot b'$ ahol $(a', b')=1$ egész számok. Ezért $a\cdot x+b\cdot y=d\cdot(a'\cdot x+b'\cdot y)$ osztható d-vel, így ha c nem osztható d-vel, akkor az adott egyenletnek nincs megoldása a Z-n. Tehát az $(a,b)=d \mid c$ feltétel egy szükséges feltétel a megoldás létezéséhez. A továbbiakban látni fogjuk, hogy ez a feltétel elégséges is. Ezek szerint $c=d\cdot c'$ alakú kell legyen, így végigosztva d-vel a megoldandó egyenletünk $a'\cdot x+b'\cdot y=c'$ alakú lesz, ahol ezúttal $(a',b')=1$. A továbbiakban megkeressük az adott egyenlet összes egész megoldását, de az előbbi megjegyzés alapján már indulásból feltételezhetjük, hogy $(a,b)=1$ mert ha nem, végigosztunk $(a,b)=d$ –vel, és ilyen esetbe kerülünk. Bebizonyítjuk, hogy $x=x_0+b\cdot t$ és $y=y_0-a\cdot t$ megadják az egyenlet *összes egész megoldását*, ha $t\in Z$, és $x_0,\ y_0$ az egyenletnek egy sajátos (partikuláris) megoldása. Valóban, az ilyen alakú számok megoldások, hiszen $ax+by=a\cdot(x_0+b\cdot t)+b\cdot(y_0-a\cdot t)=a\cdot x_0+b\cdot y_0=c$. Most belátjuk, hogy *minden megoldás ilyen alakú*! Legyen $(x,y)\in Z\times Z$ egy megoldás, ezért $a\cdot x+b\cdot y=c$. De $a\cdot x_0+b\cdot y_0=c$ is igaz, hiszen egy sajátos megoldás. Ezek alapján $a\cdot(x-x_0)+b\cdot(y-y_0)=0$ vagyis $a\cdot(x-x_0)=-b\cdot(y-y_0)$. Tehát $a \mid b\cdot(y-y_0)$ és $b \mid a\cdot(x-x_0)$ továbbá $(a,b)=1$ ezért $b \mid (x-x_0)$ vagyis létezik olyan $t\in Z$ amelyre $x-x_0=b\cdot t$ amit visszaírva az $a\cdot(x-x_0)=-b\cdot(y-y_0)$ egyenletbe $y-y_0=-a\cdot t$ adódik. Tehát $x=x_0+b\cdot t$ és $y=y_0-a\cdot t$ valóban megadják az egyenlet *összes egész* megoldását. Megválaszolatlanul maradt még az a kérdés, hogy az egyenletnek egyáltalán van-e megoldása? Ez könnyűszerrel belátható, hiszen $(a,b)=1$, ezért léteznek olyan $u,v\in Z$ számok amelyekre $a\cdot u+b\cdot v=1$, vagyis $a\cdot(u\cdot c)+b(v\cdot c)=c$ ami azt jelenti, hogy létezik $x_0=u\cdot c$ és $y_0=v\cdot c$ sajátos megoldás. Ennek kapcsán érdemes megjegyezni, hogy gyakorlatban a sajátos megoldás megtalálása céljából legalkalmasabb az Euklideszi algoritmus. Ezt most nem részletezzük, mivel ezen bemutatások célja főként az volt, hogy összehasonlíthassuk és kapcsolatot teremtsünk az $a\cdot x+b\cdot y=c$ egyenletnek az R-en, illetve a Z-n történő megoldása, és az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ egyenletnek Z_n-ben történő megoldása között. Térjünk hát rá az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ egyenletnek a Z_n-ben történő megoldására.

A továbbiakra vonatkozóan állapodjunk meg, hogy a (Z_n, +, ·) gyűrűn belül jelölje $-\hat{t}$ a $\hat{t}$ elemnek a „+” műveletre vonatkozó szimmetrikusát, amit esetünkben ellentettnek mondunk, és $\hat{t}'$ a $\hat{t}$ elemnek a „·” műveletre vonatkozó szimmetrikusát, amit esetünkben inverznek mondunk.

A továbbiakban látni fogjuk, hogy csak részben követhetjük az $a{\cdot}x+b{\cdot}y=c$ egyenletnek az Z halmazon történő megoldási módszerét, mert a (Z_n, +, ·)- ben teljesen más szempontokat kell figyelembe vennünk. A legelső eredményt a következő tételben fogalmazunk meg:

2. Tétel. Az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ moduló-egyenletnek a Z_n-ben akkor és csakis akkor van megoldása, ha $(a, b, n)= d \mid c$

Bizonyítás: Legyen $x=\hat{X}$ és $y=\hat{Y}$ az egyenletnek egy megoldása. Ekkor $\hat{a}\cdot\hat{X}+\hat{b}\cdot\hat{Y}=\hat{c}$ vagyis $a\cdot\hat{X}+b\cdot\hat{Y}=\hat{c}$, ezért létezik olyan $k\in Z$ szám amelyre $a{\cdot}X+b{\cdot}Y=c+k{\cdot}n$ vagyis $a{\cdot}X+b{\cdot}Y- k{\cdot}n=$ c. Tehát, ha $(a,b,n)= d$ akkor a baloldal osztható d-vel, így szükségszerűen $d \mid c$ is igaz kell legyen. Fordítva is nyilván igaz, hiszen ha d | c igaz, mivel $d= (a,b,n)$ ezért $d \mid a$, $d \mid b$, $d \mid n$ mind igaz, így $d \mid (a{\cdot}X+b{\cdot}Y- k{\cdot}n)$ is igaz.

Tehát az $(a,b,n)= d \mid c$ feltétel az egyenlet megoldhatóságának szükséges és elégséges feltétele. A második fontos eredmény a *megoldások számára* vonatkozik, és azt a következő tételben fogalmazzuk meg:

3. Tétel. Az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ moduló-egyenletnek a Z_n-ben $d{\cdot}n$ számú megoldása van, ahol $d=(a, b, n)$ és $d \mid c$.

Bizonyítás: $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ mindkét oldalához hozzáadva a $\hat{b}\cdot y$ ellentettjét kapjuk, hogy $\hat{a}\cdot x=\hat{c}+(\hat{-b}\cdot y)$. Ebben az egyenletben az x-et tekintsük változónak, és az $y=\hat{Y}$ pedig rögzített. Így egy $\hat{a}\,x=\hat{B}$ típusú egyismeretlenes kongruencia-egyenletnek tekintjük, ahol $\hat{B}=\hat{c}+(\hat{-b}\cdot\hat{Y})$. Az *előző részben* az **1.Tétel** alapján, az $\hat{a}\,x=\hat{B}$ egyenletnek akkor és csakis akkor van megoldása a Z_n-ben, ha $(a,n)= \delta \mid B = c-b{\cdot}y$ ami azt jelenti, hogy $\hat{c}+(\hat{-b}\cdot\hat{Y})=\hat{0}$ a Z_δ-ban (tehát nem a Z_n-ben!) vagyis $b\cdot\hat{Y}=\hat{c}$ a Z_δ-ban. Tehát $b{\cdot}Y= c+ k{\cdot}\delta$ és mivel $\delta \mid n$ ezért $\frac{n}{\delta}\in Z$, így ezen utóbbi egyenlet mindkét oldalát $\frac{n}{\delta}$-vel beszorozva kapjuk, hogy $\frac{n\cdot b}{\delta}\cdot Y=\frac{n}{\delta}c+ k{\cdot}\delta\cdot\frac{n}{\delta}$ vagyis $\frac{n\cdot b}{\delta}\cdot Y=\frac{n\cdot c}{\delta}+k{\cdot}n$ ami azt jelenti, hogy $\frac{n\cdot\hat{b}}{\delta}\cdot y=\frac{n\cdot\hat{c}}{\delta}$ ezúttal a Z_n-ben (*), és ennek az egyenletnek $\frac{n}{\delta}\cdot(b,\delta)=\frac{n}{\delta}\cdot(b,(a,n))=\frac{n}{\delta}\cdot(a,b,n)=\frac{n\cdot d}{\delta}$ számú y megoldása van (lásd az **1.Tételt** ugyancsak az *előző részben*). Legyen $y=Y_0$ az $\hat{a}\cdot x=\hat{c}+(\hat{-b}\cdot y)$ egyenletnek egy partikuláris megoldása, ekkor minden ilyen megoldásra, a $\hat{a}\cdot x=\hat{c}+(\hat{-b}\cdot\hat{Y}_0)\Leftrightarrow\hat{a}\cdot x+\hat{b}\cdot\hat{Y}_0=\hat{c}$ egyenletnek δ számú x megoldása van, ezért ez előbbiek alapján a $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ egyenletnek a Z_n-ben $\delta\cdot\frac{n\cdot d}{\delta}=n{\cdot}d$ számú megoldása van (v.ö.[1]).

Megjegyzés: Vegyük észre, hogy a $\frac{n}{\delta}$-vel való beszorzás során ha $\delta = d$ lenne, akkor $\frac{\hat{n}\cdot\hat{b}}{\delta} = \frac{\hat{n}\cdot\hat{c}}{\delta} = \hat{0}$ és így a (*) egyenlet egy $\hat{0} = \hat{0}$ azonosság (erre példát is fogunk mutatni), ami azt jelenti, hogy a (*) egyenletnek minden $y \in Z_n$ megoldása, vagyis akkor *n* számú megoldás van, de ez nem mond ellent a kapott $\frac{n \cdot d}{\delta}$ eredménynek ellenben, ilyen feltételek mellett, ez a módszer *ritkán* alkalmazható *megoldási módszernek*.

Gyakorlati szempontból az $\hat{a}\cdot x + \hat{b}\cdot y = \hat{c}$ egyenletnek a Z_n-ben való megoldása céljából a következő 2 esetet választjuk külön:

I. eset: (*a, n*)= 1 vagy (*b, n*)= 1

Ebben az esetben nyilvánvaló, hogy (*a ,n*)= 1 vagy (*b, n*)= 1 ahol természetesen nem kizáró vagyról van szó, vagyis az az eset is beletartozik amikor mindkettő igaz. Legyen pl. (*a,n*)=1 akkor $\hat{a}$ *nem zérusosztó* a Z_n**-**ben, tehát $\hat{a}$ invertálható. Az $\hat{a}\cdot x + \hat{b}\cdot y = \hat{c}$ egyenlet mindkét oldalát beszorozva az $\hat{a}$ inverzével, vagyis $\hat{a}'$-tel kapjuk, hogy: $x + \hat{b}\hat{a}'y = \hat{c}\hat{a}'$ ahonnan $x = \hat{c}\hat{a}' - \hat{b}\hat{a}'y$. Ha most *y*-nak sorra beírjuk a $\{\hat{0}, \hat{1}, \hat{2}, \ldots, \hat{n-1}\}$ halmaz *n* különböző elemét, akkor megkapjuk az *x* megoldásokat is, és az egyenletnek *n*-darab egymástól különböző megoldása van (a **3. Tétel-**ben d=1 értékre is ennyit kapunk).

Teljesen hasonlóan járunk el amennyiben csak $\hat{b}$ invertálható, vagy ha $\hat{a}$ is és $\hat{b}$ is invertálható.

1. példa: Oldjuk meg Z_6-ban a $\hat{5}x + \hat{4}y = \hat{2}$ egyenletet.

Az egyenletnek $d\cdot n$= (5, 4, 6)· 6= 6 különböző megoldása van. Látható, hogy (*a,n*)=(5,6)=1 és (*b,n*)= (*4,6*)= 2 vagyis itt az csak az $\hat{a} = \hat{5}$ invertálható. Az inverze a Z_6-ban $\hat{a}' = \hat{5}$, és ezzel beszorozva az egyenlet mindkét oldalát kapjuk, hogy: $x + \hat{2}y = \hat{4}$, és mindkét oldalhoz hozzáadva a $\hat{2}$y ellentettjét a $\hat{4}$y értéket kapjuk, hogy $x = \hat{4}y + \hat{4}$,ahol $y \in \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$. Természetesen, mivel *n*= 6 nem nagy szám, ezért könnyűszerrel behelyettesíthetjük az y értékeket, de értéktáblázattal áttekinthetőbb az összefoglalása:

y	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$x = \hat{4}y + \hat{4}$	$\hat{4}$	$\hat{2}$	$\hat{0}$	$\hat{4}$	$\hat{2}$	$\hat{0}$

Így a megoldáshalmaz: M= $\{(\hat{4},\hat{0}); (\hat{2},\hat{1}); (\hat{0},\hat{2}); (\hat{4};\hat{3}); (\hat{2},\hat{4}); (\hat{0},\hat{5})\}$.

2. példa: Oldjuk meg Z_5-ben a $\hat{2}x + \hat{3}y = \hat{4}$ egyenletet.

Az egyenletnek $d\cdot n$= (2, 3, 6)· 5=5 különböző megoldása van. Észrevehető, hogy ebben az esetben *n*= 5 és mint *a*= 2 mint *b*= 3 relatív prím az *n* számmal, ezért teljesen mindegy melyiket „fejezzük ki", vagyis melyik ismeretlent melyiknek a függvényében kapjuk meg (hiszen mint $\hat{a}$ mint $\hat{b}$ invertálhatók Z_5-ben). Az előző példa megoldásához hasonló módon kapjuk, hogy $x = y + \hat{2}$, ahol $y \in \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4},\}$, így a megoldáshalmaz a következő:

M= $\{(\hat{2},\hat{0}); (\hat{3},\hat{1}); (\hat{4},\hat{2}); (\hat{0};\hat{3}); (\hat{1},\hat{4})\}$.

3. példa: Oldjuk meg Z_5-ben a $\hat{2}x+\hat{4}y=\hat{3}$ egyenletet.

Az egyenletnek $d\cdot n$= (2, 3, 6)· 5= 5 különböző megoldása van. Ezt a példát csupán csak azért választottuk, mert a $2x+4y=3$ egyenletnek nincs megoldása a Z-n hiszen 3 nem osztható (2,4)= 2-vel, ellenben mint látni fogjuk, a Z_n-ben van megoldás, hiszen az n= 5 mellett, mivel a= 2 és b= 4 , így mint $\hat{a}$ mint $\hat{b}$ invertálhatók Z_5-ben. Az előző példák megoldási menetét követve kapjuk, hogy $x=\hat{3}y+\hat{4}$, ahol $y\in\{\hat{0},\ \hat{1},\ \hat{2},\ \hat{3},\ \hat{4}\}$, így a megoldáshalmaz a következő: M= $\{(\hat{4},\hat{0});(\hat{2},\hat{1});(\hat{0},\hat{2});(\hat{3};\hat{3});(\hat{1},\hat{4})\}$.

$II.\ \text{eset}: (a,n)=d_1\neq 1\ és (b,n)=d_2\neq 1$**:**

Ebben az esetben már nem áll az (a, n)= 1 vagy (b, n)= 1 egyike sem, vagyis sem $\hat{a}$ sem $\hat{b}$ nem invertálható a Z_n halmazon.

Legyen (a,n)= d_1 és (b,n)= d_2 . Aszerint, hogy (d_1, d_2)$\neq$ 1 vagy (d_1, d_2)= 1 két esetet szükséges megkülönböztetni:

1. eset: $(d_1, d_2)\neq 1$

Legyen tehát (d_1, d_2)= $d'\neq 1$. Először is lássuk be, hogy ha (a, b, n)= d akkor d= d'. Valóban, az (a, b, n)= d alapján $d\mid a$ és $d\mid b$ és $d\mid n$, ezért $d\mid(a,\ n)=d_1$ és $d\mid(b,\ n)=d_2$, ezért $d\mid(d_1,\ d_2)=d'$. Fordítva, mivel $d'=(d_1,\ d_2)$ ezért $d'\mid d_1=(a,n)$ és $d'\mid d_2=(b,\ n)$ ezért rendre $d\mid a$ és $d\mid b$ és $d\mid n$, így $d\mid(a,\ b,\ n)=d$. Tehát $d\mid d'$ és $d'\mid d$ alapján $d'=d$.

Így az esetünkben a következő feltételek állnak fenn:

$d_1\mid a$, $d_1\mid n$ és $d_2\mid b$, $d_2\mid n$ továbbá (d_1, d_2)= $d\neq 1$, ezért $a=d\cdot a_1$, $b=d\cdot b_1$ és $n=d\cdot n_1$ **(f)**

Legyen $x=\hat{X}$, $y=\hat{Y}$ az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ egyenlet egy megoldása a Z_n-ben**,** akkor $a\cdot X+b\cdot Y=c+kn$, ahol $k\in N^*$. De mivel a **(f)** feltételek alapján az a, b, n számok mindegyike osztható d'-vel, ezért az egyenletnek c tagja is osztható kell legyen d –vel. Ezek alapján tehát leszögezzük a következő esetet:

1.1) Ha (d_1, d_2)= $d\neq 1$ és c nem osztható d -vel, akkor az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ egyenletnek nincs megoldása a Z_n-ben. Ez teljesen összhangban van a **2. Tétel** eredményével.

4. példa: Oldjuk meg Z_6-ban a $\hat{2}x+\hat{4}y=\hat{3}$ egyenletet.

Az előző példától eltérően itt Z_6-ban számolunk, és (a,n)= 2 valamint (b,n)=4 és d'= (2,4)= 2 nem osztja a c=3 számot, azért az adott egyenletnek nincs megoldása a Z_6-ban

A továbbiakban vizsgáljuk azt az esetet, amikor $d\mid c$ teljesül. Ekkor az egyenlet $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ az **(f)** feltételek alapján így írható: $d\cdot\hat{a}_1 x+d\cdot\hat{b}_1 y=d\cdot\hat{c}_1$, ahol a_1, b_1, c_1 pozitív egész számok. Mindkét oldalhoz hozzáadva a $d\cdot\hat{c}_1$ ellentettjét kapjuk, hogy: $\hat{d}\cdot(\hat{a}_1 x+\hat{b}_1 y-\hat{c}_1)=\hat{0}$ ami *az előző részben leírt* **Következmény**-ben tárgyalt $\hat{d}\cdot z=\hat{0}$, (d,n)= $d\neq 1$, $z\in Z_n$ alakú sajátos elsőfokú egyenlet és láttuk, hogy ennek az egyenletnek k= (d,n)= d darab különböző megoldása van, és a megoldások $z=\dfrac{\hat{m}\cdot n}{d}$ alakúak,

ahol m$\in$ { $\hat{0}$, $\hat{1}$, $\hat{2}$, …, $\hat{d-1}$ }. Tehát a $\hat{d}\cdot(\hat{a}_1 x+\hat{b}_1 y-\hat{c}_1)=\hat{0}$ egyenlőség a Z_n-ben a *d* darab $\hat{a}_1 x+\hat{b}_1 y=\hat{c}_1+\frac{\hat{m}\cdot\hat{n}}{d}$ egyenlet megoldásához vezet, ahol m$\in$ { 0, 1, 2, …, $d-1$ }.

1.2) Ha (d_1, d_2)= $d \neq 1$ és $d \mid c$ akkor az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ egyenletnek $d\cdot n$ számú különböző megoldása van Z_n-ben (a **3. Tétel** szerinti is $d\cdot n$ számú megoldás van), gyakorlati szempontból pedig, az előbbi *d* számú egyenletet kell megoldanunk.

5. példa: Oldjuk meg Z_6-ban a $\hat{2}x+\hat{4}y=\hat{4}$ egyenletet.

Az egyenletnek $d\cdot n$= (2, 4, 6)· 6= 12 különböző megoldása van. Ebben az esetben *a*= 2, *b*= 4, c=4, *n*=6, (2,6)=2 és (4,6)=2 ezért *d* =2. Az előbbiekben leírtak alapján: $\hat{2}x+\hat{4}y=\hat{4} \Leftrightarrow \hat{2}(x+\hat{2}y-\hat{2})=\hat{0}$ vagyis $\hat{2}(x+\hat{2}y+\hat{4})=\hat{0}$ ami $\hat{2}\cdot z=\hat{0}$ alakú**,** és ennek az egyenletnek *k*= (2, 6)= 2 megoldása van, amit az előbbiekben leírtak alapján a következő 2 egyenlet megoldásához vezet: $x+\hat{2}y+\hat{4}=\hat{0}$ vagyis $x+\hat{2}y=\hat{2} \Leftrightarrow x=\hat{2}+\hat{4}y$ (1), illetve $x+\hat{2}y+\hat{4}=\hat{3}$ vagyis $x+\hat{2}y=\hat{5} \Leftrightarrow x=\hat{5}+\hat{4}y$ (2). A leírtak alapján mint az (1) mint a (2) egyenletnek 6-6 különböző (*x,y*) számpár megoldása van. Ezeket könnyűszerrel megkapjuk, ha az (1) illetve (2) esetben az $x=\hat{2}+\hat{4}y$ illetve $x=\hat{5}+\hat{4}y$ egyenletek esetén értéktáblázatot készítünk Z_6 - ban.

2. eset: (d_1, d_2)= 1

Ekkor tehát (a,n)=$d_1 \neq 1$ és (b,n)=$d_2 \neq 1$ és a (d_1, d_2)= 1 alapján az **(f)** feltétel ezúttal így alakul: $d_1 \mid a$, $d_1 \mid n$ és $d_2 \mid b$, $d_2 \mid n$ továbbá (d_1, d_2)= 1 , ezért $a=d_1\cdot a_1$, $b=d_1\cdot b_1$ és $n=d_1\cdot d_2\cdot n_1$ **(ff)**

Ekkor tehát az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c} \Leftrightarrow \hat{d_1}\hat{a_1}x+\hat{d_2}\hat{b_1}y=\hat{c}$ egyenlet esetén mivel $n=d_1\cdot d_2\cdot n_1$ az egyenletet (akárcsak a **3. Tétel** bizonyításában) beszorozhatjuk úgy, hogy akár az *x* vagy akár az *y* együtthatója $\hat{0}$ legyen, de egyidőben mindkettő nem lesz nulla! Valóban, szorozzuk be az egyenlet mindkét oldalát az $\frac{\hat{n}}{d_1}$-el. Ekkor észrevehető, hogy: $\hat{a}\cdot\frac{\hat{n}}{d_1}=\frac{\hat{d_1}\hat{a_1}n}{d_1}=\hat{a_1}n=\hat{0}$, de $\hat{b}\cdot\frac{\hat{n}}{d_1}\neq\hat{0}$, mert ha feltételeznénk az ellenkezőjét, akkor $\frac{nb}{d_1}=k\cdot n$ lenne ami azt jelenti, hogy $b= k\cdot d_1$ és így $d_2=(b,n)=(k\cdot d_1, d_1\cdot d_2\cdot n_1) = d_1\cdot(k, d_2\cdot n_1)$ osztható lenne d_1 –el, ami ellentmond a (d_1, d_2)= 1 feltételnek. Tehát így egy $\hat{B}y=\hat{C}$ (1') alakú egyenletet kapunk, ahol $B=\frac{b\cdot n}{d_1}$, $C=\frac{c\cdot n}{d_1}$ és $b=d_1\cdot b_1$ valamint $n=d_1\cdot d_2\cdot n_1$. Teljesen hasonló módon belátható, hogy ha az egyenlet mindkét oldalát $\frac{\hat{n}}{d_2}$-vel szoroznánk be, akkor egy $\hat{A}x=\hat{D}$ (2') alakú egyenletet kapnánk, ahol A= $\frac{a\cdot n}{d_2}$, D= $\frac{c\cdot n}{d_2}$ és $b=d_1\cdot b_1$ valamint $n=d_1\cdot d_2\cdot n_1$.

Mivel d'= (A,n) = $(d_1^2 a_1 n_1, d_1 d_2 n_1)= d_1\cdot n_1\cdot(d_1 a_1, d_2)\neq 1$ és d' $\mid$ D=c·n$_1$·d$_1$ továbbá

d"= (B,n) = $(d_2^2 b_1 n_1, d_1 d_2 n_1)= d_2\cdot n_1\cdot(d_2 b_1, d_1)\neq 1$ és d" $\mid$ C=c·n$_1$·d$_2$ is igaz

ezért mindkét esetben teljesülnek ***az előző részben*** bemutatott **1.Tétel** 3)-ik esetének a feltételei, és így az **1.Tétel** alapján (2') egyenletnek *d'* számú *x* megoldás van $x=\hat{x}_0+\frac{\hat{m}\cdot\hat{n}}{d'}$, ahol m$\in\{0,\ 1,\ 2,\ \ldots,\ d'-1\}$, úgyszintén az (1') egyenletnek *d"* számú *y* megoldás van és $y=\hat{y}_0+\frac{\hat{m}\cdot\hat{n}}{d''}$, ahol m$\in\{0,\ 1,\ 2,\ \ldots,\ d''-1\}$, ahol $\hat{x}_0$ a (2') és $\hat{y}_0$ az (1') egyenleteknek egy-egy partikuláris megoldása. Mivel a (2') egyenletnek a *d'* számú *x* megoldását, az (1') egyenletnek a *d"* számú *y* megoldásaitól teljesen függetlenül kapjuk meg, ezért az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ egyenletnek a Z_n**-**ben az **(ff)** feltételekkel és jelölésekkel *d'·d''* számú megoldása van, ami a **2. Tétel** –el összhangban *d·n* számú megoldást fog jelenteni.

6. példa: Oldjuk meg Z_6-ban a $\hat{4}x+\hat{3}y=\hat{1}$ egyenletet.

Az egyenletnek *d·n*= (*4, 3, 6*)· 6= 6 különböző megoldása van. Ebben az esetben *a*= 4, *b*= 3, *c*= 1, *n*= 6, d_1 = (*4, 6*)= *2* és d_2 =(3, 6)= 3 ezért (d_1, d_2)=(*2, 3*)= 1.

Először szorozzuk be az egyenlet mindkét oldalát $\frac{\hat{n}}{d_2}=\hat{2}$-vel és kapjuk, hogy: $\hat{2}x=\hat{2}$ amelynek *d'*= (*2, n*)= 2 megoldása van, és ezek x=$\hat{1}$ és x=$\hat{4}$. Most az adott egyenletet szorozzuk be $\frac{\hat{n}}{d_1}=\hat{3}$-mal és kapjuk, hogy $\hat{3}y=\hat{3}$ amelynek *d"*=(3,n)=3 megoldása van, és ezek y=$\hat{1}$, y=$\hat{3}$, y=$\hat{5}$. Könnyen ellenőrizhetjük, hogy a $\hat{4}x+\hat{3}y=\hat{1}$ egyenletnek Z_6-ban 2·3=6 darab (*x,y*) számpárból álló megoldása van, a kapott mindegyik *x* értéket társítanunk kell a kapott mindegyik *y* értékkel, vagyis a megoldáshalmaz elemei: ($\hat{1},\hat{1}$), ($\hat{1},\hat{3}$), ($\hat{1},\hat{5}$), ($\hat{4},\hat{1}$), ($\hat{4},\hat{3}$), ($\hat{4},\hat{5}$). A **2. Tétel** szerint is *d·n*= (4,3,6)·6=1·6=6 megoldás kell legyen.

Végezetül egy olyan feladat megoldását mutatjuk be, amelynek megoldásánál az **1.1)** és **1.2)** eseteknél bemutatott eljárás mindegyikét alkalmaznunk kell.

7. példa: Oldjuk meg Z_{12}-ben a $\hat{6}x+\hat{8}y=\hat{10}$ egyenletet.

Az egyenletnek *d·n* = (6,8,12)·12= 24 különböző megoldása van. Az **1.1)** eset alapján a $\hat{3}x+\hat{4}y=\hat{5}+\frac{\hat{12}\cdot m}{2}=\hat{6m}+\hat{5}$ **,** m$\in\{0,\ 1\}$ vagyis a $\hat{3}x+\hat{4}y=\hat{5}$ (1) és $\hat{3}x+\hat{4}y=\hat{11}$ (2) egyenleteket kell megoldanunk. Most az **1.2)** eset feltételeiben találtatunk, így az (1) egyenlet mindkét oldalát $\frac{\hat{n}}{d_2}=\hat{3}$-al beszorozva a $\hat{9}\cdot x=\hat{3}$ egyenletet kapjuk, amelynek a megoldása $x=\hat{3}+\frac{\hat{12}\cdot m}{3}=\hat{6m}+\hat{3}$, m$\in\{0,\ 1,\ 3\}$, vagyis $x\in\{\hat{3},\ \hat{4},\ \hat{7}\}$ és ezen értékek mindegyikére az (1) egyenletből természetesen ugyanazt a $\hat{4}\cdot y=\hat{8}$ egyenletet kapjuk, aminek a megoldása $y=\hat{2}+\frac{\hat{12}\cdot m}{4}=\hat{3m}+\hat{2}$, m$\in\{0,\ 1,\ 3,\ 4\}$, vagyis az $y\in\{\hat{2},\ \hat{5},\ \hat{8},\ \hat{11}\}$. A megoldásokat a kapott 3 darab *x* érték mindegyikének a kapott 4 darab *y* értékkel való társítása által kapott 12

számpár adja. Teljesen hasonlóan járunk el a $\hat{3}x+\hat{4}y=\hat{11}$ (2) egyenlet esetén is, ahol ugyancsak $\hat{3}$-mal való beszorzás után, ezúttal a $\hat{9}\cdot x=\hat{9}$ egyenlet adódik, amelynek megoldásai $x\in\{\hat{1},\ \hat{5},\ \hat{9}\}$ és ezen értékekre a (2) egyenlet alapján mindhárom esetben a $\hat{4}\cdot y=\hat{8}$ egyenlet adódik, az $y\in\{\hat{2},\ \hat{5},\ \hat{8},\ \hat{11}\}$. Itt is a 3 darab x értéknek a 4 darab y érték társításával megkapjuk a másik 12 megoldást

Megjegyzések:

1)Ezúttal is megjegyezzük, hogy az $\hat{a}\cdot x+\hat{b}\cdot y=\hat{c}$ moduló-egyenlet és az $a\cdot x+b\cdot y\equiv c(\mathrm{mod}\, n)$ kongruencia-egyenlet egyenértékűek, ellenben ezúttal is inkább az oszthatóság „nyelvezetét” választottuk, ugyanis ez jobb összhangban a tananyaggal, és alkalmasabb a témakör könnyebb megértésére.

2) Az [1]-ben kongruencia-egyenletekkel, a **3. Tétel**-nél használt bizonyítási módszerrel indukcióval, a változók száma szerint *n* ismeretlenes diofantikus egyenlet megoldásainak a számát is meghatározzák.

3) Ugyancsak az [1]-ben kongruencia- egyenletekkel és egyenlet rendszerekkel, valamint mátrixok segítségével, eléggé komplex megoldási módszert olvashatunk a többismeretlenes kongruencia-egyenletrendszerek megoldására.