Eötvös Loránd Tudományegyetem
Természettudományi Kar

Szakdolgozat

Számelmélet feladatok szakkörre

Nagy Orsolya

Matematikai elemző szakirány

Témavezető: Szalay Mihály egyetemi docens

Algebra és Számelmélet Tanszék

Budapest
2010

Tartalomjegyzék

1. fejezet

Bevezetés

Szakdolgozatom témájául azért a számelmélet feladatokat választottam, mert középiskolai tanulmányaim során ez volt az egyik kedvenc témaköröm. Egyetemi éveim alatt sikerült egy sokkal gyorsabb, átláthatóbb megoldási módszerrel is megismerkednem, ez pedig a kongruencia volt. Dolgozatom célja, hogy bemutassam hatékonyságát a gimnáziumban tanultakkal szemben.

Arra törekedtem, hogy az olvasó kis bemutatást nyerjen a számelmélet világába. Egyelőre csak a kongruencia alapjaival ismerkedhet meg, de már ebből is látszik hasznossága.

A második, harmadik fejezet elején lévő tételeim és definícióim nagy részét témavezetőm, Szalay Mihály [1.] valamint Freud Róbert – Gyarmati Edit [2.] könyveiből merítettem.

A feladványaimat az irodalomjegyzékben található írások közül válogattam. Igyekeztem alappéldáktól kezdve a versenyfeladatokig mindegyikből feldolgozni.

2. fejezet

Oszthatósági feladatok

2.1. Definíciók

1. Definíció: A b egész számot az a egész szám **osztó**jának nevezzük, ha létezik olyan q egész szám, amelyre $a = bq$.

Jelölés: $b \mid a$. Szavakkal: a osztható b-vel, illetve a többszöröse a b-nek.

Ha nem létezik olyan q egész, amelyre $a = q \cdot b$, akkor a b nem osztója a-nak. A 0 minden számmal osztható, hiszen bármely b-re $0 = b \cdot 0$.

2. Definíció: Ha egy egész szám minden egész számnak osztója, akkor **egység**nek nevezzük.

3. Definíció: Az a és b egész számok **legnagyobb közös osztó**ja d, ha

(1) $d \mid a,\ d \mid b$; és

(2) ha egy c-re $c \mid a,\ c \mid b$ teljesül, akkor $|c| \leq |d|$.

Jelölés: $d = (a, b)$ vagy d=lnko(a, b) vagy d=lnko$\{a, b\}$.

Ha $a = b = 0$, akkor nem létezik legnagyobb közös osztójuk, hiszen minden egész szám közös osztó, és ezek között nincs legnagyobb abszolút értékű.

Minden más esetben a 3. Definíciót pontosan két d szám elégíti ki, amelyek egymás ellentettjei. Mivel egy szám és a negatívja oszthatósági szempontból teljesen egyenértékű, ezért a és b összes közös osztóját úgy kapjuk meg, hogy a pozitív

közös osztók mellé vesszük azok negatívjait. A pozítív közös osztók P halmaza nem az üres halmaz, hiszen az 1 biztosan közös osztó, továbbá P-nek csak véges sok eleme lehet, mert egy nemnulla számnak csak véges sok oszója van. Ennélfogva P elemei között létezik egy legnagyobb, jelöljük h-val. Ekkor nyilván $d = h$ és $d = -h$ kielégítik a 3. Definíciót, más szám viszont nem.

4. Definíció: Az a és b számok **kitüntetett közös osztó**ja δ, ha

(1) $\delta \mid a,\ \delta \mid b$, és

(2') ha egy c-re $c \mid a,\ c \mid b$ teljesül, akkor $c \mid \delta$.

A Definícióból következik, hogy ha két számnak létezik kitüntetett közös osztója, akkor az egységszerestől eltekintve egyértelmű. Ez részletesen kifejtve azt jelenti, hogy egyrészt egy kitüntetett közös osztó bármely egységszerese is az, másrészt két kitüntetett közös osztó szükségképpen egymás egységszerese.

Ha $a = b = 0$, akkor a kitüntetett közös osztójuk a definíció szerint 0.

A továbbiakban ezzel az esettel egyáltalán nem foglalkozunk, azaz mindig eleve feltesszük, hogy az a és b közül legalább az egyik nem nulla.

Megmutatjuk, hogy ha egyáltalán létezik a δ kitüntetett közös osztó, akkor δ csak a legnagyobb közös osztó (valamelyik értéke lehet). Jelöljük d-vel a δ-val azonos előjelű legnagyobb közös osztót. Ekkor egyrészt (3. Definíció (2)) miatt $|\delta| \leq |d|$, másrészt (2') alapján $d \mid \delta$, amiből $|d| \leq |\delta|$ következik. A két egyenlőtlenségből kapjuk, hogy $|d| = |\delta|$, és így az azonos előljel miatt $d = \delta$.

Egyáltalán nem magától éretődő azonban, hogy a legnagyobb közös osztó valóban rendelkezik a (2') kitüntetett tulajdonsággal is, vagyis hogy bármely két egész számnak létezik kitüntetett közös osztója.

5. Definíció: Az $a_1, a_2, \ldots, a_k$ számok **relatív prím**ek, ha nincs egységtől különböző közös osztójuk, azaz $(a_1, a_2, \ldots, a_k) = 1$.

6. Definíció: Az $a_1, a_2, \ldots, a_k$ számok **páronként relatív prím**ek, ha közülük semelyik kettőnek sincs egységtől különböző közös osztója, azaz minden $1 \leq i \neq j \leq k$ esetén $(a_i, a_j) = 1$.

Nyilvánvaló, hogy a páronként relatív prím számok egyúttal relatív prímek is, de ez ($k > 2$ esetén) megfordítva nem igaz. Például a $(3, 11, 22) = 1$. Viszont $(11, 22) = 11$, habár $(3, 11) = 1$ és $(3, 22) = 1$ relatív prímek.

7. Definíció: A p egységtől (és nullától) különböző számot **felbonthatatlan szám**nak nevezzük, ha **csak** úgy bontható fel két egész szám szorzatára, hogy valamelyik tényező egység. Azaz

$$p = ab \Longrightarrow a \text{ vagy } b \text{ egység.}$$

A 0 nemtriviálisan is szorzattá bontható, pl. $0 \cdot 11 = 0$, ezért nem szükséges kikötni, hogy $p \neq 0$.
Továbbá a szorzatban nem lehet a is, b is egység, mert akkor p is egység lenne. **Összetett szám**nak nevezzük azt a nemnulla számot, amelynek triviálistól különböző osztója is van.

8. Definíció: A p egységtől és nullától különböző számot **prímszám**nak (vagy röviden **prím**nek) nevezzük, ha **csak** úgy lehet osztója két egész szám szorzatának, ha legalább az egyik tényezőnek osztója. Azaz

$$p \mid ab \Longrightarrow p \mid a \text{ vagy } p \mid b.$$

Előfordulhat, hogy a p a szorzat mindkét tényezőjét osztja. Mindenképpen ki kell kötnünk, hogy $p \neq 0$, mivel a 0-ra teljesül a definíció további részében megfogalmazott tulajdonság:

$$0 \mid ab \Longrightarrow ab = 0 \Longrightarrow a = 0 \text{ vagy } b = 0 \Longrightarrow 0 \mid a \text{ vagy } 0 \mid b.$$

A definícióból következik, hogy egy prímszám egy több tényezős szorzatnak is csak úgy lehet osztója, ha legalább az egyik tényezőnek az osztója.

9. Definíció: Az a és b pozitív egészek **legkisebb közös többszöröse** a k pozitív egész, ha

(1) $a \mid k,\ b \mid k$; és
(2) ha egy $c > 0$-ra $a \mid c,\ b \mid c$ teljesül, akkor $c \geq k$.

Az a és b legkisebb közös többszörösét $[a, b]$-vel (vagy lkkt(a, b)-vel) jelöljük. Mivel a két szám szorzata, ab nyilvánvalóan közös többszöröse a-nak és b-nek, így $[a, b]$ meghatározásához elég az ab-nél nem nagyobb véges sok pozitív egész között megkeresni az a és b közös többszörösei közül a legkisebbet. A legkisebb közös többszörös létezése és egyértelműsége tehát nyilvánvaló.

2.2. Tételek

Ebben a fejezetben az oszthatóság megértéséhez összegyűjtöttem az alkalmazott tételeket. Néhányat közülük nem bizonyítottam, mivel vagy triviális, vagy túl hosszú lett volna, a szakdolgozatom célja pedig nem ez.

1. Tétel: Az egész számok körében két egység van, az 1 és a -1.

Bizonyítás: Az 1 és -1 valóban egységek: bármely a-ra $\pm 1 \mid a$, hiszen $a = (\pm 1)(\pm a)$. Megfordítva, ha ε egység, akkor az ε az 1-nek is osztója, azaz alkalmas q-val $1 = \varepsilon q$. Mivel $|\varepsilon| \geq 1$ és $|q| \geq 1$, így csak $|\varepsilon| = 1$, azaz $\varepsilon = \pm 1$.

2. Tétel: Ha ε és δ egységek és a, b egész számok, valamint $b \mid a$, akkor $\varepsilon b \mid \delta a$ is teljesül.

Bizonyítás: Az ε az 1-nek is osztója, azaz alkalmas r-rel $1 = \varepsilon r$. Ha $a = bq$, akkor $\delta a = (\varepsilon b)(\delta q r)$, tehát valóban $\varepsilon b \mid \delta a$.

A 2. Tétel azt fejezi ki, hogy egy szám és az egységszerese oszthatósági szempontból teljesen azonosan viselkednek; az egységek az oszthatóság szempontjából „nem számítanak". Ennek alapján nem jelent megszorítást, ha az egész számok oszthatósági vizsgálatát leszűkítjük a nemnegatív egészekre, sőt csak a pozitív egészekkel foglalkozunk.

3. Tétel: a, b, c egész számok esetén:

(1) Minden a-ra $a \mid a$.

(2) Ha $c \mid b$ és $b \mid a$, akkor $c \mid a$.

(3) Az $a \mid b$ és $b \mid a$ oszthatóságok egyszerre akkor és csak akkor teljesülnek, ha az a a b-nek egységszerese.

(4) Ha $c \mid a$ és $c \mid b$, akkor $c \mid a + b$, $c \mid a - b$, tetszőleges (egész) k-ra $c \mid ka$, és tetszőleges (egész) r, s-re $c \mid ra + sb$.

(5) $a - b \mid a^n - b^n = (a - b) \cdot (a^{n-1} + a^{n-2} \cdot b + \ldots + b^{n-1})$

(6) $a + b \mid a^{2k} - b^{2k} = (a + b) \cdot (a^{2k-1} - a^{2k-2} \cdot b + \ldots + a \cdot b^{2k-1} - b^{2k})$

(7) $a + b \mid a^{2k-1} + b^{2k-1} = (a + b) \cdot (a^{2k-2} - a^{2k-3} \cdot b + \ldots - a \cdot b^{2k-3} + b^{2k-2})$

4. Tétel (Oszthatósági szabályok tízes számrendszerben):

- Egy szám pontosan akkor osztható 2-vel (5-tel, 10-zel), ha az utolsó számjegye osztható 2-vel (5-tel, 10-zel).
- Egy szám pontosan akkor osztható 3-mal, ha számjegyeinek összege osztható 3-mal.
- Egy szám pontosan akkor osztható 4-gyel (25-tel, 100-zal), ha az utolsó két számjegyéből alkotott szám osztható 4-gyel (25-tel, 100-zal).
- Egy szám pontosan akkor osztható 6-tal, ha osztható 2-vel és 3-mal, azaz páros és számjegyeinek összege osztható 3-mal.
- Egy szám akkor és csakis akkor osztható 7-tel, ha a szám utolsó számjegyétől kezdve a számjegyeit rendre az $1, 3, 2, -1, -3, -2, 1, 3, 2, -1, -3 - 2 \ldots$ sorozat elemeivel megszorozva, és a szorzatok összegét véve az összeg osztható 7-tel.
- Egy szám pontosan akkor osztható 8-cal (125-tel, 1000-rel), ha az utolsó három számjegyből alkotott szám osztható 8-cal (125-tel, 1000-rel).
- Egy szám pontosan akkor osztható 9-cel, ha számjegyeinek összege osztható 9-cel.
- Egy szám akkor és csakis akkor osztható 11-gyel, ha váltakozó előjellel vett számjegyeinek összege osztható 11-gyel.
- Egy szám pontosan akkor osztható 16-tal (625-tel, 10000-rel), ha az utolsó négy számjegyéből alkotott szám osztható 16-tal (625-tel, 10000-rel).

5. Tétel: Tetszőleges a és $b \neq 0$ egész számokhoz léteznek olyan egyértelműen meghatározott q és r egész számok, melyekre

$$a = bq + r \quad \text{és} \quad 0 \leq r < |b|.$$

Bizonyítás: Legyen először $b > 0$. A

$$0 \leq r = a - bq < b$$

feltétel pontosan akkor teljesül, ha

$$bq \leq a < b(q + 1),$$

azaz

$$q \leq \frac{a}{b} < q + 1.$$

Ilyen q egész szám pedig nyilván pontosan egy létezik; $q = \left\lfloor \frac{a}{b} \right\rfloor$, azaz a legnagyobb olyan egész szám, amely még kisebb vagy egyenlő, mint $\frac{a}{b}$. Ha $b < 0$, akkor a

$$0 \leq r = a - bq < |b| = -b$$

feltétel

$$q \geq \frac{a}{b} > q - 1$$

teljesülésével ekvivalens, ami ismét pontosan egy q egészre áll fenn. A maradékos osztásnál kapott q számot **hányados**nak, az r-et pedig (legkisebb nemnegatív) **maradék**nak nevezzük. A $b \mid a$ oszthatóság ($b \neq 0$ esetén) pontosan akkor teljesül, ha a maradék 0.

6. Tétel: Tetszőleges a és $b \neq 0$ egész számokhoz léteznek olyan egyértelműen meghatározott q és r egész számok, melyekre

$$a = bq + r \quad \text{és} \quad -\frac{|b|}{2} < r \leq \frac{|b|}{2}.$$

Ebben az esetben az r-et **legkisebb abszolút értékű maradék**nak nevezzük. Például legyen $a = 22, b = -6$, ekkor $22 = (-6)(-3) + 4 = (-6)(-4) - 2$, tehát a legkisebb nemnegatív maradék a 4, a legkisebb abszolút értékű maradék pedig a -2.

7. Tétel: Bármelyik két egész számnak létezik kitüntetett közös osztója.

Bizonyítás: A kitüntetett közös osztó létezését az **euklideszi algoritmus**sal igazoljuk. Az egyik számot maradékosan elosztjuk a másikkal (feltéve, hogy nem 0), utóbbit a maradékkal és így tovább, mindig az osztót a maradékkal, amíg 0 maradékhoz nem jutunk. Megmutatjuk, hogy az eljárás véges, és az utolsó nemnulla maradék lesz a két szám (egyik) kitüntetett közös osztója.
Nézzük mindezt részletesen. Tegyük fel, hogy (pl.) $b \neq 0$. Ha $b \mid a$, akkor $\delta = b$ megfelel. Ha b nem osztja a-t, akkor alkalmas q_i, r_i egészekkel

$$\begin{aligned}
a &= bq_1 + r_1, \quad ahol \quad 0 < r_1 < |b|, \\
b &= r_1 q_2 + r_2, \quad ahol \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad ahol \quad 0 < r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \quad ahol \quad 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_{n+1} \qquad\qquad r_{n+1} = 0
\end{aligned}$$

Az eljárás biztosan befejeződik véges sok lépésben, ugyanis a maradékok nemnegatív egészekből álló szigorúan csökkenő sorozatot alkotnak:

$$|b| > r_1 > r_2 > \dots$$

Most belátjuk, hogy r_n valóban az a és b számok (egyik) kitüntetett közös osztója. Az algoritmus egyenlőségein alulról felfelé haladva először azt igazoljuk, hogy r_n közös osztója a-nak és b-nek. Az utolsó egyenlőségből $r_n \mid r_{n-1}$. Az utolsó egyenlőségből megkapjuk, hogy

$$r_n \mid r_{n-1},\ r_n \mid r_n \Longrightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2},$$

ezután rekurzív módon visszahelyettesítünk. A kitüntetett tulajdonság igazolásához felülről lefelé haladunk. Legyen $c \mid a,\ c \mid b$, ekkor az első egyenlőségből $c \mid a - bq = r_1$. A második egyenlőséget nézve

$$c \mid b,\ c \mid r_1 \Longrightarrow c \mid b - r_1q_2 = r_2.$$

Ugyanígy folytatva az utolsó előtti egyenlőségből kapjuk, hogy $c \mid r_n$.

8. Tétel: Ha $c > 0$, akkor $(ca, cb) = c(a, b)$.

9. Tétel: Az a és b számok legnagyobb közös osztója alkalmas u és v egészekkel kifejezhető $(a, b) = au + bv$ alakban.

10. Tétel: Ha $c \mid ab$ és $(c, a) = 1$, akkor $c \mid b$.

11. Tétel: Az egész számok körében p akkor és csak akkor prím, ha felbonthatatlan.

Ezért jogosult a felbonthatatlan vagy prím elnevezések bármelyikének a használata, és az is, hogy a középiskolában az egészekre a felbonthatatlan számnak megfelelő tulajdonsággal értelmezik a prímszámot. A két fogalom azonban sok más számkörben nem ekvivalens.

12. Tétel (A számelmélet alaptétele): Minden, a 0-tól és egységtől különböző egész szám felbontható véges sok felbonthatatlan szám szorzatára, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű. (Az egyértelműség azt jelenti, hogy ha

$$a = p_1p_2 \dots p_r = q_1q_2 \dots q_s,$$

ahol a p_i és q_j számok valamennyien felbonthatatlanok, akkor $r = s$, és a p_i és q_j számok párba állíthatók úgy, hogy mindegyik p_i a hozzá tartozó q_j-nek egységszerese.)

13. Tétel: Minden $n > 1$ egész szám felírható

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

alakban, ahol $p_1, \dots p_r$ *különböző* (pozitív) prímek és $a_i > 0$ egész. Ez a felírás a $p_i^{\alpha_i}$ prímhatványtényezők sorrendjétől eltekintve egyértelmű.
Ezt az előállítást az n szám **kanonikus alak**jának nevezzük.
Bizonyos esetekben megengedhetjük, hogy a kanonikus alakban egyes prímek kitevője 0 lehessen, ekkor az egyértelműség természetesen ezektől a tényezőktől eltekintve értendő. Ily módon az 1 számnak is beszélhetünk kanonikus alakjáról.

14. Tétel: A

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

kanonikus alakú n számnak egy d pozitív egész akkor és csak akkor osztója, ha d kanonikus alakja

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}, \quad \text{ahol} \quad 0 \le \beta_i \le \alpha_i,\ i = 1, 2, \dots r.$$

Az osztók esetében a 0 kitevőt is megengedő módosított kanonikus alakot használtunk. Az 1, illetve n triviális osztókat abban a két speciális esetben kapjuk meg, amikor (minden i-re) $\beta_i = 0$, illetve $\beta_i = \alpha_i$.
Egy $n > 0$ egész pozitív osztóinak a számát $d(n)$-nel jelöljük.
Például $d(1) = 1, d(8) = 4, d(n) = 2 \Longleftrightarrow n$ prím.

15. Tétel: Az

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

kanonikus alakú n szám pozitív osztóinak a száma

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1).$$

2.3. Feladatok

1. Feladat: Bizonyítsa be, hogy minden $n \in \mathbb{N}$ számra $6 \mid n^3 + 11n$.

I.Megoldás: Egy szám osztható 6-tal, ha páros és számjegyeinek összege osztható 3-mal.
$n^3+11n = (n-1)n(n+1)+12n$ vizsgalatából láthatjuk, hogy mindenképpen osztható lesz hárommal, mivel az első tag 3 egymást követő egész szám szorzata és $3 \mid 12$. Kettővel is osztható, mert két páratlan és egy páros szorzata, valamint két páros és egy páratlan szorzata is páros lesz és $2 \mid 12$.

II.Megoldás: Teljes indukcióval: $6 \mid n^3 + 11n = n(n^2 + 11)$.
$n = 1$ esetén $1^3 + 11 \cdot 1 = 12 \quad 6 \mid 12$ igaz.
Tegyük fel, hogy n-re igaz, bizonyítjuk, hogy akkor $(n + 1)$-re is igaz, hogy
$6 \mid (n + 1)^3 + 11(n + 1)$.
$(n + 1)^3 + 11(n + 1) = (n^3 + 11n) + 12 + 3n(n + 1)$.
Mindegyik tag osztható 6-tal:
az $n^3 + 11n$ a feltétel miatt,
a $3n(n + 1)$ pedig azért, mert az $n(n + 1)$ két egymást követő egész szám szorzata, vagyis páros és hármas tényező is megtalálható a szorzatban.
Mivel az öröklődést is beláttuk, ezért igaz az állítás.

2. Feladat: Bizonyítsa be, hogy $19 \mid 3^{123} - 2^{123}$ és $19 \mid 3^{124} - 11 \cdot 2^{124}$.

Megoldás: $19 \mid 3^{123} - 2^{123}$:
$3^{123}-2^{123} = (3^3)^{41}-(2^3)^{41} = 27^{41}-8^{41} \Longrightarrow 27-8 \mid 27^{41}-8^{41}$, vagyis $\qquad 19 \mid 27^{41}-8^{41}$

$19 \mid 3^{124} - 11 \cdot 2^{124}$:
$3^{124} - 11 \cdot 2^{124} = 3^{124} - 3 \cdot 2^{123} + 3 \cdot 2^{123} - 11 \cdot 2^{124} = 3(3^{123} - 2^{123}) + 2^{123}(3 - 22)$.
Az előző példából: $19 \mid 3^{123} - 2^{123}$ és a másik tag is osztható 19-cel.

3. Feladat (Forrás: [4.]): Egy tányérban cseresznye van. Felszólítunk valakit, hogy a cseresznyét távollétünkben szedje ki ötösével, és minden 5 cseresznyéből tegyen egyet a következő tányérba, 4-et egy tálba. Ha már csak 5-nél kevesebb cseresznye van, azt hagyja az első tányérban, a második tányérból pedig rakja tovább ugyanilyen eljárással a cseresznyét. Ezt ismételje addig, amíg az utolsó tányérba 5-nél kevesebb cseresznye nem kerül. Ezután csak a tányérokban levő cseresznyéket nézve meg tudjuk állapítani, hány szem cseresznye volt összesen. Hogyan? Mennyi cseresznye volt, ha a négy tányérba sorra $2, 4, 1, 3$ cseresznye került és több tányérra nem volt szükség?

Hogyan alakul a helyzet, ha nem ötösével, hanem kettesével, ill. tízesével szedjük ki a cseresznyét?

Megoldás: *a*) Jelöljük a-val az 1. tányérban eredetileg lévő cseresznyék számát, amit keresünk.
Nevezzük el:

b-nek az 1. tányérból a 2.-ba tett cseresznyék számát,

c-nek az 2. tányérból a 3.-ba tett cseresznyék számát,

d-nek az 3. tányérból a 4.-be tett cseresznyék számát.

Tudjuk, hogy az öttel való osztási maradékok az a, b, c, d-nek rendre 2, 4, 1, 3.
Ebből következik, hogy:

$$\begin{aligned} a &= 5b + 2 \\ b &= 5c + 4 \\ c &= 5d + 1 \\ d &= 3 \end{aligned}$$

Behelyettesítéssel megkapjuk, hogy $a = 2 + 5(4 + 5(1 + 3 \cdot 5)) = 422$.
Vagyis **422 db** cseresznye volt a tányérban eredetileg.

b) Ha kettesével szedjük ki a cseresznyéket:

A kettővel való osztás adja meg, hogy hányszor tettünk át cseresznyét a következő tányérba, az osztási maradékok pedig azt, hogy a végén mennyi cseresznye maradt bennük.

$$\begin{aligned} 422 &= 221 \cdot 2 + \mathbf{0} \\ 221 &= 105 \cdot 2 + \mathbf{1} \\ 105 &= 52 \cdot 2 + \mathbf{1} \\ 52 &= 26 \cdot 2 + \mathbf{0} \\ 26 &= 13 \cdot 2 + \mathbf{0} \\ 13 &= 6 \cdot 2 + \mathbf{1} \\ 6 &= 3 \cdot 2 + \mathbf{0} \\ 3 &= 1 \cdot 2 + \mathbf{1} \\ 1 &= 0 \cdot 2 + \mathbf{1} \end{aligned}$$

Tehát **9 darab** tányérra lenne szükségünk, amikben rendre **0, 1, 1, 0, 0, 1, 0, 1, 1 darab** cseresznye maradna.

c) Ha tízesével szedjük ki a cseresznyéket:

A tízesével való osztás adja meg, hogy hányszor tettünk át cseresznyét a következő tányérba, az osztási maradékok pedig azt, hogy a végén mennyi cseresznye maradt bennük.

$$\begin{aligned} 422 &= 42 \cdot 10 + \mathbf{2} \\ 42 &= 4 \cdot 10 + \mathbf{2} \\ 4 &= 0 \cdot 10 + \mathbf{4} \end{aligned}$$

Tehát **3 darab** tányérra lenne szükségünk, amikben rendre **2, 2, 4 darab** cseresznye maradna.

4. Feladat (KÖMaL, 1996. szeptember): Legfeljebb hány olyan hónap lehet egy évben, amelyben öt vasárnap van?

Megoldás: Egy hónap napjainak száma 28 és 31 között változik, vagyis minden hónapban legalább 4 vasárnap van, 5-nél több viszont egyetlen hónapban sincsen. Egy év $365 = 52 \cdot 7 + 1$ napból áll, vagy pedig - szökőév esetén - $366 = 52 \cdot 7 + 2$ napból, így egy évben 52 vagy 53 vasárnap van. A tizenkét hónap mindegyike tartalmaz tehát legalább 4 vasárnapot. Az így adódó 48-on túl fennmaradó 4, illetve 5 vasárnap feltétlenül különböző hónapokra esik, mert 6 vasárnap nem lehet egy hónapban. Ez azt jelenti, hogy **legfeljebb öt** olyan hónap lehet egy évben, amelyben öt vasárnap van. Ez éppen azokban az években fordul elő, amelyekben 53 vasárnap van, vagyis, ha az év első napja vasárnap, illetve szökőév esetén, ha az első nap szombat, vagy vasárnap.

5. Feladat (Forrás: [2.]): *a*) Egy kör alakú tisztás mentén m fa áll, mindegyiken egy-egy mókus. A mókusok össze szeretnének gyűlni egy fán, de csak úgy változtathatják a helyüket, hogy két tetszőleges mókus egyidejűleg átugorhat egy-egy szomszédos fára. Ezt a lépest akárhányszor megismételhetik. Milyen m esetén tudnak összegyűlni a mókusok?

b) Mi a helyzet akkor, ha a megengedett lépést a következőképpen módosítjuk: két tetszőleges mókus egyidejűleg átugorhat egy-egy szomszédos fára, azonban ellenkező körüljárási irányban kell ugorniuk.

Megoldás:

a) Pontosan akkor tudnak összegyűlni, ha m páratlan vagy osztható 4-gyel.

Ha m páratlan, vagyis $4k \pm 1$ alakú, akkor a legnagyobb fán levő mókus maradjon ott, a két szomszédja egy lépésben odaugrik, a két másodszomszédja két lépésben odaugrik és így tovább.

Ha m osztható 4-gyel, vagyis $4k$ alakú, akkor a fenti lépések után csak a legnagyobb fával szemközti fán marad egy mókus, amely páros sok ugrással eljut a többiekhez, miközben egy másik ide-oda ugrál a legnagyobb fa és valamelyik szomszédja között.

Végül, ha m páros, de 4-gyel nem osztható, vagyis $4k + 2$ alakú, akkor a mókusok nem tudnak összegyűlni. Tekintsük ugyanis, hány ugrással juthat el egy-egy mókus a kijelölt fára. Ezeknek az ugrásszámoknak az összege mindenképpen páratlan, tehát a feladat feltételei szerint nem valósítható meg.

Megoldás:

b) Pontosan a páratlan m-ekre lesz mókusgyűlés.

Az *a*)-beli gondolatmenetek továbbra is érvényesek, ha m nem osztható 4-gyel.

A 4-gyel osztható (illetve tetszőleges páros) m-ekre számozzuk meg a fákat sorban 1-től m-ig. Minden helyzetben adjuk össze azoknak a fáknak a sorszámait, amely fákon mókus ül, mégpedig minden sorszámot annyiszor, ahány mókus található az adott fán. Ennek az összegnek az m-mel vett maradéka nem változik az ugrálás során. A kiindulási helyzetben ez a maradék $1 + 2 + 3 + \cdots + m = \frac{m(m+1)}{2} = m \cdot (m/2) + m/2$ maradéka, ami $m/2$. Ha miden mókus ugyanazon a fán tanyázik, akkor a maradék nyilván 0, tehát ez az állapot nem jöhet létre.

6. Feladat (Forrás: [6.]): Írjunk fel olyan, az $1, 2, \ldots, 6$ számjegyek valamilyen sorrendjéből álló 6-jegyű számot, melynek első két jegyéből álló szám osztható 2-vel, az első 3 jegyéből álló szám osztható 3-mal, az első 4 jegyéből álló szám osztható 4-gyel, az első 5 jegyéből álló szám osztható 5-tel és maga a szám osztható 6-tal.

Megoldás: Oszthatósági szabályok felhasználásával.[1]

Az 5. helyre mindenképpen 5-öt kell írnunk,mert csak akkor lesz osztható 5-tel (mivel nincs 0).

A 2., 4., 6. helyre mindenképpen páros szám kerül, mivel csak akkor lehet osztható 2-vel, 4-gyel, 6-tal.

Így az 1. és 3. helyre marad az 1 és a 3.

helyiérték	1.	2.	3.	4.	5.	6.
lehetséges számok	1, 3	2, 4, 6	1, 3	2, 4, 6	5	2, 4, 6

Az első 3 jegyéből álló szám akkor lesz osztható 3-mal, ha a 2. helyen 2 áll, mert csak akkor teljesül rá, hogy $3 \mid 1+3+2=6$.

Az első 4 jegyéből álló szám akkor lesz osztható 4-gyel, ha a 4. helyen nem 4 áll, mivel a 3.-4. hely csak ilyen formájú lehet: $12, 16, 32, 36$.

Emiatt a 6. helyen mindenképpen a 4-nek kell állnia és a 4. helyen mindenképpen a 6-nak.

Tehát a következő megoldások lehetségesek: **123654, 321654**.

7. Feladat (Forrás: [3.]): Bizonyítsuk be, hogy $3^{3n+3}-26n-27$ osztható 169-cel, ha n nemnegatív egész szám.

Megoldás: Kell: $169 \mid 3^{3n+3}-26n-27$

Bizonyítás teljes indukcióval:

$n=1$ esetén igaz, mert $169 \mid 3^{3\cdot 1+3}-26\cdot 1-27=676$.

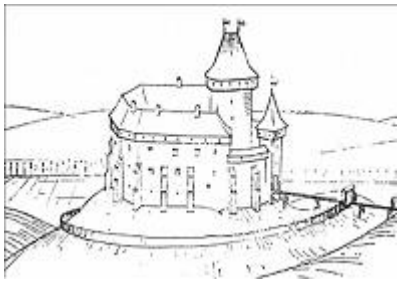
Tegyük fel, hogy n-re igaz, vagyis $169 \mid 3^{3n+3}-26n-27$, bizonyítjuk, hogy akkor $(n+1)$-re is igaz.

$$
\begin{gathered}
3^{3(n+1)+3}-26(n+1)-27= \\
3^{3n+6}-26n-26-27= \\
3^3\cdot(3^{3n+3}-26n-27)+676n+676= \\
3^3\cdot(3^{3n+3}-26n-27)+4\cdot 169(n+1)
\end{gathered}
$$

Az első tag az indukciós feltevés miatt osztható 169-cel, a második tagban pedig szorzótényezőként szerepel, tehát osztható vele.

[1] Lásd 2. fejezet 4. Tétel

8. Feladat (Forrás: [2.]): Egy kegyetlen várúr börtönének 400 szűk cellájában egy-egy rab sínylődik. A cellák ajtaján lévő zár úgy működik, hogy egy elfordítás esetén nyílik, még egy elfordítás esetén ismét bezárul. Jelenleg természetesen minden ajtó zárva van. A várúr a születésnapján elhatározza, hogy nagylelkű lesz, és megparancsolja az egyik őrnek, hogy fordítson egyet valamennyi záron. Közben azonban meggondolja magát, és utánaküld egy másik őrt, akit azzal bíz meg, hogy minden második záron fordítson egyet. Ezt követi a harmadik őr, aki minden harmadik záron változtat és így tovább, végül a négyszázadik őr a négyszázadik cella zárjának az állását módosítja. Azok a rabok szabadulnak ki, akiknek most nyitva van az ajtaja. Hány rabot bocsátott szabadon a várúr?



Megoldás: Az őrök annyiszor fordítanak az n. számú záron, amennyi osztója van az adott cellának. Meggondolva tehát, csak akkor szabadul ki egy rab, ha $d(n)$ páratlan számú, vagyis $d(n) = 2k+1$ alakú. Ez viszont csak akkor lehetséges, ha n négyzetszám. Minden más esetben $d(n)$ páros számú lesz, ugyanis a többi esetben a kanonikus alak tartalmaz páratlan kitevőjű hatványt, emiatt pedig az osztóinak a száma páros lesz.[2] Tehát 1-től 400-ig kell csak megkeresnünk a négyzetszámokat. A feltételeknek megfelelően az 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324, 361, 400 lesznek a jó cellák. Tehát összesen **20** rab lesz szabad a várúr nagylelkűsége miatt.

[2]Lásd 2. fejezet 15. Tétel.

3. fejezet

Kongruenciák

3.1. Definíciók

A kongruencia fogalma: Legyenek a és b egész számok és m pozitív egész. Azt mondjuk, hogy a **kongruens** b-vel modulo m, ha $m \mid a - b$.

Jelölés: $a \equiv b \pmod{m}$ vagy röviden $a \equiv b\ (m)$. Az (általában rögzített) m számot **modulus**nak nevezzük.

Ha a és b nem kongruensek modulo m, akkor azt mondjuk, hogy a és b **inkongruens**nek modulo m (vagy a inkongruens b-vel modulo m).

Először érdemes megjegyezni, hogy a modulus lehet ugyan negatív, de $a \equiv b \pmod{m} \iff a \equiv b \pmod{|m|}$ miatt elég nemnegatív modulusokra szorítkozni.

A modulus lehet 0 is : $a, b \in \mathbb{Z}$-re $a \equiv b \pmod{0} \iff 0 \mid a - b \iff a = b$. Az egyenlőség tehát ott van a kongruenciák között, de jól ismerjük a tulajdonságait, így elég $m \geq 1$-re szorítkozni.

Az $m = 1$ eset viszont érdektelen, mert minden $a, b \in \mathbb{Z}$-re $a \equiv b \pmod{1}$, hiszen $1 \mid a - b$.

Következtetéseinknél tehát $m \geq 2$ az érdekes eset, s legfeljebb kényelmesebb megfogalmazás céljából fordulhat elő más modulus.

Mivel $m \mid a - b \iff m \mid b - a$, ezért

$$a \equiv b \pmod{m} \iff b \equiv a \pmod{m}.$$

Definíció: Legyen $m \geq 2$ egész. Azt mondjuk, hogy a $c_1, c_2, \cdots, c_k$ egész számok $(\text{mod } m)$ **teljes maradékrendszer**t alkotnak, ha

$a)$ $k = m$.

és

$b)$ páronként inkongruensek $(\text{mod } m)$.

3.2. Tételek

Ebben a fejezetben gyűjtöttem össze a kongruenciák megértéséhez az alkalmazott tételeket.

1. Tétel: Ha a, b, c, m egész számok, akkor érvényesek a következők:
(i) $a \equiv a \pmod{m}$ (refexivitás);
(ii) $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$ (szimmetria);
(iii) $a \equiv b \pmod{m}$ és $b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$. (tranzitivitás)

Bizonyítás: $m \mid 0 = a - a$ miatt $a \equiv a \pmod{m}$.
Ha $a \equiv b \pmod{m} \Longrightarrow m \mid a - b$, így $m \mid b - a$, tehát $b \equiv a \pmod{m}$.
Ha $a \equiv b \pmod{m}$ és ha $b \equiv c \pmod{m} \Longrightarrow m \mid a - b$ és $m \mid b - c$, ezért $m \mid (a - b) + (b - c) = a - c$, tehát $a \equiv c \pmod{m}$.

2. Tétel: Legyenek a, b, c, d, m, u, v egészek. Ha $a \equiv b\ (m)$ és $c \equiv d\ (m)$, akkor tejesülnek a következők:

$a)$ $a + c \equiv b + d \pmod{m}$;

$b)$ $a - c \equiv b - d \pmod{m}$;

$c)$ $au + cv \equiv bu + dv \pmod{m}$;

$d)$ $ac \equiv bd \pmod{m}$.

Bizonyítás: A feltételek szerint $m \mid a-b$ és $m \mid c-d$. Ezért $m \mid u(a-b)+v(c-d) = (au + cv) - (bu + dv)$ adja a $c)$ állítást; ebből $u = 1; v = 1$ az $a)$ állítást; $u = 1; v = -1$ a $b)$ állítást; végül $u = c; v = b$ esetén $m \mid (ac+cb)-(bc+bd) = ac-bd$ adja a $d)$ állítást.

3. Tétel: Ha a, b, k, n egészek, $k \geq 1, n \geq 1$, akkor teljesülnek rá a következők:

$a)$ $a - b \mid a^n - b^n$;
$b)$ $a + b \mid a^{2k} - b^{2k}$;
$c)$ $a + b \mid a^{2k-1} + b^{2k-1}$;

Bizonyítás:
$a)$ $a - b \mid a - b$ révén $a \equiv b \pmod{a-b}$, tehát $a^n \equiv b^n \pmod{a-b}$.
$b)$ és $c)$ $a+b \mid a+b$ miatt $a \equiv -b \pmod{a+b}$, tehát $a^n \equiv (-1)^n b^n \pmod{a+b}$, így $a^{2k} \equiv b^{2k} \pmod{a+b}$ és $a^{2k-1} \equiv -b^{2k-1} \pmod{a+b}$.

4. Tétel: Legyenek a, b, c, m egészek, $m \neq 0$, valamint $d = (c, m)$.
Ha $ca \equiv cb \pmod{m}$, akkor $a \equiv b \pmod{\frac{m}{d}}$.

Bizonyítás: A kongruencia definíciója alapján $ca \equiv cb \pmod{m} \iff m \mid (a-b)c$, ami tovább ekvivalens az $\frac{m}{d} \mid (a-b)\frac{c}{d}$ oszthatósággal. Mivel $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$, ezért $\frac{m}{d} \mid (a-b)\frac{c}{d}$ pontosan akkor teljesül, ha $\frac{m}{d} \mid (a-b)$, azaz $a \equiv b \pmod{\frac{m}{d}}$.

5. Tétel: Legyen $c_1, c_2, \cdots, c_m$ teljes maradékrendszer $\pmod{m}$, $a \in \mathbb{Z}$ és $(a, m) = 1$. Ekkor $ac_1, ac_2, \cdots, ac_m$ is **teljes maradékrendszer** $\pmod{m}$.

Bizonyítás: Számuk láthatóan m. Ha $ac_i \equiv ac_j \pmod{m}$, akkor $(a, m) = 1$ miatt a-val egyszerűsíthetünk a modulus változtatása nélkül (lásd 4. Tétel,) így $c_i \equiv c_j \pmod{m}$, tehát $i = j$.

6. Tétel: Legyenek a, b, c rögzített egész számok. Az $ax + by = c$ diofantikus egyenletnek akkor és csak akkor létezik megoldása, ha $(a, b) \mid c$.

Bizonyítás: Először tegyük fel, hogy létezik x_0, y_0 megoldás.Ekkor $(a, b) \mid a$ és $(a, b) \mid b$ alapján szükségképpen

$$(a, b) \mid ax_0 + by_0 = c.$$

Megfordítva tegyük fel, hogy $(a, b) \mid c$, vagyis van olyan t egész, amelyre $(a, b)t = c$. A korábbiak alapján[1] $(a, b) = au+bv$ teljesül alkalmas u, v egészekkel. Ezt az egyenlőséget t-vel beszorozva megkapjuk, hogy $c = a(ut) + b(vt)$, azaz $x = ut, y = vt$ megoldása az $ax + by = c$ diofantikus egyenletnek.

[1]Lásd 2. Fejezet 9. Tétel.

7. Tétel: Legyenek a, b, m egészek, $m \neq 0$. Az $ax \equiv b \pmod{m}$ kongruencia megoldhatóságának szükséges és elégséges feltétele: $(a, m) \mid b$. Ha ez a feltétel teljesül és $x_1 \in \mathbb{Z}$ egy rögzített megoldás: $ax_1 \equiv b \pmod{m}$, akkor az $ax \equiv b \pmod{m}$ minden x egész megoldása felírható $x = x_1 + \frac{m}{(a,m)}k$ alakban, ahol k egész; végül ez a kifejezés minden k egészre valóban megoldást szolgáltat.

Érdemes még kiemelni, hogy az $x \equiv x_1 \pmod{\frac{m}{(a,m)}}$.

8. Tétel ("kis" Fermat-tétel): Tetszőleges p pozitív prímszám esetén érvényesek a következők:

a) ha $a \in \mathbb{Z}$, akkor $a^p \equiv a \pmod{p}$,
b) ha $a \in \mathbb{Z}$ és $(a, p) = 1$, akkor $a^{p-1} \equiv 1 \pmod{p}$.

Bizonyítás: Először a b) állítást bizonyítjuk. Mivel $0, 1, 2, \ldots, p-1$ teljes maradékrendszer mod p, azért $a \in \mathbb{Z}, (a, p) = 1$ esetén $0a, 1a, 2a, \ldots, (p-1)a$ is teljes maradékrendszer az **5. Tétel** szerint. Így az utóbbi számok mod p legkisebb nemnegatív maradékai *sorrendtől eltekintve* éppen $0, 1, 2, \ldots, p-1$, s pontosan az elsőé a 0, tehát $1a, 2a, 3a, \ldots, (p-1)a$ maradékai $1, 2, \ldots, p-1$. Így

$$(1a)(2a)(3a)\ldots((p-1)a) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p},$$

hiszen itt már a sorrend nem okoz bajt. Mivel a $(p-1)!$ relatív prím p-hez, így lehet vele egyszerűsíteni.

Még a-val szorozva, adódik $a^p \equiv a \pmod{p}$, ami éppen az a) állítás, de most még csak $(a, p) = 1$ esetére jött ki. Ha $(a, p) \neq 1$, akkor - mivel p prím - $(a, p) = p$, vagyis $p \mid a, a \equiv 0 \bmod p$, amikor viszont nyilvánvaló az a) állítás.

3.3. Feladatok

1. Feladat: Egy szám háromszorosa 25-tel osztva 4 maradékot ad. Milyen maradékot adhat 25-tel osztva a szám kétszerese?

Megoldás: a számot nevezzük el x-nek.
Tudjuk, hogy $3x = 25k + 4$.
Az előzőekben kimondott tételek alapján felírható:

$$\begin{aligned} 3x &\equiv 4 \pmod{25} \quad \exists \text{ megoldás, mivel } 1 = (3, 25) \mid 4 \text{ igaz.} \\ 3x &\equiv 4 + 25 \cdot 2 \pmod{25} \\ 3x &\equiv 54 \pmod{25} \\ x &\equiv 18 \pmod{\frac{25}{(3;25)}} \qquad (25, 3) = 1 \\ x &\equiv 18 \pmod{25} \end{aligned}$$

$x \equiv 18 \pmod{25}$ -ből a 2. Tétel d) része alapján $[c = d = 2\text{-vel}]$

$2x \equiv 36 \equiv 11 \pmod{25}$ adódik.

Vagyis a szám kétszerese **11** maradékot ad 25-tel osztva.

2. Feladat: Oldjuk meg a $135x^{126} - 90x^{62} - 42x^{24} + 34x^6 \equiv 0 \pmod{13}$ kongruenciát, azaz keressük meg az összes olyan x egész számot, amelyre teljesül a fenti kongruencia.

Megoldás: Mivel a konstans 0, ezért az $x \equiv 0 \pmod{13}$ megoldás.
A továbbaiakban feltesszük, hogy $x \neq 0 + 13t$.

$$\begin{aligned} 5x^{126} + x^{62} - 3x^{24} + 8x^6 &\equiv 0 \pmod{13} \\ x^{13-1} &\equiv 1 \pmod{13} \qquad \text{8. Tétel miatt,} \\ 5x^6 + x^2 - 3 - 5x^6 &\equiv 0 \pmod{13} \\ x^2 &\equiv 3 \pmod{13} \\ x^2 &\equiv 16 \pmod{13} \\ x &= 4 + 13t \\ x &= -4 + 13t \\ x &= 0 + 13t. \end{aligned}$$

3. Feladat: Állítsa elő 983-at egy 21-gyel osztható háromjegyű természetes szám és egy 31-gyel osztható háromjegyű természetes szám összegeként.

Megoldás: a, b háromjegyű természetes szám.
A háromjegyűség miatti korlátok: $99 < a < 1000, 99 < b < 1000$.
$a = 21y, b = 31x$, tehát $983 = 21y + 31x$.
Ebből $21y = 983 - 31x \Longrightarrow 21 \mid 983 - 31x$.

$$\begin{aligned} 983 &\equiv 31x \pmod{21} \\ 17 &\equiv 10x \pmod{21} \\ -4 &\equiv 10x \pmod{21} \qquad \text{mivel } (10,21)=1 \\ -2 &\equiv 5x \pmod{21} \\ 40 &\equiv 5x \pmod{21} \\ 8 &\equiv x \pmod{21} \\ x &= 8 + 21t \end{aligned}$$

Visszahelyettesítve:

$$\begin{aligned} 21y &= 983 - 31 \cdot (8 + 21t) = 735 - 31 \cdot 21t \\ y &= 35 - 31t \end{aligned}$$

$t > 1$ esetén az $a = 21y$ negatív lesz.
$t = 1$ esetén csak kétjegyű lesz.
$t \leq -1$ esetén legalább négyjegyű lesz.
$t = 0$ esetén lesz csak háromjegyű, vagyis $y = 35$, $x = 8 \Longrightarrow$
$a = 31 \cdot 8 = 248, b = 21 \cdot 35 = 735$
A megoldás: **a=248, b=735**.

4. fejezet

Gyorsabb megoldás kongruenciákkal

1. Feladat (Forrás [5.]): x 11-gyel osztva 7, y pedig 9 maradékot ad. Állapítsuk meg $x \pm y$, illetve xy 11-gyel való osztási maradékát!

I.Megoldás (oszthatósággal): $x = 11a + 7, y = 11a + 9$ (a, b egész)
$x + y = 11a + 11b + 16 = (11a + 11b + 11) + 5$. A maradék **5**.
$x - y = 11a + 7 - 11b - 9 = 11a - 11b - 2 = (11a - 11b - 11) + 9$. A maradék **9**.
$xy = (11a + 7)(11b + 9) = 121ab + 77b + 99a + 63 = (121a + 77b + 99a + 55) + 8$. A maradék **8**.

II.Megoldás (kongruenciával): Felírható: $x \equiv 7 \pmod{11}$, $y \equiv 9 \pmod{11}$

$$\begin{aligned} x + y &\equiv 7 + 9 = 16 \pmod{11} \\ x + y &\equiv 5 \pmod{11} \text{ } A \textit{ maradék } \boldsymbol{5}. \\ x - y &\equiv (7 + 11) - 9 \pmod{11} \\ x - y &\equiv 9 \pmod{11} \text{ } A \textit{ maradék } \boldsymbol{9}. \\ xy &\equiv 7 \cdot 9 = 63 \pmod{11} \\ xy &\equiv 8 \pmod{11} \text{ } A \textit{ maradék } \boldsymbol{8}. \end{aligned}$$

2. Feladat (Forrás [5.]): Mi a maradék, ha 2^{100}-t osztjuk 7-tel?

I.Megoldás (oszthatósággal): Nézzük meg az első néhány hatvány maradékát!

a szám	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7
a 7-tel való osztási maradék	1	2	4	1	2	4	1	2

Ez így megy tovább periodikusan, mert: $2^{n+1} = 2^n \cdot 2$, tehát:
2^n maradéka 1 $\Longrightarrow$ 2^{n+1} maradéka 2,
2^n maradéka 2 $\Longrightarrow$ 2^{n+1} maradéka 4,

2^n maradéka $4 \Longrightarrow 2^{n+1}$ maradéka 8, vagyis 1.

Szóval 1 után 2, 2 után 4, 4 után ismét 1 következik.

Mi történik 2^{100}-nál?

Mivel a maradékok **hármasával** ismétlődnek, ezért 100-nál ugyanaz van, mint $(100-3n)$-nél, tehát például $(100-99)$-nél, vagyis 1-nél.

2^1 osztási maradéka 2, így 2^{100} **maradéka is 2**.

Jegyezzük meg, hogy a fentiek szerint 2^n 7-tel való osztási maradéka **kizárólag attól függ**, hogy n **3-mal osztva** milyen maradékot ad.

II. Megoldás (kongruenciával): Felírható: $2^{100} \equiv x \pmod 7$

A **8. Tétel** felhasználásával felírható, hogy: $2^6 \equiv 1 \pmod 7$, ebből:

$$\begin{aligned} (2^6)^{16} &\equiv 1 \pmod 7 \\ 2^{96} &\equiv 1 \pmod 7 \\ 2^4 &\equiv x \pmod 7 \\ 16 &\equiv x \pmod 7 \\ 2 &\equiv x \pmod 7 \end{aligned}$$

Tehát 2^{100} 7-tel való osztási maradéka **2**.

3. Feladat (Forrás: [2.]): Érdekes módon $23+46+12+18=99$ és 99 osztója a számok egymás mellé írásával keletkező 23461218-nak. Tényleg a véletlen játékával állunk szemben?

Megoldás (oszthatósággal): Egy szám csak akkor osztható 99-cel, ha 11-gyel és 9-el is osztható. A vizsgálandó számunk osztható lesz 9-cel[1], mert 2+3+4+6+1+2+1+8 = 27. Egyúttal 11-gyel[2] is osztható, mert $+2-3+4-6+1-2+1-8=-11$. Bárhogy variálhatom ezeket a kétjegyű számokat, a kapott nyolcjegyű szám mindig teljesíteni fogja a 11-gyel való oszthatósági szabályt. Ennek hátterében az a feltétel teljesül, hogy a kétjegyű számok és a nyolcjegyű szám azonos számjegyei megegyeznek -helyiértéknek megfelelően - a 10 kitevőiben (mod 2) felett.

II.Megoldás (kongruenciával): A feladat így is felírható:

$$\begin{aligned} 18\cdot 100^0 + 12\cdot 100^1 + 46\cdot 100^2 + 23\cdot 100^3 &\equiv 0 \pmod{99} \\ 18 + 12\cdot 1 + 46\cdot 1^2 + 23\cdot 1^3 &\equiv 0 \pmod{99} \\ 99 &\equiv 0 \pmod{99} \end{aligned}$$

[1]Lásd 2. fejezet, 4. Tétel.

[2]Lásd ugyanott.

Nem a véletlen játékával állunk szemben, ugyanis a $100^0, 100^1, 100^2, 100^3$-nak mind 1 a 99-cel vett osztási maradéka. Így csak a 18-at, 12-t, 46-ot, 23-at kell összeadnunk és mivel az összeadás kommutatív, ezért bármelyik permutációja a számoknak osztható lesz 99-cel.

4. Feladat (Forrás: [2.]): Bizonyítsuk be, hogy bármilyen k természetes számra: $23 \mid 61^{k+1} + 11^k \cdot 7^{2k} \cdot 3^{3k} \cdot 2^{5k+3}$

Megoldás (oszthatósággal): Teljes indukcióval:
$k = 1$ esetén $23 \mid 61^2 + 11^1 \cdot 7^2 \cdot 3^3 \cdot 2^8 = 3729289$ igaz.
Tegyük fel, hogy k-ra igaz, vagyis $23 \mid 61^{k+1} + 11^k \cdot 7^{2k} \cdot 3^{3k} \cdot 2^{5k+3} =$
$61 \cdot 61^k + 8 \cdot (11 \cdot 49 \cdot 27 \cdot 32)^k$, bizonyítjuk, hogy akkor $(k+1)$-re is igaz.

$$61^{k+2} + 11^{k+1} \cdot 7^{2(k+1)} \cdot 3^{3(k+1)} \cdot 2^{5(k+1)+3} =$$
$$61^2 \cdot 61^k + 11 \cdot 11^k \cdot 49 \cdot 49^k \cdot 27 \cdot 27^k \cdot 256 \cdot 32^k =$$
$$61^2 \cdot 61^k + 3725568 \cdot 465696^k =$$
$$38(61 \cdot 61^k + 8 \cdot 465696^k) + 23(61 \cdot 61^k + 161968 \cdot 465696^k)$$

Az első tag osztható 23-mal az indukciós feltevés miatt, a második tag pedig azért, mert szorzótényezőként szerepel benne.

Megoldás (kongruenciával): Azt kell belátni, hogy

$$61^{k+1} + 11^k \cdot 7^{2k} \cdot 3^{3k} \cdot 2^{5k+3} \equiv 0 \pmod{23}$$

A bal oldalt a **2. Tétel** felhasználásával vele kongruens kifejezésekké alakítjuk, amíg 0-t nem kapunk:

$$\begin{aligned}
61^{k+1} + 11^k \cdot 7^{2k} \cdot 3^{3k} \cdot 2^{5k+3} &\equiv 0 \pmod{23} \\
61 \cdot 61^k + 11^k \cdot 49^k \cdot 27^k \cdot 8 \cdot 32^k &\equiv 0 \pmod{23} \\
61 \cdot (-8)^k + 8 \cdot 11^k \cdot 3^k \cdot 4^k \cdot 9^k &\equiv 0 \pmod{23} \\
61 \cdot (-8)^k + 8 \cdot 22^k \cdot 54^k &\equiv 0 \pmod{23} \\
61 \cdot (-8)^k + 8 \cdot (-1)^k \cdot 8^k &\equiv 0 \pmod{23} \\
(-8)^k \cdot 69 &\equiv 0 \pmod{23} \\
(-8)^k \cdot 23 \cdot 3 &\equiv 0 \pmod{23}
\end{aligned}$$

Beláttuk, hogy **osztható 23-mal**.

Észrevétel: Láthatjuk, hogy az I. megoldásnál nagy számokkal kell számolnunk, ezért nagyobb a tévesztési lehetőség is, valamint sokkal hosszabb a bizonyítása, mint a kongruenciáé. A II. megoldás során gyorsabban bizonyítható az oszthatóság.

Összefoglalás

Reményeim szerint sikerült rövid áttekintést nyerni a számelmélet egy kicsiny részéből. Szakdolgozatom második fejezetében olyan oszthatósági feladatokkal foglalkoztam, melyek felkeltik a gyerekek érdeklődését, próbáltam ezek közül minél több szövegeset, gondolkodtatót feldolgozni. Többféle megoldási módszert is felhasználtam: teljes indukciós bizonyítást, logikus következtetéseket és átalakításokat.

A harmadik fejezetben olyan kongruenciával kapcsolatos problémák szerepelnek, melyeket középiskolai tudással nem, vagy csak nagyon nehezen tudnánk megoldani.

Végül a negyedik fejezetbe gyűjtöttem össze azokat a példákat, amelyek kongruenciával gyorsabb megoldást adnak, mint oszthatósággal.

Köszönetnyilvánítás

Elsősorban Szalay Mihálynak, témavezetőmnek szeretném megköszönni precizitását, útmutatásait, ösztönző leveleit és kitartását velem kapcsolatban.

Továbbá családomnak mind az anyagi, mind a lelki támogatást. Nélkülük nem sikerült volna idáig eljutnom.

Végül, de nem utolsó sorban szaktársamnak, Szalai Gábornak mondok köszönetet, aki időt, fáradtságot nem kímélve mindig a segítségemre volt a technikai részletekben a szakdolgozat megírásakor.

Felhasznált irodalom

[1.] Szalay Mihály : *Számelmélet (középiskolai tankönyv és szakköri füzet).* TYPOTEX, Nemzeti Tankönyvkiadó, 1998.

[2.] Freud Róbert – Gyarmati Edit : *Számelmélet.* Nemzeti Tankönyvkiadó, 2000.

[3.] Sárközy András – Surányi János : *Számelmélet feladatgyűjtemény.* Tankönyvkiadó, 1974.

[4.] Erdős Pál – Surányi János : *Válogatott fejezetek a számelméletből.* Tankönyvkiadó Vállalat, 1960.

[5.] Pósa Lajos: *Összefoglalás.* Műszaki Könyvkiadó,1999.

[6.] Róka Sándor: *2000 feladat az elemi matematika köréből.* TYPOTEX, 2000.