Dr. Szalkai István

Algebra és számelmélet feladatgyűjtemény

A jegyzet az EFOP-3.4.3-16-2016-00009 számú
"A felsőfokú oktatás minőségének és hozzáférhetőségének
együttes javítása a Pannon Egyetemen"
projekt keretében készült.

SZÉCHENYI 2020
MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Regionális Fejlesztési Alap
BEFEKTETÉS A JÖVŐBE

2021.

Algebra és számelmélet feladatgyűjtemény

Dr. Szalkai István

2021. február 11.

Készült,digitális formátumban
21,6 ív terjedelemben

ISBN:978-963-396-186-5

Tartalomjegyzék

Bevezetés

A feladatgyűjteményt elsősorban *informatikai* (IT) szakos hallgatóknak készítettük. Nem csak az általános (absztrakt) algebrai és számelméleti tanulmányokhoz, hanem a titkosírások matematikai alapjainak elsajátításához is. Ahol lehetséges volt, a feladatokat igyekeztünk gyakorlati, algoritmikus szempontból megvizsgálni és, az elméleti algoritmusok megértését is sok feladat részletes kiszámolása segíti. Természetesen más szakok hallgatói és oktatói is sikerrel forgathatják ezt a feladatgyűjteményt.

Témája *absztrakt algebra* (relációk, [elsőrendű] algebrai- és faktor- struktúrák, permutációk, polinomok, véges testek) és *számelméleti algoritmusok* (Euklideszi algoritmus és alkalmazásai, RSA titkosírás). A számelméleti feladatok a 4.2. "*A* $\mathbb{Z}_m$ *maradékosztályok*" és a 4.3. "*Euklideszi gyűrűk*" fejezetekben találhatóak.

A feladatgyűjtemény aránylag vékony (!), hiszen a legtöbb feladathoz *részletes megoldást*, számolást közlünk, ami a könyvnek közel 2/3 -át teszi ki. Ezen kívül sok elméleti definíciót, állítást, tételt, megjegyzést is megtalálhatunk, vagyis tankönyvként is haszonnal forgathatjuk. Név- és tárgymutató, rengeteg lábjegyzet, ábra és táblázat is segíti az anyag megértését. Elméleti segédanyagként elsősorban az $[SzD]$ könyvet ajánljuk.

A feladatok zöme elemi, sőt sok általános- és középiskolai feladattal is találkozhatunk. Természetesen igyekeztünk általános megoldási módszereket ismertetni, amik már nem feltétlenül szólnak elemi iskolásoknak.

Köszönetem fejezem ki kollégáimnak, barátaimnak, akik sok megjegyzésükkel segítették a feladatgyűjtemény létrejöttét: Tarján Klárának, Dósa Györgynek, Hartung Ferencnek és Róka Sándornak. Köszönöm az EFOP-3.4.3-16-2016-00009 azonosító számú pályázat[1)] támogatását is!

[1)] "A felsőfokú oktatás minőségének és hozzáférhetőségének együttes javítása a Pannon Egyetemen"

A könyv szedését, tördelését, nyomtatását LaTeX "*segítségével*" a Szerző saját kezűleg végezte, és örömmel fogad az Olvasóktól bármilyen észrevételt, hibát, javaslatot, megjegyzést.

Veszprém, 2021. február

Dr. Szalkai István
SZALKAI@ALMOS.UNI-PANNON.HU
Pannon Egyetem
Veszprém
Matematikai Tanszék

I. rész

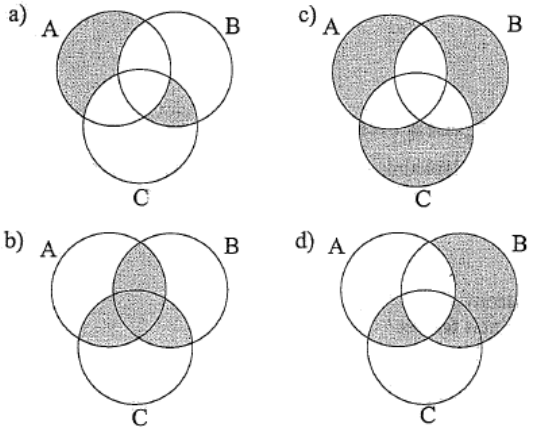
Feladatok

1. fejezet

Halmazok, relációk, függvények

1.1. Halmazok

1.1.0) Az alábbi Venn-diagramokon bejelölt halmazokat írjuk fel az A, B, C halmazok és az $\cup$, $\cap$, — műveletek segítségével[1)]:



1.1.0) feladat

1.1.1) Ábrázoljuk az alábbi halmazokat Venn-diagramon:

a) $(A \backslash B) \cup (C \backslash A)$,

b) $A \cap \overline{B} \cap \overline{C}$,

[1)] lehetőleg a Diszjunktív Normálformának megfelelő alakban

c) $(A \cup \overline{B}) \cap (B \cup C)$,

d) $\left(A \cap \overline{B}\right) \cup C$.

1.1.2) a) Eleme-e x az $U = \{\{x\}, y\}$ halmaznak?

b) Egyszerűsítsük a $V = \{x\} \cup \{\{x\}, y\}$ kifejezést.

c) Hány eleme van a

$$W = \{0, \{0\}, \{0, \{0\}\}, \{0, \{0\}, \{0, \{0\}\}\}\}$$

halmaznak ?

1.1.3) A következő relációk közül melyek igazak:

a) $x \in \{x\}$,

b) $\{x\} \subseteq \{x\}$,

c) $\{x\} \in \{x\}$,

d) $\{x\} \in \{\{x\}\}$,

e) $\emptyset \subseteq \{x\}$,

f) $\emptyset \in \{x\}$,

1.1.4) Igazak-e az alábbi állítások? Ha igen, bizonyítsuk be, ha nem, adjunk ellenpéldát! (X,Y és Z egy adott U alaphalmaz *tetszőleges* részhalmazai.)

a) $X \cap (Y \backslash Z) = (X \cap Y) \backslash (X \cap Z)$,

b) $X \backslash (Y \cup Z) = (X \backslash Y) \cup Z$,

c) $X \backslash (Y \backslash Z) = (X \backslash Y) \backslash Z$,

d) $\overline{X \cap Y} \subseteq X$,

e) $(X \cap Y) \cup (Y \backslash X) = X$, $(X \cap Y) \cup (X \backslash Y) = X$,

f) $(X \cup Y) \cap Z = X \cup (Y \cap Z)$,

g) $(X \cup Y) \cap (Y \cup Z) \cap (Z \cup X) = (X \cap Y) \cup (Y \cap Z) \cup (Z \cap X)$,

h) $Y \backslash Z = Y \cap \overline{Z}$,

i) $X \cup \emptyset = X \cup \{\emptyset\}$.

1.1.5) Igazolja a következő azonosságokat:

a) $(A \cup B) \cap A = (A \cap B) \cup A = A$ (*elnyelési tulajdonságok*),

b) $A \cup B = A \cup (B \backslash A)$,

c) $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$,

d) $A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C)$,

e) $A \backslash (A \backslash B) = A \cap B$,

f) $(A \cup B) \backslash C = (A \backslash C) \cup (B \backslash C)$.

1.1.6) Tetszőleges A, B halmazok esetén legyen

$$A \triangle B := (A \backslash B) \cup (B \backslash A)$$

az A és B halmazok **szimmetrikus differenciá**ja.

a) Igazoljuk az alábbi egyenlőségeket tetszőleges A, B, C halmazokra (azaz $\triangle$ kommutatív, asszociatív és disztributív a $\cap$ műveletre nézve):

$$\begin{aligned} A \triangle B &= B \triangle A \\ A \triangle (B \triangle C) &= (A \triangle B) \triangle C \\ A \cap (B \triangle C) &= (A \cap B) \triangle (A \cap C) \\ A \backslash B &= A \triangle (A \cap B) \end{aligned}$$

b) Mivel egyenlő $A \triangle \emptyset =?$

c) Mely halmazokra teljesülnek az alábbi azonosságok:

$$\begin{aligned} A \triangle B &= \emptyset \\ A \triangle C &= B \triangle C \\ A \cup (B \triangle C) &= (A \cup B) \triangle (A \cup C) \end{aligned}$$

1.1.7) Igazolja a következő azonosságokat (U az univerzális halmazt jelöli):

a) $A \triangle U = \overline{A}$,

b) $(A \cup B) \cap (A \cup \overline{B}) \cap (\overline{A} \cup B) \cap (\overline{A} \cup \overline{B}) = \emptyset$,

c) $\overline{\overline{A \cap B} \cup C} \cup \overline{A \cap \overline{C}} \cup B = \overline{A} \cup B \cup C$,

d) $\overline{\big(\overline{A \cap B} \cup C\big) \cap A} \cup \overline{B} \cup C = U$,

e) ha $A \cap B = \emptyset$ akkor $A \triangle B = A \cup B$,

f) ha $A \subseteq B$ akkor $\overline{A} \supseteq \overline{B}$,

g) ha $A \subseteq B$ akkor $A \cup C \subseteq B \cup C$,

h) ha $A \subseteq B$ akkor $C \setminus A \supseteq C \setminus B$.

1.1.8) Mutassa meg, hogy

a) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$,

b) $\mathcal{P}(A \cup B) = \{C \cup D \,:\, C \in \mathcal{P}(A),\, D \in \mathcal{P}(B)\}$.

1.1.9) Adja meg az $A \times B$ halmazt, ha

a) $A = \{1, 2\}$, $B = \{a, b, c\}$,

b) $A = [1, 2]$, $B = \{2, 3, 5\}$.

1.1.10) Felírhatók-e az alábbi halmazok $A \times B$ alakban? Ha igen, adja meg az A és B halmazokat!

a) $H_1 = \{(1, 2),\ (1, 3),\ (2, 2),\ (2, 3),\ (2, 1),\ (3, 1)\}$,

b) $H_2 = \{(a, 1),\ (b, 1),\ (a, 2),\ (b, 2),\ (c, 2),\ (c, 1)\}$.

1.1.11) Mutassa meg, hogy

a) $(A \cup B) \times C = (A \times C) \cup (B \times C)$,

b) $(A \cap B) \times C = (A \times C) \cap (B \times C)$,

c) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$,

d) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

1.1.12) Adjon meg *öt* (minőségileg) független halmazt[2)] az

$\mathbb{I}_{32} = \{0, 1, ..., 31\}$ halmazon!

(Ld. még [*SzI*] 1. fejezetét is.)

[2)] **Definíció:** az $A_1, ..., A_k$ halmazok **minőségileg függetlenek**, ha tetszőleges $\varepsilon_1, ..., \varepsilon_k \in \{+1, -1\}$ esetén $A^{\varepsilon_1} \cap ... \cap A^{\varepsilon_k} \neq \emptyset$ ahol $A^{+1} = A$ és $A^{-1} = \bar{A}$. □

1.2. Relációk

A relációk különböző tulajdonságainak definícióit és elnevezéseit pl. $[SzSzGy]$ összeállításának 3. és 4. részének (16)-(49) pontjaiban találhatjuk meg, http://www.ontologia.hu/therelthe.pdf (ellenőrizve 2021.02.06.)

1.2.1) Adja meg az alábbi relációk[3)] alaphalmazát és típusát:

a1) n prímszám, páros egész szám,

b1) x negatív valós szám,

c1$_0$) a sík/tér egy pontja illeszkedik egy egyenesre/síkra,

c1) a sík/tér két pontja *kollineáris* (egy egyenesbe esnek),

d1) a sík/tér *három* pontja kollineáris,

e1) a tér négy pontja *koplanáris* (egysíkú),

f1) $\underline{u_1}, \ldots, \underline{u_k} \in V$ lineárisan független vektorok a V vektortérben,

g1) $A \subsetneqq B$ ahol A, B tetszőleges halmazok,

h1$_1$) $A \subsetneqq B$ ahol $A, B \subsetneqq X$ egy adott $X \neq \emptyset$ rögzített halmaz részhalmazai,

h1$_2$) $|A| \leq |B|$ ahol $A, B \subsetneqq X$ egy adott $X \neq \emptyset$ rögzített halmaz részhalmazai,

---

[3)] Néhány forrás még az alábbi fogalmakat is használja:

Definíció: (i) ρ (**kétváltozós/bináris**) **reláció** (*az A halmazon*), *ha* $\rho \subseteq A \times A$, *és* ρ (**n-változós/n-ary**) **reláció**, *ha* $\rho \subseteq A^n$.

(ii) ρ **megfeleltetés** *az A halmazból a B halmazba, ha* $\rho \subseteq A \times B$.

(iii) ρ **leképezés** (**függvény**) *az A halmazról a B halmazba, ha $\rho \subseteq A \times B$ megfeleltetés, továbbá minden $a \in A$ elemhez pontosan egy $b \in B$ található, amelyre* $(a, b) \in A \times B$. *Ekkor használhatjuk a* $\rho : A \to B$ *jelölést.*

(iv) ρ **parciális** *leképezés (függvény), ha $\rho \subseteq A \times B$ leképezés és* $Dom(\rho) \subseteq A$.
ρ **teljes** *leképezés (függvény) ha* $Dom(\rho) = A$.
A parciális függvényekre használatos a $\rho : A \hookrightarrow B$ *jelölés is.*

(v) *Egy (tetszőleges) A halmaz elemeit* **konstansoknak** *hívjuk.*

(vi) ρ (**n-változós/n-ary) művelet**, *ha* $\rho : A^n \to A$ *teljes leképezés (függvény). A 0-változós műveleteket* **konstansoknak** *szokás hívni.* □

Mi egyszerűen **relációnak** hívjuk $A \times B$ és A^n minden részhalmazát, illetve függvényeknél (általában) nem teszünk különbséget parciális és teljes függvények között.

i1$_1$) $f = \mathcal{O}(g)$ ("nagy Ordó")[4],

i1$_2$) $f(x) \approx g(x)$ (aszimptotikusan egyenlő függvények[5]).

A következő relációkban $x, y \in \mathbb{N}$ természetes számok:

j1) x és y *relatív prímek*[6],

k1) $x \sim_k y$ ha $3 \mid x + y$,

l1) $x \sim_\ell y$ ha $x \mid 2 - y$,

m1) $x \sim_m y$ ha $x = y^2$,

n1$_i$) $x \sim_{ni} y$ ha $i \mid x^2 - y^2$ $(i = 1, 2, 3, ...$ esetén) ,

o1$_i$) $x \sim_{oi} y$ ha $i \nmid x^2 - y^2$ $(i = 1, 2, 3, ...$ esetén) .

1.2.2) Vizsgálja meg az *előző* feladatban szereplő *és* az alábbi *bináris* relációk tulajdonságait (reflexív, irreflexív, szimmetrikus, antiszimmetrikus, tranzitív, teljes, ekvivalencia, rendezés, sűrű- ill. jól-rendezés). Az ekvivalencia relációk esetében adja meg az ekvivalencia osztályokat (a partíciót) és egy lehetséges reprezentáns-rendszert (az alaphalmaz faktorizációját) is!

a2) $H :=$ egy osztály tanulói, $X \sim_a Y$ ha egyneműek,

b2) $E :=$ emberek, $X \sim_b Y$ ha barátok,

c2) $F :=$ földrajzi nevek, $X \sim_F Y$ ha az X város az Y folyó partján épült,

d2) $C :=$ városok, $X \sim_C Y$ ha az X várost vízi út köti össze az Y várossal,

e2) $V :=$ egy gráf csúcsai, $X \sim_c Y$ ha van út X és Y között,

f2$_1$) $a \mid b$ ha $a, b \in \mathbb{Z}$ egész számok és a osztója b -nek,

f2$_2$) $a \mid b$ ha $a, b \in \mathbb{N}$ természetes számok,

---

[4] **Definíció:** *Tetszőleges* $f, g : \mathbb{N} \to \mathbb{R}_+$ *függvények esetén* $f = \mathcal{O}(g)$ ("**f értéke nagy ordó g**" / "**f is big oh of g**"), *ha valamely fix* $c_1, c_2 \in \mathbb{R}$ *számokra teljesül a* $c_1 \cdot g(n) < f(n) < c_2 \cdot g(n)$ *egyenlőtlenség minden elég nagy* $n \in \mathbb{N}$ *számra.* □

[5] **Definíció:** $f(x) \approx g(x)$ ha $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$. □

[6] **Definíció: i)** $x, y \in \mathbb{Z}$ **relatív prímek** *ha* $lnko(x, y) = 1$.
ii) *Az* $x_1, ..., x_k \in \mathbb{Z}$ **számok páronként relatív prímek**, *ha* $lnko(x_i, x_j) = 1$ *minden* $i \neq j$ *esetén.* □

f2$_3$) $a \lhd b$ ha $\mathfrak{p}(a) \subseteq \mathfrak{p}(b)$ ahol $\mathfrak{p}(x)$ jelöli x prímosztóinak *halmazát* ($a, b \in \mathbb{N}$ természetes számok),

g2$_1$) $a \equiv_m b$ ("a *kongruens* b *-vel*") ha $m \mid a-b$, ahol $a, b, m \in \mathbb{Z}$ egész számok, m rögzített,
(vizsgálja meg külön az $m = 0$, $m = 1$ speciális eseteket),

g2$_2$) $a \bowtie b$ ha a és b prímosztóinak *halmaza* megegyezik: $\mathfrak{p}(a) = \mathfrak{p}(b)$, ahol $a, b \in \mathbb{Z}$ egész számok,

h2$_1$) $a \sim_m b$ ha $|a-b| \leq m$ ($a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ tetszőleges rögzített),
(vizsgálja meg külön az $m = 0$ és $m \neq 1$ eseteket),

h2$_2$) $a \sim_{h2} b$ ha $0 \leq a - b \leq 6$ ($a, b \in \mathbb{Z}$),

i2$_1$) $a \sim_{i1} b$ ha $lnko(a, b) = 1$ ("relatív prímek", $a, b \in \mathbb{N}$),

i2$_2$) $a \sim_{i2} b$ ha $lnko(a, b) = 1$ ($a, b \in \mathbb{Z}$),

j2) $e \parallel f$ ha az e és f síkbeli/térbeli egyenesek párhuzamosak,

k2) $u \parallel v$ ahol $u, v \in V$ egy (tetszőleges) $V \neq \{\emptyset\}$ vektortér vektorai[7)],

l2) $x \sim_{\mathbb{Q}} y$ ha $x, y \in \mathbb{R}$ valós számok és $x - y \in \mathbb{Q}$,

m2) $A \sim B$ ha $A, B \in \mathbb{R}^{n\times n}$ hasonló[8)] mátrixok,

n2) $\iota := \{ (a, a) \mid a \in A \}$ (**egyenlőség**),

o2) $\mathcal{U} := A \times A$ (**teljes/univerzális reláció**), A tetszőleges halmaz,

p2$_1$) $A \sim_{p1} B$ ha az A és B síkidomok *végszerűen egyenlőek*[9)],

p2$_2$) $A \sim_{p2} B$ ha az A és B síkidomok *hasonlóak*,

[7)] **Definíció:** Az $u, v \in V$ (absztrakt) vektorok **párhuzamosak**, vagyis $u \| v$, ha $u = \lambda v$ vagy $v = \mu u$ valamely $\lambda \in \mathbb{R}$ vagy $\mu \in \mathbb{R}$ valós számra. □
Például: $\sin(3x) \nparallel e^{3x}$ és $\sin(3x) \nparallel 7\sin(3x) + 2$ de $\sin(3x) \| 7\sin(3x)$.

[8)] **Definíció:** *Tetszőleges $A, B \in \mathbb{R}^{n\times n}$ négyzetes mátrixok* **hasonlóak**, *jelben $A \sim B$, ha $B = C \cdot A \cdot C^{-1}$ valamely $C \in (\mathbb{R}^{n\times n})^*$ invertálható mátrixra.* □

[9)] Bolyai Farkas **Definíció**ja: *Két* síkidom **végszerűen egyenlő**, *ha véges számú, páronként egybevágó darabokra (diszjunkt részhalmazokra) oszthatók.*
Más szavakkal: *bármelyik síkidomot ollóval feldarabolhatjuk (nem csak egyenes vágásokkal) úgy, hogy a részekből a másik síkidom kirakható.* □
Bolyai Farkas **Tétele**: *Bármely két, azonos területű* sokszög *végszerűen egyenlő.* □

p2$_3$) $A \sim_{p3} B$ ha az A és B síkidomok *egybevágóak*,

p2$_4$) $A \sim_{p4} B$ ha az A és B síkidomok *területe egyenlő.*

q2$_1$) $a \sim_0 b$ ha *van olyan* $c > 0$ valós szám amelyre $|\frac{a}{b}| < c$ és $|\frac{b}{a}| < c$,

q2$_2$) tetszőleges $c > 0$ *rögzített* valós számra

$a \sim_c b$ ha $|\frac{a}{b}| < c$ és $|\frac{b}{a}| < c$,

r2$_1$) $|a| = |b| \quad (a, b \in \mathbb{R})$,

r2$_2$) $|a| = |b| \quad (a, b \in \mathbb{C})$,

s2) $a^2 = b^2 \quad (a, b \in \mathbb{R})$,

t2) $a < b - 1 \quad (a, b \in \mathbb{R})$,

u2$_1$) $n - m$ *páros* $(m, n \in \mathbb{Z})$,

u2$_2$) $n - m$ *páratlan* $(m, n \in \mathbb{Z})$,

v2) p és q azonos fokú polinomok,

w2) p fokszáma $\leq q$ fokszáma,

x2$_1$) e és f egymást metsző síkbeli egyenesek,

x2$_2$) e és f egymásra merőleges síkbeli egyenesek,

x2$_3$) e és f olyan síkbeli egyenesek, melyek egyenlő távol vannak az origótól,

y2) $\mathcal{R}_X := \{(A, B) : A, B \subseteq X,\ A \cap B \neq \varnothing\} \subset \mathcal{P}(X) \times \mathcal{P}(X)$

ahol X tetszőleges, adott nemüres halmaz,

z2) $\mathcal{R}_{X,xo} := \{(A, B) : A, B \subseteq X,\ A \cap B \ni x_0\} \subset \mathcal{P}(X) \times \mathcal{P}(X)$

ahol X tetszőleges, adott nemüres halmaz és $x_0 \in X$ rögzített.

1.2.3) Tekintsük az $A := \{1, 2, 3, 4, 5\}$ halmazt és a rajta értelmezett

a) $\rho := \{\ (1, 2), (2, 4), (4, 3), (5, 2)\ \}$,

b) $\rho := \{\ (1, 2), (1, 3), (2, 5), (4, 2)\ \}$

relációt. Rajzolja fel a ρ, ρ^2, ρ^3 relációk *irányított* gráfját! Adja meg a ρ reláció tranzitív lezártját[10)] és rajzolja fel annak irányított gráfját is.

[10)] **Definíció:** *Egy* $\rho \subseteq A \times A$ *bináris reláció* **hatványai**: $\rho^1 := \rho$,
$\rho^{i+1} := \rho^i \circ \rho = \{(a, b) \in A \times A\ :\ \exists c \in A :\ (a, c) \in \rho^i$ *és* $(c, b) \in \rho\}$ $(i \in \mathbb{N})$,
és **tranzitív lezártja** $\overline{\rho} := \bigcup\{\rho^i : i \in \mathbb{N}\}$ □

1.2.4) Legyen $D_n := \{k \in \mathbb{N} \,:\, k \mid n,\, 2 \leq k\}$ és tekintsük a D_n halmazon az $\mid$ ("osztója") rendezési relációt. Rajzolja fel a D_{30} , D_{27} , D_{56} , D_{60} , D_{80} és a $D_{24} \cap D_{27}$ rendezett halmazok diagramját! Van-e legkisebb, legnagyobb, minimális, maximális elemük? Ha igen, adja meg az összeset!

1.2.5) Adjon példát (rajzolja fel a gráfját) olyan részben rendezett halmazra, amelynek

a) pontosan három minimális eleme van,

b) egy minimális eleme van, de nincs legkisebb eleme,

c) két minimális és két maximális eleme van.

1.2.6) Tekintsük az $A := \{1, 2, 3, 4, 5\}$ halmazt és azon a

a) $\rho := \{(1, 2), (1, 3), (3, 4)\}$,

b) $\rho := \{(1, 2), (2, 4), (5, 3), (4, 1)\}$,

c) $\rho := \{(1, 2,), (2, 4), (5, 3), (4, 5,)\}$

relációt.

Kiterjeszthető-e ρ részbenrendezéssé A -n? Ha igen, adjon meg *két különböző* kiterjesztést, és ábrázolja ρ és kiterjesztéseinek irányított gráfjait és Hasse -diagramjait. Ha nem, indokolja!

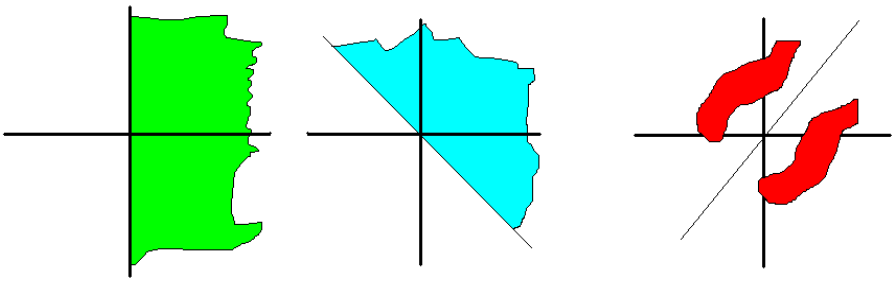
Kiterjeszthető-e ρ *teljes* rendezéssé A -n? Ha igen, adjon meg kiterjesztéseket és ábrázolja a relációkat.

1.2.7) Rajzolja fel az alábbi $\rho \subseteqq \mathbb{R}^2$ *relációk gráfjait*:

a) $x = y$, $x < y$, $x \leq y$,

b) $x \equiv_m y$ $(x, y, m \in \mathbb{Z}$ egész számok) .

1.2.8) Az alábbi rajzon mely $\tau \subseteqq \mathbb{R}^2$ relációk gráfjait láthatjuk? Adjuk meg a megadott relációk tulajdonságait!



1.2.9) Hogyan olvashatók le relációk gráfjairól a relációk tulajdonságai (mint pl. reflexív, szimmetrikus, teljes, antiszimmetrikus, stb.) ?

1.2.10) Keressen olyan relációt, amely

a) reflexív, szimmetrikus de nem tranzitív,

b) reflexív, nem szimmetrikus és nem tranzitív,

c) reflexív, antiszimmetrikus és nem tranzitív,

d) nem reflexív, szimmetrikus de nem antiszimmetrikus és tranzitív,

e) nem reflexív, nem szimmetrikus de tranzitív.

1.2.1. Ekvivalenciák

1.2.11) Igazolja, hogy az alábbi relációk *ekvivalenciák*. Adja meg az osztályokat is egy-egy reprezentánsukkal együtt.

a) $\{(m,n) \in \mathbb{N}^2 \ : \ m-n$ osztható 3-mal$\}$

b) $\{(e,f) \ : \ e$ és f síkbeli egyenesek, távolságuk az origótól egyenlő$\}$

c) $\{(P,Q) \ : \ P$ és Q síkbeli pontok, távolságuk a sík egy fix egyenesétől egyenlő$\}$

d) $\{(P,Q) \ : \ P$ és Q síkbeli pontok, távolságuk a sík egy fix *pontjától* egyenlő$\}$

e) legyen X egy (tetszőleges) halmaz, és legyen

$\{(A,B) : A,B \subseteq X, \ |A| = |B|$ ha mindkettő véges; vagy mindkettő végtelen$\}$.

1.2.12) Adja meg az 1.2.1) és 1.2.2) feladatokban szereplő *ekvialencia-relációk* által meghatározott partíciókat és ekvivalencia-osztályokat!

Keressen a fenti relációk között finomabb és durvább relációkat!

1.2.13) Legyen $R \subset (\mathbb{Z}^- \times \mathbb{Z}^-)^2$ a következő reláció:

$$(a,b) \ R \ (c,d) \quad \overset{def}{\Leftrightarrow} \quad ad = bc \quad .$$

Mutassa meg, hogy R ekvivalenciareláció, és

$$\left(\mathbb{Z}^- \times \mathbb{Z}^-\right) \ / \ R \quad \cong \quad \mathbb{Q}\backslash\{0\} \quad .$$

1.2.14) Legyen $W \leq V$ rögzített altér a V vektortérben.

a) Mutassa meg, hogy $\Pi := \{W + y \mid y \in V\}$ *partíció*ja V -nek ,

b) Adja meg az $x \sim_\Pi y$ relációt.

1.2.15) a) Vizsgálja meg a különböző *modulusok*hoz tartozó $\equiv_m$ relációk kapcsolatát (tartalmazás szempontjából), azaz melyik *finomabb,* melyik *durvább*[11] ?

b) Mely $A \subseteqq \mathbb{R}$ részhalmaz esetén lesz a $\sim_A \subseteqq \mathbb{R}^2$ reláció ekvivalencia, ha tetszőleges $x, y \in \mathbb{R}$ valós számok esetén

$$x \sim_A y \overset{def}{\iff} x - y \in A \quad .$$

1.2.16) a) Jelölje $\mathcal{K}$ azon konvergens számsorozatok halmazát, amelyeknek véges sok eleme 0 , és tekintsük $\mathcal{K}$ -n a következő relációt: legyen $(a_n) \leftrightsquigarrow (b_n)$ pontosan akkor, ha $\lim\limits_{n\to\infty} \dfrac{a_n}{b_n} = 1$. Mutassa meg, hogy $\leftrightsquigarrow$ ekvivalencia reláció $\mathcal{K}$ -n, és adja meg $\leftrightsquigarrow$ ekvivalencia osztályait.

b) Jelölje $\mathcal{S}$ az összes (tetszőleges) számsorozat halmazát és tekintsük $\mathcal{K}$ -n a következő relációt: legyen $(a_n) \backsim (b_n)$ pontosan akkor, ha $\lim\limits_{n\to\infty} \dfrac{a_n}{b_n} \in \mathbb{R} \setminus \{0\}$ létezik (azaz a két sorozat **ekvikonvergens** Weierstrass[12] szerint.) Ekvivalencia reláció-e $\backsim$ az $\mathcal{S}$ halmazon, és ha igen, akkor adja meg ekvivalencia osztályait.

1.2.17) Vizsgálja meg, hogy a 3.2. "*Speciális elemek félcsoportokban*" fejezet 3.2.8) feladatában szereplő reláció mely struktúrákban ekvivalencia, és adja meg az ekvivalenciaosztályokat ezekben a struktúrákban!

---

[11] **Definíció:** az $R, S \subseteqq A^n$ relációk közül R **finomabb** mint S , vagyis S **durvább** mint R ha $R \subseteqq S$, azaz xRy esetén xSy . *Másképpen:* R osztályai részhalmazai S osztályainak: $[a]_R \subseteqq [a]_S$ minden $a \in A$ esetén. □

[12] Karl Theodor Wilhelm Weierstraβ (1815-1897) német matematikus, a modern függvényelmélet (analízis) egyik megalapozója.

1.2.2. Rendezések

1.2.18) Az alábbi relációk közül melyek rendezések, teljesek, sűrű- ill. jól-rendezések? Melyikben van legkisebb/minimális/legnagyobb/maximális elem?

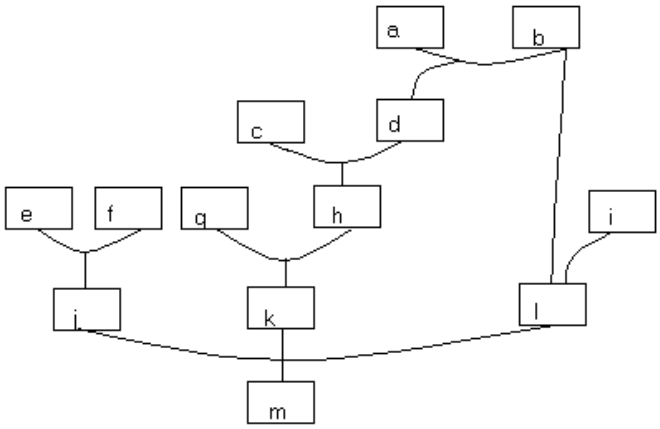
a) $< \text{ és } \leq \subseteq \mathbb{R}^2$, $\leq \subseteq \mathbb{Q}^2$,

b) $\leq \subseteq \mathbb{N}^2$ és $\leq \subseteq \mathbb{Z}^2$,

c) $|_{\mathbb{N}} \subseteq \mathbb{N}^2$ és $|_{\mathbb{Z}} \subseteq \mathbb{Z}^2$ (oszthatóság) ,

d) $\underline{x} \ll \underline{y}$ ha $x_i \leq y_i$ minden $i \leq n$, $\underline{x}, \underline{y} \in \mathbb{R}^n$ esetén (komponensenkénti rendezés),

e)



1.2.18)e) feladat

1.2.19) Van-e legkisebb/minimális/legnagyobb/maximális elem az 1.2.1) és 1.2.2) feladatokban található rendezett halmazokban? Adja meg ezeket az elemeket!

1.2.20) Rajzolja fel az alábbi rendezési relációk gráfjait:

a) $A_3 = \{1, 2, 3\}$ és $A_4 = \{1, 2, 3, 4\}$ halmazok *részhalmazainak* a $\subseteq$ reláció szerinti hálóját (vagyis a $(P(A_3), \subseteq)$ és $(P(A_4), \subseteq)$ rendezett halmazok gráfjait),

b) $N_{40} = \{1, 2, 3, ..., 40\}$ halmaz $|$ (oszthatóság) reláció.

1.2.21) Legyenek $x_1 < x_2 < x_3 < x_4 < x_5$ tetszőleges (nem ismert) különböző valós számok. Tekintsük az

$$A := \{x_i + x_j : 1 \leq i < j \leq 5\}$$

alaphalmazon a szokásos $\leq$ rendezést. Rajzolja fel az $(A, \leq)$ rendezett halmaz gráfját!

1.2.22) Keressünk a szokásostól eltérő *rendezési* relációkat az $\mathbb{N}$, $\mathbb{Z}$ és $\mathbb{R}$ számhalmazokhoz.

1.2.23) a) Tegye teljessé az $| \subset \mathbb{N}^2$ (oszthatóság) parciális rendezést (azaz adjon meg *legalább egy* teljes kiterjesztését a $|$ rendezésnek)!

b) Tegye teljessé az 1.2.1) és 1.2.2) feladatokban található rendezési relációkat!

1.2.24) Adja meg az $(\mathbb{N}, \ | \ )$ és $(\mathbb{R}, \leq)$ rendezett halmazokban tetszőleges véges H részhalmaz supremumát és infimumát!

1.2.25) Adjon meg három olyan egész számot, melyek relatív prímek de nem páronként relatív prímek[13)]

1.2.26) Az alábbi $(A, \leq)$ rendezett halmazokban adja meg az A alaphalmaz

$$H_{\leq}(a) := \{x \in A \mid x \leq a\}$$

részhalmazait, majd vizsgálja meg a megadott műveletek és relációk, valamint a $H_{\leq}$ halmazok közötti halmazműveletek kapcsolatait:

a) $(\mathbb{R}, \leq)$, $+, \leq$, **b)** $(\mathbb{N}, \ | \ )$, $\cdot$, $\div$, $lnko$, $lkkt$.

1.2.27) Legyen $\mathcal{A} = \{f : \mathbb{N} \to \mathbb{R}\}$ $(Dom\,(f) = \mathbb{N})$ és $f, g \in \mathcal{A}$ esetén legyen $f \lhd g$ ha valamely $n_0 \in \mathbb{N}$ küszöbtől kezdve (vagyis $n_0 \leq n$ esetén) $f\,(n) \leq g\,(n)$.

a) Tekinthető-e a $\lhd$ reláció rendezésnek? Parciális vagy teljes?

b) Igaz-e, hogy: *bármely* $f, g \in \mathcal{A}$ *kompatibilis* alulról vagy felülről $\lhd$ szerint (vagyis: $(\forall f, g \in \mathcal{A})\ (\exists h, k \in \mathcal{A})\ (h \lhd f \wedge h \lhd g)$ illetve $(f \lhd k \wedge g \lhd k)$).

[13)] **Definíció: (i)** *Az* $a, b \in \mathbb{Z}$ *egész számok* **relatív prímek**, *ha* $lnko(a, b) = 1$.

(ii) *Az* $a_1, a_2, ..., a_t \in \mathbb{Z}$ *egész számok* **relatív prímek**, *ha* $lnko(a_1, a_2, ..., a_t) = 1$. *Ezek a számok* **páronként relatív prímek**, *ha* $lnko(a_i, a_j) = 1$ *minden* $i, j \geq t$ *indexpárra.* □

1.3. Függvények, műveletek

Ebben a fejezetben a függvényeket (nem csak $\mathbb{R} \to \mathbb{R}$) algebrai szempontból vizsgáljuk, "algebrai" függvényekről szólunk. A feladatok előtt érdemes most röviden összefoglalnunk a függvények "szokásos" (pl. analízisbeli) és algebrai *jelölései* közötti különbségeket.

Egy $f : A \to B$ függvény és $x \in A$, $y \in B$, $f : x \mapsto y$ esetén a szokásos írásmód $y = f(x)$, míg algebrai jelöléssel $y = xf$.

Ha $f : A \to B$ és $g : B \to C$, akkor a $h : A \to C$ összetett függvény (f és g kompozíciója) szokásos írásmódban $h = g \circ f$ és képlete $h(x) = g(f(x))$, vagyis $(g \circ f)(x) = g(f(x))$. *Ugyanezt* algebrai alakban így írjuk[14)]: $h = f \cdot g$ vagy $h = fg$, és h képlete $xh = (xf)\, g$, vagyis $x(fg) = (xf)\, g$. Érdemes még felrajzolni h -t Venn diagramokkal is, valamint átgondolni a 3.1.8) feladatot és részletes megoldását.

Természetesen abban a speciális esetben, ha az f és g függvények **kommutálnak** (felcserélhetőek), vagyis ha $f \circ g = g \circ f$, az algebrai és analízis jelölések között nincs különbség: $f \circ g = g \circ f = f \cdot g = g \cdot f$.

A fenti megjegyzéseknek többek között a 3.4. "*Szimmetria- és szimmetrikus csoportok*" fejezetben van jelentősége.

1.3.1) Adja meg a $\rho := \{(x, y) \mid y = x^2\} \subset \mathbb{Z} \times \mathbb{Z}$ reláció értelmezési tartományát és értékkészletét! Parciális leképezés ill. leképezés-e ρ ? Adja meg ρ megfordítását, parciális leképezés ill. leképezés-e ρ^{-1} ?

1.3.2) Legyen $A := \{1, 2, 3, 4\}$, $B := \{a, b, c, d, e\}$, $C := \{+, -, o\}$, és tekintsük a

$$\rho := \{\ (1, b),\ (1, e),\ (3, a),\ (3, b),\ (3, e),\ (4, b),\ (4, d)\ \} \subsetneqq A \times B$$

és a

$$\tau := \{\ (b, +)\ ,\ (b, -)\ ,\ (b, o)\ ,\ (c, +)\ ,\ (c, o)\ ,\ (d, -)\ \} \subsetneqq B \times C$$

relációkat. Ábrázolja ρ -t és τ -t *nyíldiagramon.*

Adja meg a $\rho\tau$, $\rho\rho^{-1}$, $\rho^{-1}\rho$ és $\tau\tau^{-1}$ megfeleltetéseket és nyíldiagramjukat.

1.3.3) Határozza meg az alábbi megfeleltetések értelmezési tartományát és értékkészletét!

[14)] néha előfordul a $h = f \bullet g$ jelölés is

Melyek parciális leképezések illetve leképezések közülük?
Mely megfeleltetések inverze parciális leképezés illetve leképezés közülük?

a) $\{(x,y) \,:\, x \geq y\} \subseteqq \mathbb{Z} \times \mathbb{N}$,

b) $\{(x,y) \,:\, x = y^2\} \subseteqq \mathbb{Z} \times \mathbb{N}_0$,

c) $\{(x,y) \,:\, x^2 = y\} \subseteqq \mathbb{Z} \times \mathbb{Z}$,

d) $\{(x,y) \,:\, x = y^2\} \subseteqq \mathbb{N}_0 \times \mathbb{Z}$,

e) $\{(x,y) \,:\, tg(x) = y\} \subseteqq \mathbb{R} \times \mathbb{R}$,

f) $\{(x,y) \,:\, x$ és y relatív prímek$\} \subseteqq \mathbb{N} \times \mathbb{N}$.

1.3.4) Tekintsük a

a) $\varphi : \mathbb{R} \to [-1,+1]$, $\quad x \longmapsto \sin(x)$,

b) $\varphi : \mathbb{R} \to \mathbb{R}_0^+$, $\quad x \longmapsto x^2$

leképezéseket. Adja meg a leképezések magját[15], azaz a $Ker(\varphi) \subseteqq A \times A$ ekvivalencia relációt, és ábrázolja a síkon.

1.3.5) Ellenőrizze, hogy *ha α másodfokú algebrai egész* szám[16], akkor
a) a

$$\mathbb{Z}[\alpha] := \{x + \alpha \cdot y \mid x, y \in \mathbb{Z}\}$$

halmaz zárt az összeadás, a kivonás és a szorzás műveletekre,

b) a

$$\mathbb{Q}(\alpha) := \left\{ \frac{x + \alpha \cdot y}{u + \alpha \cdot v} \mid x, y, u, v \in \mathbb{Z} \right\}$$

halmaz zárt az összeadás, a kivonás, a szorzás *és az osztás* műveletekre.

1.3.6) Mely $t \in \mathbb{R}$ valós számok esetén lesz a pozitív valós számok halmazán értelmezett

$$x * y := x + y + t\sqrt{xy}$$

---

[15] **Definíció:** *Tetszőleges $\varphi : A \to B$ függvény esetén legyen $Ker(\varphi) := \{(a,b) : \varphi(a) = \varphi(b)\} \subseteq A \times A$ a φ függvény* **magja** (**kernel**). □
$Ker(\varphi)$ mindig ekvivalencia reláció.

[16] **Definíció:** *Az $\alpha \in \mathbb{C}$ komplex (valós) szám* **k-fokú algebrai egész** *szám, ha kielegít egy $\alpha^k + p_{k-1}\alpha^{k-1} + ... + p_0 = 0$ k-fokú (algebrai) egyenletet valamely $p_{k-1}, ..., p_0 \in Z$ egész együtthatókkal.* □

művelet asszociatív[17] ?

1.3.7)** Tetszőleges $r, s \in [0,1] \cap \mathbb{Q}$ racionális számok esetén értelmezzük a számok **köztesét** (vagy **mediánját**)[18]: ha $r = \frac{a}{b}$, $s = \frac{c}{d} \in [0,1] \cap \mathbb{Q}$, $lnko(a,b) = lnko(c,d) = 1$, $b, d > 0$, akkor legyen

$$r \boxtimes s = \frac{a}{b} \boxtimes \frac{c}{d} := \frac{a+c}{b+d} \quad .$$

a)** Ellenőrizzük a művelet alábbi azonosságait (az alábbiakban minden tört *redukált* alakú[19], azaz tovább már nem egyszerűsíthető):

ha $cb - ad = 1$ akkor $\frac{a}{b} < \frac{c}{d}$ és $\frac{a}{b} < \frac{a}{b} \boxtimes \frac{c}{d} < \frac{c}{d}$,

sőt az $\frac{u}{v} = \frac{a}{b} \boxtimes \frac{c}{d}$ jelölés esetén $ub - av = 1$ és $cv - ud = 1$.

b) Vizsgáljuk meg a $\boxtimes$ művelet algebrai tulajdonságait (kommutatív, asszociatív, stb.).

1.3.8)* Legyen

$$\mathbb{Q}_{növ} := \{ f : \mathbb{Q} \to \mathbb{Q} \quad | \quad f \textit{ mon. növő} \text{ és } \mathrm{Im}(f) = \mathbb{Q} \} \quad .$$

Vizsgáljuk meg, hogy ez a halmaz zárt-e a + (összeadás) műveletére.

1.3.9)* Az $y = x^3$ egyenletű síkgörbe (mint az $\mathbb{R}^2$ sík egy részhalmaza) pontjain értelmezzük a következő $*$ műveletet[20]: Ha A és B a görbe két pontja, akkor legyen $A * B$ az AB egyenes és a görbe harmadik metszéspontjának az origóra való tükörképe. (Ha a definícióban szereplő valamelyik két pont egybeesik, akkor összekötő egyenesük helyett vegyük a görbe adott pontbeli érintőjét.)

---

[17] KöMaL F3286.feladata (1999/5, 297.old.), megoldása a 2000/1 szám 34.oldalán.

[18] Ennek a műveletnek a tovább már nem egyszerűsíthető törtek nevezőinek vizsgálatakor van jelentősége (ld. pl. a KöMaL 1999/1 számának 15-21.oldalain Holló-Szabó Ferenc részletes cikkét.)

Ezt jelöli a **Riemann-féle** R **függvény:** $R(x) :=$ *x nevezője* ha x racionális és nem egyszerűsíthető. □

[19] **Definíció:** *Az* $\frac{a}{b} \in \mathbb{Q}$ *tört* **redukált**, *ha tovább már nem egyszerűsíthető, azaz* $lnko(a,b) = 1$. □

[20] A 400 évig megoldatlan **Nagy Fermat Tétel** bizonyításában játszanak fontos szerepet a síkgörbék pontjain végzett ilyen és hasonló műveletek. A modern titkosírások is használják az **elliptikus görbék** feletti hasonló csoportokat.

Mutassuk meg, hogy a $*$ művelet asszociatív[21] !

1.3.10)* Van-e olyan $\bullet : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ művelet, amely teljesíti a következő tulajdonságokat bármely $x, y, z \in \mathbb{R}$ számokra[22] :

a) $x \bullet y = y \bullet x$,

b) $(x \bullet y)z = (xz) \bullet (yz)$,

c) $(x \bullet y) + z = (x + z) \bullet (y + z)$?

1.3.11)* A $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ műveletre teljesül bármely $x, y, z \in \mathbb{R}$ számokra, hogy

$$x * (y + z) = (y * x) + (z * x) \quad .$$

Mutassa meg, hogy $*$ kommutatív[23] !

1.3.12)* Keressük meg azt a $\# : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ műveletet, amelyre minden $x, y \in \mathbb{Z}$ egész szám esetén teljesül, hogy[24]

a) $x\#0 = x$

b) $0\#y = -y$

c) $((x + 1)\#y) + (x\#(y + 1)) = 3(x\#y) - xy + 2y$.

1.3.13)* A $\boxtimes : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ műveletre teljesül minden $x, y, z \in \mathbb{R}$ valós számra:

i) $0 \boxtimes a = a$, **ii)** $a \boxtimes (b \boxtimes c) = c \boxtimes (b \boxtimes a)$.

Mutassa meg, hogy a $\boxtimes$ művelet asszociatív[25].

1.3.14)* A $\otimes : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ műveletre teljesül minden $x, y, z \in \mathbb{R}$ valós számra:

a) $(x \otimes y) \otimes z = x \otimes (y \otimes z)$,

b) $(x \otimes y) \otimes z = (y \otimes z) \otimes x$,

c) Minden $x \neq y$ esetén van olyan $z \in \mathbb{R}$, amelyre .

---

[21] KöMaL F.3278 feladata (1999/3, 170.old.), megoldása a 2000/1, 28.old.
[22] Középiskolai Matematikai Lapok Gy.1632 gyakorlat
[23] Középiskolai Matematikai Lapok Gy.2335 gyakorlat
[24] Középiskolai Matematikai Lapok Gy.2335 gyakorlat
[25] Középiskolai Matematikai Lapok F2364 feladat

Mutassa meg, hogy a $\otimes$ művelet kommutatív[26)].

1.3.15). Legyen $(L, \precapprox)$ egy tetszőleges jólrendezett[27)] halmaz. Vizsgáljuk meg L -en a következő kétváltozós művelet algebrai tulajdonságait:

$$a * b := S(b) \qquad (a, b \in L) \quad .$$

[26)] Középiskolai Matematikai Lapok F2452 feladat

[27)] **Definíció:** az $(L, \precapprox)$ rendezett halmaz **jólrendezett**, ha tetszőleges $A \subseteqq L$ nemüres részhalmazának van minimális eleme. $\square$

Következmények: **(i)** ekkor $(L, \precapprox)$ teljes (azaz lineáris) rendezés.

(ii) ekkor minden $x \in L$ elemnek van ($S(x)$ vagy x^+ -al jelölt) **rákövetkezője (successor):** $x^+ \succapprox x$, $x^+ \neq x$ és L egyetlen eleme sincs x és x^+ között. $\square$

2. fejezet

Általános struktúrák

2.1. Algebrai struktúrák (Algebrák)

2.1.1) Elsőrendű (algebrai) struktúrák-e a következők, és ha igen, mi a típusuk? Ha nem, miért nem? (A műveletek zártságát ne feledjük ellenőrizni!)

a) $\mathcal{R} := (\mathbb{R}, +, -, \cdot, \div)$, $\mathcal{R}_{\leq} := (\mathbb{R}, +, -, \cdot, \div, \leq)$,

b) $\mathcal{R}_1 := (\mathbb{R}, \sin, 0)$,

c) $\mathcal{R}_2 := (\mathbb{R}, +, \cdot, \ln, \lneq, 0)$,

d) $\mathcal{R}^n_+ := (\mathbb{R}^n, +)$ (vektorok összeadása),

e) $\mathcal{R}^n := (\mathbb{R}^n, +, \cdot)$ (vektortér),

f) $\mathcal{R}^{n\times n} := (\mathbb{R}^{n\times n}, +, \cdot)$ (mátrixok),

g) $\mathcal{A} := (A, \leq)$ ($A \neq \emptyset$ tetszőleges rendezett halmaz),

h) $\mathcal{P}_X := (P(X), \cup, \cap, \ \dot{-}\ , \emptyset, X, \subset)$ ($X \neq \emptyset$ tetszőleges halmaz),

i) $\mathcal{G} := (V, E)$ (gráf),

j) $\mathcal{P}_{\mathbb{P}} := (\mathbb{P}, \cdot)$,

k) $\mathcal{O} := (\emptyset, *, \emptyset)$,

l) $(\mathbb{N}, *)$ ahol $x * y := xy - x + y$,

m) $(\mathbb{N}_0, *)$ ahol $x * y := xy - x + y$,

n) $(\mathbb{Z}[\sqrt{2}], \circ)$ ahol $x \circ y := x^2 + y \cdot \sqrt{2}$,

o) $(A, \cap)$ ahol $A = \{\{a\}, \{b\}, \{a, b\}, \{a, c\}, \{a, b, c\}\}$,

p) $(A, \cup)$ ahol $A = \{\{a\}, \{b\}, \{a, b\}, \{a, c\}, \{a, b, c\}\}$.

2.1.2) írja fel az alábbi struktúrák művelettáblázatait (ún. *Cayley-tábla*):

a) $(\mathbb{Z}_5, \oplus)$ ahol $m \oplus n := m + n$ 5-tel való osztási *maradéka*,

b) $(\mathbb{Z}_5, \cdot)$,

c) $(A, \triangle)$ ahol $A = \mathcal{P}(\{a, b\}) := \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$,

d) $(\{i, h\}, \Rightarrow)$,

e) $(\mathbb{Z}_3, +) \times (\mathbb{Z}_4, +)$ és $(\mathbb{Z}_{12}, +)$,

f) $(\mathbb{Z}_2, +) \times (\mathbb{Z}_4, +)$ és $(\mathbb{Z}_8, +)$.

2.1.3) Határozza meg a $(\mathbb{Z}_p, +)$, $(\mathbb{Z}_m, +)$, $(\mathbb{Z}_p, \cdot)$, $(\mathbb{Z}_m, \cdot)$, $\left(\mathbb{Z}_p^*, \cdot\right)$, $(\mathbb{Z}_m^*, \cdot)$ struktúrák *részstruktúráit* ($p \in \mathbb{P}$ prímszám, $m \in \mathbb{N}$ összetett).

2.1.4) Mutassa meg, hogy $\mathbb{R}^{\mathbb{R}}$ alábbi részhalmazai részstruktúrái $\left(\mathbb{R}^{\mathbb{R}}, \circ\right)$-nak:

a) $\mathbb{R}[x]$, **b)** $\mathbb{R}^{\mathbb{R}}_{Lin}$, **c)** $\mathbb{R}^{\mathbb{R}}_{LinRac}$

2.1.5) Mutasson példát olyan struktúrákra, amelyeknek nincs (valódi) részstruktúrája!

2.1.6) Határozza meg az alábbi struktúrák adott részhalmazainak generátumait:

a) $\{2\} \subset (\mathbb{Z}_6, +)$, $\{2\} \subset (\mathbb{Z}_6, \cdot)$

b) $\{10\} \subset (\mathbb{Z}_{12}, +)$, $\{10\} \subset (\mathbb{Z}_{12}, \cdot)$

c) $\{9\} \subset (\mathbb{Z}_{12}, +)$, $\{2\} \subset (\mathbb{Z}_6, \cdot)$

d) $\{4\} \subset (\mathbb{Z}_{13}, +)$, $\{4\} \subset (\mathbb{Z}_{13}, \cdot)$

2.1.7) Mutassa meg, hogy $n \in \mathbb{Z}_m$ pontosan akkor generátoreleme $(\mathbb{Z}_m, +)$ -nak, ha n és m relatív prímek.

2.1.8) Döntse el, hogy az alábbi struktúrák közül melyek végesen generáltak ill. ciklikusak:

a) $(\mathbb{Z}_{12}, +)$, $(\mathbb{Z}_{12}, +) \times (\mathbb{Z}_{12}, +)$,

b) $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$.

2.2. Homomorfizmusok, kongruenciák, faktorok

2.2.1) Homomorfizmusok-e az alábbi függvények a megadott struktúrák között? Melyik beágyazás, izo- vagy automorfizmus?

a) $\alpha : (\mathbb{N}, +, \cdot) \to (\mathbb{N}, +, \cdot)$, $\alpha : n \mapsto 2n$,

b) $\beta : (\mathbb{N}, |) \to (\mathbb{N}, |)$, $\beta : n \mapsto 2n$,

c) $\gamma : (\mathbb{Z}, |) \to (\mathbb{N}, |)$, $\gamma : m \mapsto |m|$,

d) $\delta : (\mathbb{N}, |) \to (\mathbb{N}, \leq)$, $\delta : n \mapsto n$,

e) $\varepsilon : (\mathbb{Z}_6 \times \mathbb{Z}_9, +, \cdot) \to (\mathbb{Z}_{54}, +, \cdot)$, $\varepsilon : (i, j) \mapsto i \cdot j$,

f) $\varphi : (\mathbb{Z}_6 \times \mathbb{Z}_7, +, \cdot) \to (\mathbb{Z}_{42}, +, \cdot)$, $\varphi : (i, j) \mapsto i \cdot j$,

g) $\rho : (\mathbb{Z}[\sqrt{2}], +, \cdot) \to (\mathbb{Z}[\sqrt{2}], +, \cdot)$, $\rho : a + b\sqrt{2} \mapsto a - b\sqrt{2}$,

h) $\vartheta : (\mathbb{Z}[\sqrt{2}], +) \to (\mathbb{Z}^2, +)$, $\vartheta : a + b\sqrt{2} \mapsto (a, b)$,

i) $\iota : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_m, +, \cdot)$, $\iota : k \mapsto k$ -nak m -el való osztási maradéka,

j) $\zeta : (\mathbb{R}, +, \cdot) \to (\mathbb{C}, +, \cdot)$, $\zeta : x \mapsto x$.

2.2.2) Mutassa meg, hogy az alábbi leképezések valóban homomorfizmusok. Melyek izomorfizmusok ?

a) $\varphi_1 : (\mathbb{Z}, \cdot) \to (\mathbb{N}_0, \cdot)$, $n \longmapsto |n|$,

b) $\varphi_2 : (\mathbb{Z}, +) \to (\mathbb{Q}, \cdot)$, $n \longmapsto 2^n$,

c) $\varphi_3 : (\mathbb{R}_+, \cdot) \to (\mathbb{R}, +)$, $x \longmapsto \log(x)$,

d) $\varphi_4 : (\mathbb{Q}[\sqrt{3}], +) \to (\mathbb{Q}[i], +)$, $x + y\sqrt{3} \longmapsto x + yi \quad (x, y \in \mathbb{Q})$,

e) $\varphi_5 : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_5, +, \cdot)$, $n \longmapsto n$ *-nek* 5 *-tel való osztási maradéka*,

f) $\varphi_6 : (\{i, h\}, \Leftrightarrow, \vee) \to (\mathcal{P}(X), \triangle, \cap)$, $i \longmapsto \emptyset$, $h \longmapsto X$

2.2.3) A $H_{\leq}(a)$ halmazok különböző változatait ld. az 1.2 *Relációk* fejezet 1.2.26) feladatában.

2.2.4) a) Adja meg a fenti feladatokban található *izomorfizmusok* inverzét!

b) Izomorfak-e az előző alfejezet 2.1.2) e) illetve f) pontjában szereplő struktúrák?

2.2.5) Kongruenciareláció-e (algebrai[1)] értelemben) az alábbi példákban megadott $\theta \subseteq A \times A$ ekvivalencia reláció az $\mathfrak{A} = (A, ...)$ struktúrákban, és ha igen, mi az általa nyert $A/_\theta$ faktorhalmaz és a $\mathfrak{A}/_\theta$ faktorstruktúra?

a) $\mathfrak{A} = (\mathbb{Z}, +, \cdot)$ és $\theta = \equiv_m \subseteq \mathbb{Z} \times \mathbb{Z}$ (számelméleti kongruencia-reláció),

b) $\mathfrak{A} = (\mathbb{Z}, +, \cdot)$ és $\theta = \bowtie \subseteq \mathbb{Z} \times \mathbb{Z}$ (ld. előző fejezet 1.2.2)g2_2)).

[1)] **Definíció:** *Egy* $\mathfrak{A} = (A, f_1, ..., f_m, R_1, ..., R_n)$ *struktúra* A *alaphalmazán értelmezett* $\theta \subseteq A \times A$ *ekvivalenciareláció* **algebrai kongruencia (reláció),** *vagy* **kompatibilis osztályozás** *ha*

(i) tetszőleges $i \leq m$, $\tau = \tau_i$, $x_1, ..., x_\tau, y_1, ..., y_\tau \in A$, $x_k \theta\, y_k$ $(k = 1, ..., \tau)$ esetén $f(x_1, ..., x_\tau)\ \theta\ f(y_1, ..., y_\tau)$,

(ii) tetszőleges $j \leq n$, $\pi = \pi_j$, $x_1, ..., x_\pi, y_1, ..., y_\pi \in A$, $x_\ell \theta\, y_\ell$ $(\ell = 1, ..., \pi)$ esetén $(x_1, ..., x_\tau) \in R_j \iff (y_1, ..., y_\tau) \in R_j$. $\square$

3. fejezet

Félcsoportok és csoportok

3.1. Gruppoidok, félcsoportok

3.1.1) Asszociatívok-e, kommutatívok-e az alábbi műveletek:

o) Valós számok alapműveletei, halmazműveletek ($\cup$, $\cap$, $\setminus$, Δ),

a) $a \diamond b := a + b + ab \qquad (a, b \in \mathbb{R})$,

b)[1] $a \otimes b := a \cdot b + \sqrt{(a^2 - 1) \cdot (b^2 - 1)} \qquad (a, b \in [1, \infty))$,

c) $a \boxtimes b := \frac{a+b}{1-ab} \qquad (a, b \in (0, 1))$,

d) $lnko(m, n) :=$ m és n legnagyobb közös osztója $\qquad (m, n \in \mathbb{Z})$,

e) $lkkt(m, n) :=$ m és n legkisebb közös többszöröse $\qquad (m, n \in \mathbb{Z})$,

f) $A \setminus B \qquad (A, B \subset X \ , \ X \neq \emptyset$ tetszőleges),

g) $\max(x, y)$, $\min(x, y) \qquad (x, y \in \mathbb{R})$?

3.1.2) Félcsoportot alkotnak-e az alábbi algebrák?

a) $(\mathbb{N}, +)$,

b) $(\mathbb{N}_0, \cdot)$,

c) $(\mathbb{Z}, -)$,

d) $([0, 1], \cdot)$,

e) $(\mathcal{P}(X), \cup)$,

[1] Kömal F.3185 (1998/3, 158.old.)

f) $(\mathcal{P}(X), \setminus)$,

g) $(\{i, h\}, \Leftrightarrow)$,

h) $(\{i, h\}, \Rightarrow)$,

i) $\mathbb{R}_+$ -en $\quad a \odot b := a^b$

j) $\mathbb{R}$ -en $\quad a \oplus b := \frac{a+b}{2}$

3.1.3) Asszociatívok-e ill. kommutatívok-e az alábbi műveletek:

a) az $A = \{a, b, c\}$ halmazon a

*	a	b	c
a	a	a	c
b	a	b	b
c	c	c	a

Cayley- táblázattal megadott művelet ,

b) $(\mathbb{Q}\setminus\{0\}, \circ)$ ahol $\quad x \circ y := \frac{xy}{x+y}$,

c) $(\mathbb{Z}, *)$ ahol $\quad x * y := x + 2y$.

3.1.4) Milyen $f, g \in \mathbb{N}^{\mathbb{N}}$ függvényekre teljesül $\quad f \circ g = g \circ f$?
(Lásd még az 3.1.7) feladatot.)

3.1.5) Mutassa meg, hogy $\mathbb{R}^{n\times n}$ -ben a szorzás művelete asszociatív de nem kommutatív!

3.1.6) Vizsgálja meg az alábbi félcsoportok adott részhalmazait, hogy azok *rész-félcsoportok* illetve *csoportok* -e:

a) $(\mathbb{R}^{n\times n}, \cdot)$ -ben $\quad \mathbb{R}^{n\times n}_{\triangle}$, $\mathbb{R}^{n\times n}_{\setminus}$, $(\mathbb{R}^{n\times n})^*$, $(\mathbb{R}^{n\times n}_{\triangle})^*$, $\left(\mathbb{R}^{n\times n}_{\setminus}\right)^*$,

b) $(\mathbb{R}[x], \circ)$ -ben $\quad \mathbb{R}^{\mathbb{R}}_{Lin}$, $\mathbb{R}^{\mathbb{R}}_{LinRac}$,

c) $(\mathbb{R}[x], +)$ -ben $\quad \mathbb{R}^{\mathbb{R}}_{Lin}$, $\mathbb{R}^{\mathbb{R}}_{LinRac}$.

3.1.7) Legyen $(A, \circ)$ egy *tetszőleges* félcsoport, és tekintsük A -n a következő binér relációt:

$$x \overset{\circ}{\sim} y \Leftrightarrow x \circ y = y \circ x \quad .$$

Vizsgálja meg a $\overset{\circ}{\sim}$ reláció tulajdonságait

a) általában,

b) a következő struktúrákban:

$\mathcal{R} = (\mathbb{R}, \cdot)$, $\mathcal{R}^{n\times n} = (\mathbb{R}^{n\times n}, \cdot)$, $\mathcal{N}_\circ = (\mathbb{N}^{\mathbb{N}}, \circ)$, $\mathcal{A}_\circ = (A^A, \circ)$.

3.1.8)!) Számítsa ki az alábbi hatványokat a megadott félcsoportokban[2)]:

a) $(\mathbb{R}^{n\times n}, \cdot)$ -ben $(A \cdot B)^5$, például $\left(\begin{pmatrix} 2 & -5 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 7 & 1 \\ 6 & 8 \end{pmatrix}\right)^5$,

b) $\left(\mathbb{R}^{\mathbb{R}}, \circ\right)$ -ben $(f \circ g)^5$, például $(\sin \circ \lg)^5$ vagy $\left(\cos \circ \sqrt{\ }\right)^3$ ("kompozícióhatványok")

c) $(\mathbb{R}[x], \circ)$ -ben $(p(x))^3 = (p \circ p \circ p)(x)$ és $(p(x) \circ q(x))^3 = (p \circ q)^3(x)$, például $p(x) = x^2 + 4x - 5$ és $q(x) = 7 - 9x$,

d) $(\mathbb{R}[x], \cdot)$ -ben $(p(x))^3$ és $(p(x) \cdot q(x))^5$, például a c) -beli polinomokkal,

e) $(\mathbb{C}[x], \cdot)$ -ben $(u)^5$ és $(u \cdot v)^5$, például $u = 2 + i$ és $v = 5 - 3i$.

Lásd még a 3.4."*Szimmetria- és szimmetrikus csoportok*" fejezetben a permutációk hatványaira és felcserélhetőségére vonatkozó feladatokat is.

3.2. Speciális elemek félcsoportokban

3.2.1) Tekintsük az $\mathcal{N}_\circ = \left(\mathbb{N}^{\mathbb{N}}, \circ\right)$ struktúra $g : \mathbb{N} \to \mathbb{N}$, $g : x \longmapsto 2x$ elemét. Döntsük el: nullosztó-e balról/jobbról, invertálható-e balról/jobbról, lehet-e vele jobbról- ill. balról egyszerűsíteni?

3.2.2) Vannak-e az alábbi struktúrákban bal- és jobboldai *zérus-*, *egység-* (=*null-*) illetve *nullosztó* elemek? Mely elemekkel lehet balról vagy jobbról *egyszerűsíteni*? Mely elemeknek van bal- illetve jobboldali *inverze*?

a) $\mathcal{A}_\circ := (A^A, \circ)$, $A \neq \emptyset$ tetszőleges halmaz,

b) $\mathcal{S}_{\mathbb{N}} := (S_{\mathbb{N}}, \circ)$,

c) $\mathcal{Z}^{(\cdot)} := (\mathbb{Z}, \cdot)$, $\mathcal{Z}^{(+)} := (\mathbb{Z}, +)$, $\mathcal{N}^{(\cdot)} := (\mathbb{N}, \cdot)$,

[2)] **A feladat megoldásában részletes magyarázatot találunk a bemutatott műveletek és struktúrák tulajdonságairól!**

d) $\mathcal{Z}_m^{(\cdot)} := (\mathbb{Z}_m, \cdot)$, $\mathcal{Z}_m^{(+)} := (\mathbb{Z}_m, +)$ ($m \in \mathbb{Z}$ tetszőleges[3)] egész szám), $\mathcal{Z}_m^* := (\mathbb{Z}_m^*, \cdot)$, $\mathcal{Z}_p^* := (\mathbb{Z}_p^*, \cdot)$ (p prímszám),

$\mathcal{R}_{2\pi}^{(+)} := (\mathbb{R}_{2\pi}, +)$, $\mathcal{R}_{2\pi}^{(\cdot)} := (\mathbb{R}_{2\pi}, \cdot)$,

e) $\mathcal{R} := (\mathbb{R}^{\mathbb{R}}, \circ)$,

f) $\mathcal{N}_\circ := (\mathbb{N}^{\mathbb{N}}, \circ)$,

g) $\mathcal{R}_{Lin} := (\mathbb{R}_{Lin}^{\mathbb{R}}, \circ)$,

h) $\mathcal{R}_{LinRac} := (\mathbb{R}_{LinRac}^{\mathbb{R}}, \circ)$,

i) $\mathcal{R}^{n\times n} := (\mathbb{R}^{n\times n}, \cdot)$,

j) $\mathcal{F}_X := (X^*, \hat{})$ ahol $x_1x_2...x_n\hat{}\,y_1y_2...y_m := x_1x_2...x_ny_1y_2...y_m$.
(ún. **szabad félcsoport**, free semigroup)

3.2.3) Mutassa meg, hogy az alábbi struktúrák félcsoportok. Van-e egységelem, zéruselem, nullosztó? Ha van egységelem, akkor mely elemek invertálhatóak, és adja meg az invertálható elemek inverzeit is.
(A tetszőleges, rögzített halmaz.) .

a) $(\mathbb{Z}, \circ)$ ahol $x \circ y := x + y + 1$,

b) $(\mathbb{Z}, *)$ ahol $x * y := x + y - xy$,

c) $(\mathcal{I}_A, \circ)$ ahol $\mathcal{I}_A = \{f : A \to A \mid f \text{ injektív}\}$,

d) $(\mathcal{Z}_A, \circ)$ ahol $\mathcal{Z}_A = \{f : A \to A \mid f \text{ szürjektív}\}$,

e) $(\mathcal{P}(X), \cap)$.

3.2.4) Tekintsük a valós számokon az

$$x \diamond y := x + y + xy \quad (x, y \in \mathbb{R})$$

kétváltozós műveletet.

a) Mutassuk meg, hogy $(\mathbb{R}, \diamond)$ kommutatív félcsoport.

b) Keressük meg ebben a félcsoportban az egységelemet, zéruselemet, nullosztókat, az invertálható elemek inverzeit.

[3)] az $m = 1$ és $m = 0$ eset külön vizsgálatot igényel!

c) Igaz-e, hogy az $(\mathbb{R}\backslash\{-1\}, \diamond)$ struktúra Abel[4]-csoport[5]?

3.2.5) Keressünk *idempotens* elemeket[6] az alábbi struktúrákban:

o) $(2\cdot\mathbb{Z}, \cdot)$ (a páros egész számok multiplikatív félcsoportja) ,

a) $(\mathbb{Z}_m, \cdot)$ tetszőleges $m \in \mathbb{Z}$ egész számra (pl. $m = 10$, ...) ,

b) $(\mathbb{R}^{n\times n}, \cdot)$,

c) $\left(\mathbb{R}^{\mathbb{R}}, \circ\right)$,

d) $\mathcal{S}_{\mathbb{R}}$, $\mathcal{S}_{\mathbb{N}}$, $\mathcal{S}_n$,

e) síkbeli geometriai transzformációk $\left(=\left(A^A, \circ\right)\right.$ ahol $\left.A = \mathbb{R}^2\right)$,

f) $(P(X), \cup)$, $(P(X), \cap)$ (X tetszőleges halmaz) ,

g) $(G, \cdot)$ (*tetszőleges* G multiplikatív *csoport*) .

3.2.6) Keressünk *involutorius* műveleteket[7] (!) az alábbi halmazokon:

$P(X)$, $\mathbb{C}$, $\mathbb{R}$, $\{i, h\}$, $\mathbb{R}^2$, $\mathbb{R}^3$, ...

3.2.7) Mely $f \in A^A$ függvény lesz önmaga inverze?

3.2.8)* Keressen az alábbi félcsoportokban *kommutáló* elemeket[8] ! Van-e a félcsoportnak olyan eleme, amely *minden* elemmel kommutál?

a) $\mathcal{A}_\circ := (A^A, \circ)$, **b)** $(\mathbb{R}^{n\times n}, \cdot)$.

---

[4] **ABEL, Niels Henrik** (1802-1829), norvég matematikus. Többek között igazolta, hogy az 5 -öd és magasabb fokú egyenleteket megoldó gyökképletek *nem* léteznek (ún. "*Abel-Ruffini-Bolyai János*" -tétel).

[5] A *kommutatív* csoportokat hívják **Abel-csoportoknak.** □

[6] **Definíció:** $x \in S$ **idempotens elem** a $\cdot$ műveletre nézve, ha $x^2 := x \cdot x = x$ (ahol $(S, \cdot)$ félcsoport) .
A $\cdot$ **művelet idempotens**, ha S minden eleme idempotens a $\cdot$ műveletre. □

[7] **Definíció:** az $f : A \to A$ *egyváltozós művelet* **involutorius**, ha $f^2(a) = f(f(a)) = a$ *minden* $a \in A$ elemre. □

[8] **Definíció:** Tetszőleges $(S, \cdot)$ félcsoport $x, y \in S$ elemei **kommutálnak**, ha $x \cdot y = y \cdot x$. □

3.3. Csoportok

3.3.1) Csoportot alkotnak-e az alábbi struktúrák?

a) $(\mathbb{N}, +)$,

b) $(\mathbb{Q}\backslash\{0\},\ /\ )$,

c) $(\{i, h\}, \Longleftrightarrow)$,

d) $(\{i, h\}, \wedge)$,

e) $(\mathcal{P}(X), \cup)$,

f) $(\mathcal{P}(X), \triangle)$,

g1) $\left(\mathbb{R}^{\mathbb{R}}_{Lin}, \circ\right)$ = az $ax + b$ alakú lineáris függvények halmaza, a $\circ$ kompozíció műveletével,

g2) ugyanaz, mint az előző, de csak az $a \neq 0$ feltételnek eleget tevő függvényeket tekintjük,

h) $(H, \circledcirc)$ ahol $H = \{A, B, C, S\}$ egy szabályos háromszög csúcsai és súlypontja, továbbá legyen:

(súlypont) $\circledcirc$ (csúcspont) := (ez a csúcspont) ,

(csúcspont) $\circledcirc$ (önmaga) := (súlypont) ,

(súlypont) $\circledcirc$ (súlypont) := (súlypont) ,

(egyik csúcspont) $\circledcirc$ (másik csúcspont) := (harmadik csúcspont) .

3.3.2) írja fel a $(\mathbb{Z}_5, +)$, $(\mathbb{Z}_5, \cdot)$ és a $(\mathbb{Z}_6, \cdot)$ struktúrák művelettábláit. Melyek alkotnak csoportot?

3.3.3) Mutassa meg, hogy az alábbi struktúrák csoportot alkotnak:

a) $(A, *)$ ahol $A = \{a, b, c\}$ és

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

,

b) $(\mathcal{H}_2, \cdot)$ ahol $\mathcal{H}_2 := \{2^n : n \in \mathbb{Z}\}$,

c) $(\mathbb{Z} \times \mathbb{R}_+, *)$ ahol $(a, b) * (c, d) := (a + c, bd)$,

d) $(\mathcal{H}_4, \circ)$ ahol $\mathcal{H}_4 := \{f_1, f_2, f_3, f_4\}$ a következő $f_i : \mathbb{R} \to \mathbb{R}$ függvényekkel:

$$f_1(x) = x, \quad f_2(x) = \frac{1}{x}, \quad f_3(x) = -x, \quad f_4(x) = \frac{-1}{x} \quad ,$$

e) $\mathcal{D}_3$ (a szabályos ABC háromszög önmagára történő egybevágósági transzformációinak csoportja, az ún. 3-rendű *diédercsoport*) .

3.3.4) Vizsgálja meg az alábbi csoportok adott részhalmazait, hogy azok *részcsoportok* -e, adja meg az általuk meghatározott bal- és jobboldali *mellék osztályokat*[9]. Melyek *normálosztók*[10] közülük?
(Lásd még a 3.4.3. feladatot.)

a) $(\mathbb{R}^2, +)$ -ben (sík) $\mathbb{R}^1$ (origón átmenő egyenes),

b) $(\mathbb{R}^{n\times n}, +)$ -ben $\mathbb{R}^{n\times n}_{\triangle}$, $\mathbb{R}^{n\times n}_{\setminus}$, $(\mathbb{R}^{n\times n})^*$, $(\mathbb{R}^{n\times n}_{\triangle})^*$, $\left(\mathbb{R}^{n\times n}_{\setminus}\right)^*$,

c) $(\mathbb{R}^{n\times n}, \cdot)^*$ -ben $(\mathbb{R}^{n\times n})^*$, $(\mathbb{R}^{n\times n}_{\triangle})^*$, $\left(\mathbb{R}^{n\times n}_{\setminus}\right)^*$,

d) $(\mathbb{Z}, +)$ -ban (m) [11]

3.3.5) a) írja fel $\mathbb{Z}^*_{20}$ elemeit.

b) Zárt-e ez a halmaz a szorzásra (és miért)?

c) Számítsa ki elemeinek rendjét!

d) Adja meg a vizsgált elemek által generált részcsoportokat.

e) Mutassa meg, hogy minden elemnek van multiplikatív inverze (azaz $(\mathbb{Z}^*_{20}, \cdot)$ csoport).

---

[9] **Definíció:** Egy $(G, \cdot)$ csoport $H \leq G$ részcsoportja *szerinti* **jobb-** ill- **baloldali mellékosztályai** a $H\cdot a := \{h \cdot a : h \in H\}$ ill. az $a\cdot H := \{a \cdot h : h \in H\}$ részhalmazok, ahol $a \in G$ tetszőleges elem. □

[10] **Definíció:** Egy $(G, \cdot)$ csoport $H \leq G$ részcsoportja **normális részcsoport**, vagy röviden **normálosztó**, ha a H szerinti jobb- és baloldali mellékosztályok megegyeznek, azaz $\forall a \exists b\ H \cdot a = b \cdot H$ és $\forall b \exists a\ H \cdot a = b \cdot H$. Ennek jelölése: $H \lhd G$. □

[11] **Definíció:** *Tetszőleges $m \in \mathbb{Z}$ egész számra* $(m) := \{m \cdot x : x \in \mathbb{Z}\}$
az m által **generált főideál** $\mathbb{Z}$ *-ben (m többszörösei).* □

3.3.6) Az alábbi csoportokban[12)] adja meg az adott a elem által generált (ciklikus[13)]) részcsoportot, és határozza meg $o(a)$ -t, azaz az a csoportelem rendjét[14)]:

a) $(\mathbb{C}, +)$, $a = i$,

b) $(\mathbb{Z}, +)$, $a = 2$,

c) $(\mathbb{Q}\backslash\{0\}, +)$, $a = 2$,

d) $(\mathcal{H}_2, \cdot)$, $a = 1/4$,

e) $(\mathbb{Z} \times \mathbb{R}_+, *)$, $a = (1, 3)$,

f) $(\mathcal{H}_4, \circ)$, $a = f_2$,

g) $\mathcal{D}_3$, $a =$ az A csúcson átmenő tengelyre való tükrözés,

h) $\mathcal{D}_3$, $a =$ a középpont körüli 120^o -os forgatás.

3.3.7) a) Melyek $(\mathbb{C}\backslash\{0\}, \cdot)$ -ban a végesrendű elemek ?

b) Tekintsük az

$\mathcal{M}_{[0,1]} := \{f : [0, 1] \to [0, 1]$ intervallumon monoton növő függvények halmaza$\}$

függvényhalmazt a kompozíció $\circ$ műveletével. Melyek $\left(\mathcal{M}_{[0,1]}\ ,\ \circ\right)$ -ban a végesrendű elemek ?

3.3.8) Részcsoportot alkotnak-e a *páratlan nevezőjű* törtek[15)] az összeadásra nézve (azaz részcsoportja-e a $(\mathbb{Q}, +)$ struktúrának) ?

3.3.9) a) Legyenek $A, B, C \in \mathbb{R}^{n\times n}$ tetszőleges adott invertálható mátrixok. Vannak-e olyan $X, Y \in \mathbb{R}^{n\times n}$, szintén invertálható mátrixok, amelyekre

$$A \cdot X \cdot B \cdot C \cdot X = A \cdot B \cdot X \quad \text{illetve} \quad Y \cdot A \cdot Y = B \cdot B \cdot A^{-1} \quad ?$$

[12)] a jelöléseket lásd a 3.3.3) feladatban

[13)] **Definíció:** *Az egy elemmel generálható csoportokat* **ciklikus** *-nak hívjuk. Az a elem által* **generált** *részcsoport* $[a] := \{a^n : n \in \mathbb{Z}\}$. □
Állítás: $|[a]| = o(a)$. □ Tehát $[a]$ lehet véges halmaz is.

[14)] **Definíció:** *Tetszőleges $a \in G$ csoportelem* **rendje** $o(a)$ *jelöli a legkisebb $m \in \mathbb{N}$ számot (ha van ilyen) amelyre $a^m = 1$, és $o(a) := \infty$ ha nincs ilyen $m \in \mathbb{N}$ szám.* □

[15)] Pontosabban az összes olyan törtre gondolunk, amelyek *felírhatók* páratlan nevezővel is (mint pl. 2/6 felírható 1/3 alakban is) .

Ha igen, számítsuk ki az $X, Y \in \mathbb{R}^{n\times n}$ mátrixokat!

b) Legyenek $a, b, c : \mathbb{R} \to \mathbb{R}$ tetszőleges adott invertálható függvények. Vannak-e olyan $f, g : \mathbb{R} \to \mathbb{R}$, szintén invertálható függvények, amelyekre

$$a(f(b(c(f(x))))) = a(b(f(x))) \quad \text{illetve} \quad g(a(g(x))) = b(b(a^{-1}(x))) \quad (\forall x \in \mathbb{R})$$

vagy olvashatóbban:

$$a \circ f \circ b \circ c \circ f = a \circ b \circ f \quad \text{illetve} \quad g \circ a \circ g = b \circ b \circ a^{-1} \quad ?$$

Ha igen, számítsuk ki az $f, g \in: \mathbb{R} \to \mathbb{R}$ függvényeket!

c) Legyen $(G, \cdot)$ egy tetszőleges csoport, $a, b, c \in G$ tetszőleges adott elemek. Oldjuk meg az

$$axbcx = abx \quad \text{és} \quad yay = bba^{-1}$$

egyenleteket ($x, y \in G$ ismeretlenek) !

Egyértelmű-e a megoldás? Adjon meg legalább egy megoldást !

3.3.10) írja fel a $(\mathbb{Z}_3, +)\times(\mathbb{Z}_4, +)$ struktúra Cayley tábláját! Ciklikus-e ez a struktúra?

3.3.11) a) írja fel a $(\mathbb{Z}_4, +)$ és a $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ struktúrák művelettábláit! Izomorf-e a két struktúra?

b) Izomorfak-e a $(\mathbb{Z}_4, +)$ és $(\mathbb{Z}_2, +) \times (\mathbb{Z}_4, +)$ struktúrák?

c) Izomorf-e a $(\mathbb{Z}_{12}, +)$ és a $(\mathbb{Z}_3, +) \times (\mathbb{Z}_4, +)$ struktúra? Adjon meg konkrét izomorfizmust a két struktúra között!

d) Általában mikor izomorfak a $(\mathbb{Z}_m, +)\times(\mathbb{Z}_n, +)$ és $(\mathbb{Z}_{mn}, +)$ struktúrák?

3.3.12) Sorolja fel az összes (például) 12 , 15 , 19 , 20 , 27 és 30 elemű kommutatív (Abel) csoportot!

3.3.13) Adja meg a következő *Abel-csoportok* exponenseit: $(\mathbb{Z}_m[x], +)$, $(\mathbb{Z}_m^*, +)$, $(\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +)$.

3.3.14) Sorolja fel a legfeljebb 20 elemű *tetszőleges* csoportokat!

3.4. Szimmetria- és szimmetrikus csoportok

3.4.0) Keressen gyakorlati példákat permutációkra.

3.4.1) Adja meg az alábbi mértani alakzatok *szimmetria-* (vagy *transzformáció-*) csoportjait[16]:

a) szabályos (síkbeli) sokszögek,

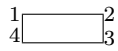
b) háromszögek, téglalap, parallelogramma, szimmetrikus- és általános trapéz, általános négyszög, kör,

c) szabályos (térbeli) testek,

d) téglatest, parallelepipedon, henger, kúp, gömb, stb.

3.4.2) a) Adja meg az előző feladatban szereplő síkbeli *sokszögek* szimmetriacsoportjait az S_n szimmetrikus csoport részcsoportjaiként.

b) A téglalap milyen transzformációját írja le az $\binom{1\,2\,3\,4}{1\,4\,3\,2}$ permutáció? (A csúcsokat körbejárva számozzuk az 1,2,3,4 számokkal az ábra szerint.)



3.4.3) a) Írja fel az $\mathcal{S}_3$ szimmetrikus csoport elemeit és *művelettábláját.*

b) Keresse meg a három- és kételemű ciklusokat (transzpozíciókat[17]).

c) Tekintsük S_3 következő részhalmazát:

$$H := \left\{ id, \binom{1\,2\,3}{2\,1\,3} \right\} \quad .$$

Mutassa meg, hogy $H \leq S_3$ (részcsoport).

d) Adja meg a H szerinti jobb- és baloldali mellékosztályokat! Normálosztó-e ez a részcsoport[18] ?

---

[16] Az $S_{\mathcal{A}}$ **szimmetria-** és S_n **szimmetrikus-** *csoportokat* nem szabad összetévesztenünk: minden $S_{\mathcal{A}}$ részcsoportja valamely S_n -nek.

$S_{\mathcal{A}}$ másik neve **transzformáció csoport**, S_n másik neve **permutációcsoport**.

[17] a kételemű ciklusokat hívjuk **transzpozíciók**nak (szó szerint: át-helyezés)

[18] A normálosztók definíciója a 3.3.4. feladat lábjegyzetében található.

3.4.4) Sorolja fel A_4 elemeit[19]! Általában, hány eleme van A_n -nek?

3.4.5) Az alábbi permutációkat bontsa fel diszjunkt (idegen) *ciklusok* szorzatára, illetve a felbontott permutációkat írja vissza hagyományos alakba. Minden elem pályáját (trajektória, orbit) is határozza meg!

$\sigma_1 = \binom{1\,2\,3\,4\,5}{5\,1\,2\,3\,4}$, $\sigma_2 = \binom{1\,2\,3\,4\,5}{3\,2\,1\,5\,4}$,

$\sigma_3 = \binom{1\,2\,3\,4\,5\,6}{4\,2\,1\,3\,6\,5}$, $\sigma_4 = \binom{1\,2\,3\,4\,5\,6}{5\,1\,2\,6\,3\,4}$,

$\sigma_5 = \binom{1\,2\,3\,4\,5\,6\;\;7\,8\,9\,10\,11\,12\,13\,14\,15}{5\,1\,8\,6\,4\,2\,14\,3\,7\,12\,15\,10\,13\,11\;\;9}$,

$\sigma_6 = \binom{1\,2\,3\,4\,5\,6\;\;7\,8\,9\,10\,11}{2\,4\,1\,5\,8\,3\,10\,9\,6\;\;7\,11}$,

$\sigma_7 = (6,4,1,3,7,5)$, $\sigma_8 = (2,4,1,3) \circ (7,8)$,

$\sigma_9 = (1,2,5,10,4,3) \circ (6,11,8,16,19) \circ (12,9,14,18,20,15) \circ (13,17)$,

$\sigma_{10} = (2,4,1,3)(5)(7,8)$.

3.4.6) Hány ciklus (azaz *ciklikus permutáció*) van S_n -ben?

3.4.7) A 3.4.5) feladatban szereplő permutációknak keressük meg az inverzeit.

3.4.8) Számítsa ki a $\rho = \binom{1\,2\,3\,4\,5\,6\,7}{3\,2\,7\,1\,6\,4\,5}$ és a $\sigma = \binom{1\,2\,3\,4\,5\,6\,7}{7\,5\,6\,3\,4\,1\,2}$ permutációk hatványait.

3.4.9) Legyen $\tau := (1,2) \circ (3,5,4)$. Számítsa ki a τ^{25} és a τ^{26} permutációkat.

3.4.10) Legyen $\sigma := \binom{1\;\;2\;\;3\;\;4\;\;5\;\;6\;\;7\;\;8\;\;9\;10\;11\;12\;13\;14\;15\;16\;17\;18\;19\;20}{2\;\;5\;\;1\;\;3\;10\;11\;\;7\;12\;14\;\;4\;16\;\;9\;17\;18\;\;8\;19\;13\;20\;\;6\;15}$.

a) Számítsa ki a következő hatványokat: σ^2, σ^5, σ^{18}, σ^{83}, σ^{547}, σ^{5048}, ...

b) Számítsa ki σ rendjét.

3.4.11) Számítsa ki az alábbi permutáció -hatványokat:

$\binom{1\,2\,3\,4\,5\,6\,7}{5\,4\,1\,6\,3\,7\,2}^{63}$, $\binom{1\,2\,3\,4\,5\,6}{1\,4\,6\,5\,2\,3}^{53}$, $\binom{1\,2\,3\,4\,5\,6}{4\,2\,1\,3\,6\,5}^{95}$.

---

[19] **Definíció:** Tetszőleges $n \in \mathbb{N}$ esetén $A_n := \{\pi \in S_n : sgn(\pi) = +1\}$ a páros permutációk részhalmaza, az ú.n. **alternáló** (rész-) **csoport**. □

3.4.12) Adja meg a σ^{-1}, σ^2, τ^{-1}, τ^3, $\tau\circ\sigma$ és a $\sigma\circ\tau$ permutációkat[20], ha

a) $\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\5&1&2&3&4\end{smallmatrix}\right)$, $\tau = \left(\begin{smallmatrix}1&2&3&4&5\\3&2&1&5&4\end{smallmatrix}\right)$,

b) $\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6\\4&2&1&3&6&5\end{smallmatrix}\right)$, $\tau = \left(\begin{smallmatrix}1&2&3&4&5&6\\5&1&2&6&3&4\end{smallmatrix}\right)$,

c) $\sigma = (1,5,3,2)\circ(2,5,4)\circ(1,3)$, $\tau = (4,3,1)\circ(1,3,2)\circ(3,1,4)$,

d) rajzolja fel grafikusan a σ és τ permutációkat, és adja meg az egyes elemek pályáit[21] .

3.4.13) o) Legyen $\rho = \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&0\\3&2&5&4&1&6&9&8&7&0\end{smallmatrix}\right)$ és $\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&0\\1&8&3&0&5&4&7&2&9&6\end{smallmatrix}\right)$. Ciklusokra bontás *nélkül* számolja ki a $\rho\sigma$ és $\sigma\rho$ permutációkat, és magyarázza meg a tapasztalt jelenséget!

a) Adjunk meg olyan ρ,σ permutációkat, amelyek *nem* diszjunktak[22] de kommutálnak, azaz $\rho\sigma = \sigma\rho$.

b) Igaz-e, hogy ha két permutáció kommutál, akkor a közösen mozgatott elemeket ugyanúgy mozgatják[23]?

3.4.14) Vannak-e olyan $\rho,\sigma,\tau \in S_3$ permutációk, amelyre

a) $\rho^2 = (1,3,2)$, **b)** $\sigma^2 = (1,3)$, **c)** $\tau^2 = (1,2,3,4,5,6,7,8,9)$?

Ha igen, adjon meg egy ilyen σ permutációt[24], ha nem, akkor indokolja, hogy miért nem létezik. (Lásd még a 3.4.20. feladatot.)

3.4.15) Keresse meg a következő permutációk rendjét[25]:

a) $\sigma = (2,4,1,3)(7,8)$,

---

[20] ne feledjük a 1.3. "*Függvények, műveletek*" fejezet elején írt megjegyzéseket az algebrai és a "szokásos" jelölésekről.

[21] **Definíció:** *Adott $\sigma \in S_H$ permutáció esetén egy $a \in H$ elem* **pályája /orbit / trajektória** *σ szerint:* $T_\sigma(a) := \{\sigma^n(a) \mid n \in \mathbb{Z}\}$ $\square$
az a elem által "befutott/érintett" elemek halmaza, a σ permutáció "hatására".

[22] pontosabban: a mozgatott elemek $M(\rho)$ és $M(\sigma)$ halmazai diszjunktak: $M(\rho)\cap M(\sigma) = \emptyset$.

[23] vagyis: ha $M(\rho)$ és $M(\sigma)$ a mozgatott elemek halmaza, $H = M(\rho)\cap M(\sigma)$, és $f|H$ jelöli az f függvény leszűkítését a H halmazra, akkor $\rho|H = \sigma|H$?

[24] a β permutációt α **négyzetgyökének** hívjuk, ha $\beta^2 = \alpha$.

[25] A definíciót lásd a *csoportelem rendje* címszónál.

b) $\pi = (1,2,7,3)(4,8,5)$,

c) $\rho = (1,7,6)(4,8)(2,5,9,10,3)$,

d1) $\tau = t$ -hosszúságú ciklus,

d2) $\xi = \sigma_1\sigma_2...\sigma_k$ ahol σ_i egy t_i -hosszúságú ciklus ha $i = 1,...,k$.

3.4.16) a) Keressen **maximális rendű** permutációkat S_n -ben ($n \leq 20$).

b) Keressen maximális rendű permutációkat S_{100} -ban.

3.4.17) Bontsa fel *transzpozíciók* szorzatára a következő permutációkat és állapítsa meg előjelüket[26)].

$\sigma_1 = \left(\begin{smallmatrix}1&2&3&4&5&6&7\\5&3&2&6&4&7&1\end{smallmatrix}\right)$, $\sigma_2 = \left(\begin{smallmatrix}1&2&3&4&5\\3&2&1&5&4\end{smallmatrix}\right)$,

$\sigma_3 = \left(\begin{smallmatrix}1&2&3&4&5&6\\4&2&1&3&6&5\end{smallmatrix}\right)$, $\sigma_4 = \left(\begin{smallmatrix}1&2&3&4&5&6\\5&1&2&6&3&4\end{smallmatrix}\right)$,

$\sigma_5 = \left(\begin{smallmatrix}1&2&3&4&5&6&7&8\\3&5&2&8&1&4&6&7\end{smallmatrix}\right)$, $\sigma_6 = \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10&11\\2&4&1&5&8&3&10&9&6&7&11\end{smallmatrix}\right)$,

$\sigma_7 = \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10&11&12&13&14&15\\5&1&8&6&4&2&14&3&7&12&15&10&13&11&9\end{smallmatrix}\right)$,

$\sigma_8 = (6,4,1,3,7,5)$, $\sigma_9 = (2,4,1,3) \circ (7,8)$,

$\sigma_{10} = (1,2,5,10,4,3) \circ (6,11,8,16,19) \circ (13,17) \circ (8,12,9,14,18,20,15)$,

$\sigma_{11} = (5,2,3)$, $\sigma_{12} = (1,3,7,5)$,

$\sigma_{13} = \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9\\3&7&4&1&9&8&6&2&5\end{smallmatrix}\right)$, $\sigma_{14} = \left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10&11\\2&4&1&5&8&3&10&9&6&7&11\end{smallmatrix}\right)$.

3.4.18) Kirakhatók-e az alábbi **15-ös** (**kombinett**[27)]-) játékok?

a)

2	5	1	7
10	3	8	4
15	11	6	
9	12	13	14

b)

12	1	9	4
2		5	10
11	8	3	13
7	15	14	6

[26)] **Definíció:** *Tetszőleges $\sigma \in S_n$ permutáció* **előjele** (=**sgn**(σ) = σ **signuma**) : *a felbontásában szereplő transzpozíciók számának* paritása: $+1$ *jelöli a páros,* -1 *a páratlan esetet.* □ A definíció érvényességéhez szükséges az alábbi eredmény:

Állítás: *Tetszőleges $\sigma \in S_n$ permutáció felbontásában a transzpozíciók számának paritása állandó.* □

[27)] **Sam Loyd** (1841-1911) amerikai matematikus azt állította, hogy a játékot találta ki 1878 -ben, bár egyesek szerint már előtte is ismert volt. Hírhedt (megoldhatatlan) feladványában 1000$ -t tűzött ki, ami rengeteg *súlyos* balesetet okozott Amerikában és Európában is, lásd pl. https://mathshistory.st-andrews.ac.uk/Biographies/Loyd/ , http://www.mathpuzzle.com/loyd/ , https://en.wikipedia.org/wiki/Sam_Loyd

c)

2	3	1	
11	6	15	4
5	8	7	9
10	13	12	14

d)

15	6	14	8
2	7	10	11
1	4	5	3
9	13	12	

3.4.19) Sam Loyd előző 15-ös játékához (kombinett) hasonlóan egy 3×3-as dobozban 8 számozott kockát helyeztünk el, egy helyet pedig üresen hagytunk. A kockákat odébb tologathatjuk úgy, hogy minden lépésben az egyik szomszédos kockát toljuk az üres helyre. A lépések sorozatát az F, L, J, B betűkkel kódolhatjuk: minden egyes betű azt jelenti, hogy a megfelelő lépésben felfelé, lefelé, jobbra vagy balra tolunk egy kockát. Például a középső ábrán látható helyzetből négy lépésben (JFFB) juthatunk el a baloldali ábrán látható alapállapotba.

a) Mekkora a legkisebb lépésszám, amivel el lehet jutni a jobboldali állapotból az alapállapotba?

b) Keressünk *invariáns*[28] tulajdonságot annak eldöntésére, hogy egy helyzetből el tudunk-e jutni (tologatásokkal) az a) alapállapotba.

3.4.20) Egy kártyakeverő gép minden egyes alkalommal ugyanazon módszer szerint rendezi át a lapokat. Ebbe a gépbe beletesszük az összes kőrt *ásztól a királyig sorrendben*[29]. Összekevertetjük a lapokat, majd azokat újra betesszük a gépbe. A második keverés után a lapok sorrendje a következő: **10, 9, Q, 8, K, 3, 4, A, 5, J, 6, 2, 7** . Mi volt a lapok sorrendje az első keverés után? (Lásd még a 3.4.14. feladatot[30].)

[28] A játék egy tulajdonsága **invariáns**, ha a játék folyamán nem változik meg.

[29] A csomagban levő figurák eredeti sorrendje: A, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K .

[30] Hasonló feladatot találunk a KöMal F.2848. feladatában is.

Kártyakeverőgép

3.4.21) Amikor *Bendegúz* érvényes helyjegyével felszállt a *Göcsej* expressz 78 -személyes vasúti kocsijába, döbbenten vette észre, hogy ott már minden hely foglalt. Az történt ugyanis, hogy *Dömötör* helyjegy nélkül szállt fel. A többi 77 utas pedig – köztük *Elek* is – vásárolt ugyan helyjegyet, de nem feltétlenül ültek oda, ahová a helyjegyük szólt. Bendegúz felállítja azt, aki a helyét elfoglalta. Aki feláll, az most már szintén a saját helyére szeretne leülni, és így tovább. Mindez addig folytatódik, míg végül Dömötör lelepleződik. Mennyi a valószínűsége annak, hogy Elek ülve nézheti végig az eseményeket[31)] ?

3.4.22) Baloldalt egy sáska, középen egy szöcske, jobboldalt egy tücsök ül egy hosszú, egyenes árokban. Időnként valamelyik átugorja egyik szomszédját (és két társa közé pottyan). Előfordulhat-e, hogy 1999 ugrás után újra a kiinduló sorrendben ülnek, ha végig csak az árokban (egy egyenes mentén) ugrálnak[32)] ?

3.4.23) Mi a következő képrejtvény megfejtése: $\boxed{\circ\bullet}$?

[31)] KöMaL B.3391.feladata (2000/6, 361.old), megoldása a 2001/3 szám 157.old.

[32)] KöMaL B.3296.feladata (1999/6, 361.old.), megoldása a 2000/2 szám 98.oldalán.

4. fejezet

Gyűrűk

4.1. Alapfogalmak

4.1.1) Vizsgálja meg, hogy az alábbi struktúrák gyűrűt alkotnak-e:

o) $\big(A^A, +, \circ\big)$ $(A \neq \emptyset$ tetszőleges halmaz),

a) $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$,

b) $(\mathbb{Z} \cdot 2, +, \cdot)$ (=páros számok a szokásos műveletekkel)

c) $(\mathbb{Z}_m, +, \cdot)$ $(m \in \mathbb{Z}$ tetszőleges egész szám),

d) $(\mathbb{R}[x], +, \cdot)$,

e) $(\mathbb{Z}[u], +, \cdot)$ ahol $u = i$, $\sqrt{2}$, $\sqrt{-5}$ vagy $\varepsilon = \frac{1}{2} + \frac{\sqrt{3}}{2} i$,

f) $(\{i, h\}, \vee, \wedge)$ (logikai műveletek),

g) $(\mathcal{P}(X), \cup, \cap)$ (halmazműveletek).

4.1.2) Mutassa meg, hogy az alábbi struktúrák gyűrűk:

o) $(\mathbb{R}^{n \times n}, +, \cdot)$,

a) $(\mathbb{Z}_5, +, \cdot)$,

b) $(\{i, h\}, \Leftrightarrow, \vee)$,

c) $(\mathcal{P}(X), \triangle, \cap)$,

d) $(\mathbb{Z}[\sqrt{3}], +, \cdot)$,

e) $\mathbb{Q}_{pn} := \big\{ \frac{a}{b} \in \mathbb{Q} \mid b \ \textit{páratlan} \big\}$ a szokásos műveletekkel,

f)

$$R[[x]] := \left\{ \sum_{i=0}^{\infty} r_i x^i : r_i \in R \right\}$$

ún. **formális hatványsorok** halmaza (R tetszőleges gyűrű), az alábbi (szokásos) műveletekkel:

$$\left(\sum_{i=0}^{\infty} r_i x^i \right) \boxplus \left(\sum_{i=0}^{\infty} s_i x^i \right) := \left(\sum_{i=0}^{\infty} (r_i + s_i)\, x^i \right)$$

és

$$\left(\sum_{i=0}^{\infty} r_i x^i \right) \boxdot \left(\sum_{i=0}^{\infty} s_i x^i \right) := \left(\sum_{i=0}^{\infty} t_i x^i \right) \quad ahol \quad t_i = \sum_{j=0}^{i} r_j s_{i-j} \quad .$$

(Az $R[[x]]$ jelölésben nem tévedés a dupla [[ ]] zárójel.)

g) $(\mathbb{Z}_{p^\infty}, \oplus, \odot)$ ahol tetszőleges $\overrightarrow{a}$, $\overrightarrow{b} \in \mathbb{Z}^{\mathbb{N}}$ (végtelen) sorozatokra

$$\overrightarrow{a} \oplus \overrightarrow{b} := \overrightarrow{c} \quad \overset{def}{\Longleftrightarrow} \quad \sum_{i=0}^{n} c_i p^i := \left(\sum_{i=0}^{n} a_i \right) + \left(\sum_{i=0}^{n} b_i \right) \pmod{p^{n+1}}$$

és

$$\overrightarrow{a} \odot \overrightarrow{b} := \overrightarrow{d} \quad \overset{def}{\Longleftrightarrow} \quad c_i := \left(\sum_{i=0}^{n} a_i \right) \cdot \left(\sum_{i=0}^{n} b_i \right) \pmod{p^{i+1}} \quad .$$

(Azaz $\mathbb{Z}_{p^\infty}$ elemei, az ún. *p-adikus egészek* tulajdonképpen "végtelen hosszú", p-alapú számrendszerben felírt egész számok, az összeadás és a szorzás műveleteit a közönséges egész számok összeadásának és szorzásának megfelelően végezzük[1)].)

[1)] úgy, ahogyan általános iskolában tanultuk. A szabályok bonyolultságát a maradékok "p-adikus" ["tízes"] átvitele okozza.

4.1.3) Mik az *egységek*[2] , *asszociált*[3]- , *irreducibilis-* és *prímelemek*[4] az előző feladatban felsorolt struktúrákban?

4.1.4) Miért nem test a polinomok halmaza?

4.2. A $\mathbb{Z}_m$ maradékosztályok

Ez a fejezet lényegében az egész számok oszthatóságról szól, kicsit másképpen mint a középiskolában.

4.2.1. Alapműveletek

4.2.1.0) a) Igaz-e, hogy $7 \cdot 3 \equiv -3 \pmod{12}$?

b) Igaz-e, hogy *"páros+páros=páros"* (mod 9) ?

c) Mutassuk meg, hogy a $(\mathbb{Z}_m, +)$ struktúrában nincs a + művelettel kompatibilis rendezési reláció.

4.2.1.1) a) Adja meg 5 és 3 (multiplikatív) inverzét (mod 9) !

b) Oldja meg az $5x = 3$ egyenletet $GF(9)$ -ben!

c) Számítsa ki $5/3$ értékét $GF(9)$ -ben és (mod 20) !

d) Számítsa ki $\sqrt{7}$ értékét mod 13 !

4.2.1.2) Oldja meg az alábbi egyenleteket a megadott struktúrákban:

---

[2] **Definíció:** *Tetszőleges* $(S, \bullet)$ *félcsoportban* **(i)** *az* $a \in S$ *elem* **osztója** a $b \in S$ *elemnek* (*vagy:* b **osztható** a*-val* / **többszöröse** a *-nak*), *ha* $b = a \bullet c$ *valamilyen* $c \in S$ *elemre.* **(ii)** $u \in S$ **egység**, *ha* u *osztója* S *minden elemének.* □

Jegyezzük meg: egység≠egységelem! A fenti fogalmaknak csak akkor van "értelme", ha S *nem* csoport, hiszen minden csoportban bármely elem osztható bármelyikkel.

[3] **Definíció:** *Tetszőleges* $(S, \bullet)$ *félcsoportban az* $a, b \in S$ *elemek* **asszociáltak** (="társítottak"), *ha* $a = u \bullet b$ *valamely* $u \in S$ *egységre.* □

[4] **Definíció:** *Tetszőleges* $(S, \bullet)$ *félcsoportban* **(i)** *az* $a \in S$ *elem* **irreducibilis (felbonthatatlan)**, *ha bármely* $a = b \bullet c$ *felbontásra* b *vagy* c *egység (azaz* c *vagy* b *asszociált* a *-hoz).*

(ii) $a \in S$ **prímtulajdonságú** (*vagy* **prím**), *ha bármely* $u, v \in S$ *elemekre* $a \mid u \bullet v$ *esetén* $a \mid u$ *vagy* $a \mid v$. □

a) $5x + 7 \equiv 9 \pmod{13}$,

b) $\frac{3x+4}{5-x} \equiv 7$ $GF(47)$ -ben,

c) $x^2 - 5x + 6 = 0$ $GF(13)$ -ban,

d) $x^2 + 3x + 9 = 0$ $GF(17)$ -ban,

e) $x^3 + 4x^2 - 5x + 6 = 0$ $GF(17)$ -ban,

f) $5x + 3y \equiv 9 \pmod{13}$.

4.2.1.3) Határozza meg az $f(x) = x^2 + 2x - 1$ kifejezés szélsőértékeit $\mathbb{Z}_{11}$ -ben

4.2.1.4) a) Ellenőrizze, hogy $g = 3$ *primitív gyök*[5] -e $\pmod{17}$.

A feladatgyűjtemény végén megtalálható *Index- és hatványtáblázatok (mod p)* segítségével számítsa ki az alábbiakat.

b) Mennyi $3^{40} \pmod{17}$ és mennyi $3^{40} \pmod{43}$?

c) Keresse meg a táblázatban $ind_{43}^{(3)}(28)$ értékét, és ellenőrizze.

Mennyi ennek alapján $28^8 \pmod{43}$?

d) Mennyi $11^{40} \pmod{43}$ és mennyi $11^{40} \pmod{47}$?

e) Keresse meg 7 , 16 és -1 indexét a 3 primitív gyökre vonatkoztatva $\pmod{17}$, majd számítsa ki $6/7$, $\sqrt{16}$ és $\sqrt{-4}$ értékét $\pmod{17}$.

f) Keresse meg 7 (multiplikatív) inverzét[6] $\pmod{47}$, majd oldja meg a $7x \equiv 11 \pmod{47}$ egyenletet.

g)* Mennyi $13^{-195} \pmod{1271}$? Mennyi $13^{-195} \pmod{24}$ illetve $3744^{-1} \pmod{9875}$?

h) Oldja meg az alábbi egyenleteket. (Ahol lehet, *ne* próbálgatással oldja meg.)

---

[5] **Definíció:** $g \in \mathbb{Z}_p$ **primitív-gyök** $\bmod p$ ($p \in \mathbb{P}$ prímszám), ha $[g] = (\mathbb{Z}_p, \cdot)$, azaz g hatványai kiadják $\mathbb{Z}_p$ összes elemét. □

(Lásd még a könyv végén levő táblázatokat.)

[6] **Definíció:** *Tetszőleges $(S, *)$ (multiplikatív) félcsoportban egy $a \in S$ elem* **inverze** $a^{-1} \in S$, *ha* $a * a^{-1} = e$ *ahol e az S egységeleme.* □

Definíció: *Tetszőleges $a \in \mathbb{Z}$ szám* **multiplikatív inverze** $\pmod{n}$ $a^{-1} \in \mathbb{Z}$, *ha* $a \cdot a^{-1} \equiv 1 \pmod{n}$. □

$x^2 \equiv 8 \pmod{17}$, $x^2 \equiv 14 \pmod{17}$,

$x^3 \equiv 11 \pmod{41}$, $x^3 \equiv 18 \pmod{41}$,

$x^3 - 3x^2 + 2x - 1 \equiv 0 \pmod{39}$.

4.2.1.5) A kerékpár *hajtó* és *hajtott* fogaskerekeinek egy-egy fogát megjelöltük. Milyen számelméleti műveletet tudunk így kísérletileg elvégezni? Hogyan lehet így meghatározni az *lnko* -t ? (A könyv címlapján egy szemléltető ábrát láthatunk.)

Lásd még a 4.3.4. *"Lineáris Diophantikus egyenletek"* fejezet feladatait is.

4.2.2. Általános- és középiskolás feladatok

4.2.2.0) a) Igazolja az (általános iskolában tanult) 2-es, 3-as, 4-es, 5-ös, 9-es (oszthatósági) "próbákat".

b) Mutassa meg, hogy: *egy tetszőleges $n \in \mathbb{Z}$ egész szám pontosan akkor osztható* 11 *-gyel, ha számjegyeit* váltakozó előjellel *összeadva a kapott összeg osztható* 11 *-gyel.* (Ún. 11 **-es próba**.)[7)]

Osztható-e 11 -gyel a 2835789423753918071 szám?

c) "Ellenőrizze" a következő (általános iskolai) számolásokat anélkül, hogy a végeredményt ténylegesen kiszámolná:

$673 \cdot 427 = 287\,371$, $917\,425 \cdot 25\,168 = 23\,089\,752\,420$,

$907\,159 : 382 = 2\,374 + (\textit{maradék}\ 291)$,

$2\,830\,917 : 427 = 6634 + (\textit{maradék}\ 199)$,

$601\,524 \cdot 548\,120 = 329\,797\,334\,880$,

$135498 \cdot 759054 = 102850298793$.

4.2.2.1) Mennyi maradékot adnak az alábbi kifejezések:

a) $9136 + 143^5 + 731 \cdot 54329 \cdot 42437 - 437^3 + 1$, 18 -al osztva?

b) $79346 + 146^{100} \cdot 1723 + 1$, 13 -al osztva?

[7)] További oszthatósági "próbákat" találunk még pl. a *The Mathematical Gazette* folyóirat 510 (2003), 497 (1999) számaiban.

c) $3^{29} + 4^{30} + 6^{32} + 7^{33}$, 5 -tel osztva[8] ?

d) $1 \cdot 7 \cdot 13 \cdot 19 \cdot ... \cdot 1993 \cdot 1999$, 6 -tal osztva[9] ?

4.2.2.2) a) Határozza meg az $1! + 2! + ... + 2005!$ kifejezés utolsó két jegyét[10].

b) Határozza meg az $1^2 + 2^2 + ... + 2005^2$ kifejezés utolsó két jegyét.

c) Adjuk meg

$$1001^{1965} \quad \textit{és} \quad 1001^{\left(1001^{1965}\right)}$$

utolsó 9 számjegyét! (*Pontosan hány jegyű* is a 1001^{1965} szám?)

d) Milyen számjegyre végződik a $5 + 5^2 + ... + 5^{150}$ kifejezés a 186 alapú számrendszerben felírva[11] ?

e) Milyen jegyre végződik (a tízes számrendszerben) $9^{2002} + 2002^9$? Mi az utolsó *két* jegye? Mennyi a kifejezés 5 -ös maradéka[12] ?

4.2.2.3) Hány lába van összesen egy tyúknak, hat kutyának és hét palpigradinak? (A palpigradi egy állat latin neve.) Az alábbi öt válasz közül *pontosan egy* helyes[13]:
A) 46 , B) 52 , C) 66 , D) 78 , E) 82 .

4.2.2.4) Mutassa meg, hogy minden 6 -ra végződő négyzetszámban a tízesek helyén páratlan számjegy áll!

4.2.2.5) Bizonyítsa be, hogy tetszőlegesen választott öt egész szám között mindig van olyan három, amelynek összege osztható 3 -mal !

4.2.2.6) Legyen n tetszőleges pozitív egész szám. Mennyi a maradék, ha az $1^n + 2^n + 3^n + 4^n$ összeget elosztjuk 4 -gyel ?

---

[8] Varga Tamás matematikaverseny 2002., 7. osztály megyei forduló.
[9] Abacus Int.Math.Comp., 2001.Nov, grade 5, http://www.gcschool.org/abacus.html
[10] Abacus Int.Math.Comp.2005.Febr.,for grade 7-8, Problem C.478., http://www.gcschool.org/pages/program/Abacus.html
[11] Abacus Internat. Math. Comp. 2003/04. Febr., Problem C.424. for grade 7-8, ld. http://www.gcschool.org/pages/program/Abacus.html
[12] Bem J. városi matematikaverseny 2002., 7. osztály.
[13] Zrínyi Ilona matematikaverseny 2001., általános iskolák 3.o.számára, megyei forduló.

4.2.2.7) Egy (általános) iskolai feladat volt, hogy a tanulók számolják ki 14! értékét. Peti eredménye = 87 178 290 120, Pannié = 87 178 290 200. Számológép és függvénytáblázat nélkül döntsük el, melyik eredmény (lehet) helyes. Keressünk több ellenőrzési módszert![14)]

4.2.2.8) A 10839 és a 11863 számokat ugyanazzal a háromjegyű számmal elosztva mind a kétszer ugyanaz a maradék. Mennyi ez a maradék[15)] ?

4.2.2.9) Három egymást követő pozitív egész szám köbének összege osztható 18-cal. Mennyit kapunk maradékul, ha a legkisebb és legnagyobb szám szorzatát 18 -cal osztjuk el[16)] ?

4.2.2.10) Adjuk meg azt a legkisebb pozitív egész számot, amellyel az 1999 -et megszorozva a kapott szám utolsó négy jegye[17)] 2001.

4.2.2.11) Számológép nélkül mutassa meg, hogy $333,333,331$ osztható 17 -tel[18)].

4.2.2.12)* Határozzuk meg az s alapú számrendszerben felírt

$$F_s := 1 + 22 + 333 + 4444 + ... + \underbrace{sss...s}$$

összegnek (a legutolsó szám s -jegyű)

a) utolsó jegyét ,

b) $(s-1)$ -gyel való osztási maradékát[19)].

4.2.2.13)* Mutassuk meg, hogy tetszőleges n természetes szám esetén a 3^n oldalú konvex sokszög oldalait és átlóit be tudjuk színezni 3 színnel úgy, hogy a színezett élek lefedhetők 3^{n-1} homogén (egyszínű) háromszöggel[20)]!

[14)] "Abacus" újság ált.iskolásoknak, 2005. B634. feladat, 6.oszt. részére

[15)] Összefoglaló feladatgyűjtemény matematikából, 3945.feladat

[16)] Felvételi feladat 2001.V.22.de.7.példa.

[17)] KöMaL C.576.feladata (2000/3, 168.old.), megoldása a 2000/9 szám 525.old.

[18)] A 31 , 331 , ..., $33,333,331$ számok mind prímszámok, és (régen) sokáig úgy gondol ták, hogy minden ilyen szám prím. Még ma sem tudjuk, hogy a 33...31 alakú számok között van -e végtelen sok prímszám.

[19)] KöMaL F.3269.feladata, 1999.

[20)] Kürschák J. matematikaverseny 2002.

4.2.2.14) Egy fejszámolóművésztől a következő mutatványt láttam: a nézők gondolnak néhány, akármilyen nagy, legalább 1 de legfeljebb 8 db páratlan számot (nem feltétlenül különbözőket), és négyzeteik összegéből a "fejszámolóművész" *azonnal* megmondja, hogy *hány* szám négyzetét adták össze a nézők[21)]. Mi a trükk megfejtése?

4.2.3. Euler és Fermat tételei, nagy kitevőjű hatványok

4.2.3.0) Hány jegyű a 3425^{5432} kifejezés a tízes számrendszerben felírva? És kettes számrendszerben?

4.2.3.1) a) Számítsa ki $\varphi(p)$ és $\varphi(p \cdot q)$ értékét tetszőleges $p, q \in \mathbb{P}$ prímszámokra.

b) Határozza meg tetszőleges $n \in \mathbb{N}$ természetes szám *Euler-féle* φ - függvényének értékét!

c) Határozza meg $\varphi(1500)$, $\varphi(2520)$ és $\varphi(13860)$ értékeit.

d) Mutassa meg, hogy φ (gyengén) multiplikatív[22)] számelméleti[23)] függvény.

4.2.3.2) Számítsa ki az alábbi hatványokat:

a) $6456^{4652} \pmod{9786}$,

b) $4326^{1818} \pmod{1003}$,

c) $2222^{5555} \pmod{137}$.

[21)] A bűvésztrükköt Pósa Lajostól hallottam.

[22)] **Definíció: (i)** *Az* $f : \mathbb{N} \to \mathbb{R}$ *függvény* **multiplikatív**, *ha* tetszőleges $m, n \in \mathbb{N}$ *relatív prím számok esetén* $f(uv) = f(u) \cdot f(v)$.

(ii) *Az* $f : \mathbb{N} \to \mathbb{R}$ *függvény* **totálisan multiplikatív**, *ha* tetszőleges $m, n \in \mathbb{N}$ *számok esetén* $f(uv) = f(u) \cdot f(v)$. □

[23)] **Definíció:** *Az* $f : \mathbb{N} \to \mathbb{R}$ *típusú függvényeket hívjuk* **számelméleti** *függvényeknek.*□

4.2.4. RSA - titkosírás

Ebben a fejezetben a következő speciális jelöléseket használjuk:

$p, q \in \mathbb{P}$ prímszámok, $n = p \cdot q$,
$s = \varphi(n) = (p-1) \cdot (q-1)$,
$ef \equiv 1 \pmod{s}$ ahol e a nyilvános és f a titkos kulcs.

A használt ABC -k:

00 = szóköz mindig, a rövid üzenetek *elejét* 0-val töltjük fel.

Sajnos a különböző példák különböző ABC -ket használnak, ezért alább ismertetjük a használt ABC -ket, valamint minden feladatban megadjuk a példában használt ABC betűszámát (26, 30 vagy 35).

01=A, 02=B, 03=C, 04=D, 05=E, 06=F, 07=G, 08=H, 09=I, 10=J, 11=K, 12=L, 13=M, 14=N, 15=O, 16=P, 17=Q, 18=R, 19=S, 20=T, 21=U, 22=V, 23=W, 24=X, 25=Y, **26**=Z **/26-betűs ABC/**.

01=A, 02=Á, 03=B, 04=C, 05=D, 06=E, 07=É, 08=F, 09=G, 10=H, 11=I, 12=J, 13=K, 14=L, 15=M, 16=N, 17=O, 18=Ö, 19=P, 20=Q, 21=R, 22=S, 23=T, 24=U, 25=Ü, 26=V, 27=W, 28=X, 29=Y, **30**=Z **/30-betűs ABC/**.

01=A, 02=Á, 03=B, 04=C, 05=D, 06=E, 07=É, 08=F, 09=G, 10=H, 11=I, 12=í, 13=J, 14=K, 15=L, 16=M, 17=N, 18=O, 19=Ó, 20=Ö, 21=Ő, 22=P, 23=Q, 24=R, 25=S, 26=T, 27=U, 28=Ú, 29=Ü, 30=Ű, 31=V, 32=W, 33=X, 34=Y, **35**=Z **/35-betűs ABC/**.

4.2.4.0) Faktorizálja[24)] az alábbi számokat:

a) $n = 440\,747$,

b) $n = 2\,347\,589$,

c) $n = 97\,189\,241$,

d) $n = 17\,967\,876\,255\,379$,

e) $n = 444\,113\,096\,135\,661\,846\,937$

4.2.4.1) a) Kódolja a "Wir treffen uns am Samstag" [*Találkozzunk szombaton*] üzenetet, ha $n = 55$ és $e = 27$ (26 betűs ABC).

[24)] bontsuk fel prímszámok szorzatára

b) Dekódolja a 24, 14, 34, 51, 05 RSA üzenetet, ha $n = 55$ és $f = 17$ (35 betűs ABC).

c) Dekódolja a 10, 62, 64, 34, 62 60 RSA üzenetet, ha $n = 77$ és $f = 7$ (35 betűs ABC).
(Ezek csak betűnkénti kódolások, ld. a 4.2.4.**7)** feladatot.)

4.2.4.2) Adottak a $p = 269$ és $q = 241$ prímszámok és az $e = 53201$ nyilvános kulcs.

a) Számolja ki $s = \varphi(n)$ értékét,

b) ellenőrizze, hogy e és s relatív prímek, majd számolja ki f értékét,

c) kódolja az $x = 48055$ üzenetet,

d) dekódolja az előbb kapott titkos üzenetet (azaz ellenőrizze a fenti számításokat),

e) kódolja a "HELLO" = 0008 0512 1215 üzenetet (26 betűs ABC),

f) dekódolja a 36376 28210 53334 üzenetet.

4.2.4.3) a)-d) Oldja meg az előző feladatot a $p = 109$, $q = 271$, $e = 13201$ és $x = 11418$ értékekkel.

e) kódolja a "HELLO" = 0008 0512 1215 üzenetet (26 betűs ABC),

f) dekódolja a 424 20621 üzenetet.

4.2.4.4) Tegyük fel, hogy a mi kódrendszerünk p=23, q=37, n=851, s=792, e=13, f=61, egy társunké p=29, q=31, n=899, s=80, e=29, f=29. Hitelesítsük aláírásunkat részére a "ZSEBSZÁMOLÓGÉP" szöveggel (35 betűs ABC).

4.2.4.5) Legyenek $n = 49,891,381$, $e = 209$, míg f , p , q és s titkosak, használjuk a 30 betűs ABC -t.

a) Kódolja az "ANNA ÖRÖK" = 00000001 16160100 18211813 üzenetet.

b) Kódoljuk az "OLVASD EL" üzenetet (26 betűs ABC) .

c) Ellenőrizze az $z \equiv x^f \equiv 49691150 \pmod{n}$ aláírás hitelességét.

d) Törje fel a kódot (f, p, q, s =?), majd dekódolja az
$y = x^e \equiv 37791786$, 01150082 , 32137718 $\pmod{n}$ üzenetet.

4.2.4.6) Ha n a 2.4.0) e) feladatbeli szám[25] és $f = 2039$ akkor mennyi e értéke és mennyi az $x = 32$ kódja?

4.2.4.7) Milyen hosszú blokkokat (hány betűt egyszerre) lehet kódolni ha az n kulcs k -jegyű?

4.2.4.8)***** Törje fel az alábbi kódrendszert: $e = 9007$,

$n = 11438162\ 5757888867\ 6692357799\ 7614661201\ 0218296721\ 2423625625\ 6184293570\ 6935245733\ 8978305971\ 2356395870\ 50589890751\ 4759929002\ 6879543541$ (129 jegyű),

a titkosított üzenet:

$C = 9686\ 9613754622\ 06147714092\ 2254355882\ 90575999112\ 4574319874\ 6951209308\ 16298225145\ 70835693147\ 6622883989\ 6280133919\ 9055182994\ 5157815154$ (26 betűs ABC)

4.2.4.9) További gyakorló kódrendszerek:

a) $p = 5,\ q = 11,\ n = 55,\ s = 40,\ e = 27,\ f = 3$,

b) $p = 7,\ q = 11,\ n = 77,\ s = 60,\ e = 11,\ f = 11$,

c) $p = 5,\ q = 13,\ n = 65,\ s = 48,\ e = 29,\ f = 5$,

d) $p = 7,\ q = 13,\ n = 91,\ s = 72,\ e = 29,\ f = 5$,

e) $p = 11,\ q = 13,\ n = 143,\ s = 120,\ e = 11,\ f = 11$,

f) $p = 17,\ q = 19,\ n = 323,\ s = 288,\ e = 17,\ f = 17$,

g) $p = 229,\ q = 233,\ n = 53,357,\ s = 52,896,\ e = 169,\ f = 313$.

4.2.5. Struktúrák vizsgálata

4.2.5.1) a) Adja meg tetszőleges $m \in \mathbb{Z}$ egész szám esetén (m) -et, az m által generált főideált[26]!

---

[25] $n = 444\ 113\ 096\ 135\ 661\ 846\ 937 = 3\ 719\ 977\ 867 * 119\ 385\ 951\ 211$

[26] **Definíció: i)** Egy $\mathbf{R}$ gyűrű $\mathbf{H} \leq \mathbf{R}$ részgyűrűje **ideális részgyűrű**, vagy röviden **ideál**ja, ha a *külső szorzás*ra is zárt, vagyis tetszőleges $r \in \mathbf{R}$ esetén $r\mathbf{H} := \{rh \mid h \in \mathbf{H}\} \subseteqq \mathbf{H}$. Az ideálokat általában $\mathbf{I}$ betűvel jelöljük: $\mathbf{I} \lhd \mathbf{R}$.

ii): Egy $\mathbf{I} \leq \mathbf{R}$ ideál **főideál**, ha egy elemmel generálható, vagyis ha létezik olyan $m \in \mathbf{R}$ amelyre $\mathbf{I} = (m) := \mathbf{R}\{m\} = \{rm \mid r \in \mathbf{R}\}$. □

b) Mutassa meg, hogy

$$(\mathbb{Z}_m, +, \cdot) \cong (\mathbb{Z}, +, \cdot)/(m) \quad .$$

4.2.5.2) Mutassa meg, hogy $\mathbb{R}^{n\times n}$ $(n \geq 2)$ azon elemeinek (mátrixok) halmaza, amelyek első sorának minden eleme 0 , $\mathbb{R}^{n\times n}$ -nek jobbideálját alkotják. Balideál-e ez a halmaz? Keressen balideált $\mathbb{R}^{n\times n}$ -ben!

4.3. Euklideszi gyűrűk

4.3.1. Alapfogalmak

(Az Euklideszi gyűrűk $\varphi(r)$ függvénye helyett sokszor $|r|$, $\|r\|$ vagy $N(r)$ -et írunk, és az $r \in R$ elem **abszolút értékének** vagy **normájának** is nevezzük.)

4.3.1.1) Vizsgálja meg, hogy az alábbi gyűrűk közül melyek Euklideszi gyűrűk[27)]! Adja meg a φ normát és a maradékos osztás algoritmusát is!

a) $(\mathbb{N}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z} \cdot 2, +, \cdot)$ (ez utóbbi a páros számok gyűrűje),

b) $(\mathbb{N}[x], +, \cdot)$, $(\mathbb{Z}[x], +, \cdot)$, $(\mathbb{Z}_p[x], +, \cdot)$, $(\mathbb{Z}_m[x], +, \cdot)$, $(\mathbb{Q}[x], +, \cdot)$, $(\mathbb{R}[x], +, \cdot)$, $(\mathbb{C}[x], +, \cdot)$, $(\mathcal{Q}[x], +, \cdot)$, $(\Gamma[x], +, \cdot)$ polinomgyűrűk
(ahol $\mathcal{Q}$ a kvaterniók teste, Γ egy tetszőleges test)

c) $(\mathbb{Z}[\alpha], +, \cdot)$ ahol $\alpha = i$, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{3}i$, $\sqrt{5}$, $\sqrt{5}i$, $\sqrt{6}i$, $\sqrt[4]{-1}$, $\sqrt{19}i$, $\sqrt{43}i$, $\sqrt{67}i$, $\sqrt{163}i$, $1 + \frac{\sqrt{19}i}{2}$ vagy $\sqrt[3]{1} = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$,

d) $\mathbb{Q}_{pn} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid b \text{ páratlan} \right\}$,

---

[27)] **Definíció:** *Egy* $(R, +, \cdot)$ *gyűrűt* **Euklideszi gyűrűnek** *hívunk, ha van olyan* $\varphi : R \to \mathbb{N}$ *függvény, amelyre teljesül:*
(i) $\varphi(r) = 0$ *csak* $r = 0$ *esetén áll fenn,*
(ii) *minden* $a \in R$ *elem* **maradékosan osztható** *bármely* $b \in R$ *elemmel, ha* $\varphi(a) \neq 0$ *és* $\varphi(b) \neq 0$, *azaz vannak olyan* $c, d \in R$ *elemek:* $a = b \cdot c + d$ *és* $\varphi(d) < \varphi(b)$. *Ekkor* c *-t* **hányados***nak, míg* d *-t* **maradék***nak hívjuk.*
$\varphi(r)$ *helyett gyakran* $|r|$, $\|r\|$ *vagy* $N(r)$ *-et írunk, és az* $r \in R$ *elem* **abszolút értékének** *vagy* **normájának** *nevezzük.* □

e) $(R[[x]], +, \cdot)$ (formális hatványsorok),

f) $(\mathbb{Z}_{p^\infty}, \oplus, \odot)$ (p -adikus egészek).

4.3.1.2)* Mutassuk meg, hogy *ha* az $\alpha \in \mathbb{C}$ komplex szám *másodfokú algebrai egész*, vagyis gyöke egy $\alpha^2 + p\alpha + q = 0 \quad (p, q \in \mathbb{Z})$ egyenletnek, *és* α' jelöli az egyenlet másik gyökét, akkor a $(\mathbb{Z}[\alpha], +, \cdot)$ struktúra elemein értelmezett

$$N(a + b\alpha) := (a + b\alpha) \cdot (a + b\alpha')$$

függvényre teljesülnek az alábbiak:

a) *tetszőleges* $u, v \in \mathbb{Z}[\alpha]$ számokra $N(uv) = N(u)N(v)$
(azaz N **totálisan multiplikatív**),

b) ha $\alpha \notin \mathbb{R}$ akkor minden $u \in \mathbb{Z}[\alpha]$ számra $N(u) = |u|^2$
(mint $u \in \mathbb{C}$ szám abszolút értékének négyzete).

4.3.2. Prímfelbontás

4.3.2.1) Mutassa meg, hogy a $(\mathbb{Z}\cdot 2, +, \cdot)$ struktúrában (a páros számok gyűrűje) *nem* teljesül az egyértelmű prímfelbontás tulajdonsága.

Lásd még az előző alfejezet utolsó feladatát, valamint a 4.4 "*Polinomok*" fejezet megfelelő feladatait (pl. 4.4.3)) is!

4.3.3. Euklidesz algoritmusa

4.3.3.1) Keresse meg az alábbi számok legnagyobb közös osztóját:

a) 7732 és 149 ,

b) 94542 és 24981 .

4.3.3.2) Keresse meg az 56354 és 2956 számok *legkisebb közös többszörösét*!

4.3.3.3) Keresse meg a 65924, 33284 és 53142 számok legnagyobb közös osztóját!

4.3.3.4) a) Számítsa ki $lnko(a,b,c)$, $lnko(a,b,c,d)$, $lkkt(a,b,c)$ és $lkkt(a,b,c,d)$ értékét általában, és az $a = 29601$, $b = 26565$, $c = 16302$, illetve az $a = 5292$, $b = 7623$, $c = 6435$, $d = 5005$ számok esetében.

b) Relatív prímek-e az $u = 14700$, $v = 21021$ és $w = 9867$ számok?

c) Adjon meg három olyan számot, amelyek relatív prímek de *páronként nem* relatív prímek .

4.3.3.5) Kör alakú futópályán két versenyző tart edzést, egyszerre indulnak, és ugyanazon irányban futnak. A pályát

a) egyikük 6 perc, a másik 10 perc,

b) egyikük 20 perc, a másik 35 perc,

c) egyikük 5 perc, a másik 15 perc

alatt kerüli meg. Hány percenként találkoznak?

d) Oldjuk meg a feladatot általánosan is: Ha a pályát t_1 ill. t_2 perc alatt kerülik meg, akkor hány perc múlva, *és hol* (a pálya mely részénél) találkoznak? Mely esetekben találkozhatnak *csak* a startjelnél?

(Ne feledjük, hogy általában $t_1, t_2 \in \mathbb{R}$ tetszőleges *valós* számok is lehetnek!)

4.3.3.6) Oldjuk meg az előző feladatot, ha

a) a versenyzők a körpályán *ellentétes* irányban futnak,

b) a játékosok hintán ülnek (a játszótéren), egyszerre és *egyazon* irányba lendülve indulnak ("ingamozgás"),

c) a hintákon *ellentétes* irányba lendülve indulnak.

Tegyük fel, hogy a két hinta kilengései (amplitúdók *és* frekvenciák) azonos nagyságúak.

4.3.3.7) Egy kör alakú pályán ketten futnak ugyanabban az irányban állandó sebességgel. Egy adott pillanatban az egyik futó 10 m-rel van a másik előtt, de miután az élen futó 22 m-t megtett, a másik utoléri. *Hány* olyan különböző pontja van a pályának, ahol a későbbiek során a második futó lekörözheti az elsőt?

4.3.3.8) Két busszal mehetünk haza: az A jelű 14 percenként, a B jelű 20 percenként jár. Mennyi a legkevesebb, és mennyi a legtöbb idő, melyet a megállóban kell várakoznunk, ha

a) reggel 08 : 00 -kor mindkettő ott van a megállóban,

b) az A jelű reggel 08 : 00 -kor, a B jelű 08 : 03 -kor van a megállóban (menetrend szerint).

4.3.3.9) Mely $n \in \mathbb{Z}$ egész számok esetén lesz a következő törtek értéke szintén egész szám:

a) $\dfrac{n+11}{n-9}$, **b)** $\dfrac{3n+5}{n+3}$, **c)** $\dfrac{n^2+1}{n+1}$.

4.3.3.10) Mely $n \in \mathbb{Z}$ egész számok esetén egyszerűsíthetők a következő törtek:

a) $\dfrac{n+13}{n-9}$, **b)** $\dfrac{5n+6}{8n+7}$, **c)** $\dfrac{21n+4}{14n+3}$.

4.3.3.11) Osszuk el maradékosan

a) 20 -t 3 -al,

b) $(2+7i)$ -t $(-1+3i)$ -vel.

4.3.3.12) Számítsuk ki az alábbi *legnagyobb közös osztókat* Euklidesz algoritmusával az alábbi $\mathbb{Z}[\alpha]$ struktúrákban:

a) $lnko(6+6i,\, 5+3i) = ?$

b) $lnko(5-13i\sqrt{2},\, 17+5i\sqrt{2}) = ?$

c) $lnko(17/2-13i\sqrt{3}/2,\, 23) = ?$

d) $lnko(74-47\sqrt{2},\, 58-41\sqrt{2}) = ?$

e) $lnko(13+8i,\, 5+3i) = ?$

f) $lnko(3+22i,\, 39-20i) = ?$

4.3.4. Lineáris Diophantikus egyenletek

4.3.4.1) Adja meg az alábbi (lineáris Diophantikus[28)]) egyenletek egész gyökeit:

a) $3141x + 6120y = 4$,

b) $5682x + 4836y = 30$,

c) $10518x + 5682y = 6$,

d) $4512x + 1111y = 3248$,

e) $1683x + 114y = 3$.

4.3.4.2) Egy 2520 m hosszú vezetéket $2,4m$ és $3,3m$ darabokra kell feldarabolnunk. *Hányféleképpen* tehetjük meg, ha a sorrend *nem* számít[29)]? (Vegyük észre, hogy most csak az egyenlet *pozitív* gyökeit keressük!)

4.3.4.3) a) 4 Ft és 2Ft 50f[30)] bélyegekből tudunk-e ragasztani 42Ft értékűt a borítékra?

b) Át tudunk -e fejteni $4,6\ell$ bort 1ℓ és $7d\ell$ -es üvegekbe úgy, hogy levegő buborék egy üvegben se maradjon?

c) 15 × 85cm és 15 × 60cm -es lécekből tudunk-e $7m \times 1,5m$ méretű zsaluanyagot készíteni (fűrészelés nélkül, hiszen nagyon sok kell) ?

Ne feledjük, hogy ezekben a feladatokban is az egyenletek *pozitív* gyökeit keressük !

4.3.4.4) Oldja meg az alábbi lineáris kongruenciákat:

a) $4x \equiv 3 \pmod 6$,

b) $238x \equiv 436 \pmod{28}$.

4.3.4.5) a) Oldja meg a $114x \equiv 3 \pmod{1683}$ egyenletet.

b) Keresse meg 18 multiplikatív inverzét $(\mathrm{mod}\, 175)$.

[28)] **Diophantosz** ókori görög matematikus Kr.u.250. körül foglalkozott először olyan egyenletekkel, amelyeknek csak az egész gyökeit kereste.

[29)] KöMaL 1999/4, 214. old. C 513. gyakorlat : ott a sorrend *számít.*

[30)] **f** = fillér = a Ft váltópénze (1993-ban megszűnt): 1Ft = 100f . □

4.3.4.6) Melyik az a négyjegyű szám, amellyel 25707 -et elosztva 32 -őt, 37568 -at elosztva 43 -at kapunk maradékul[31)]?

4.3.4.7*) Adja meg az

$$ax + by + cz = m \qquad (a, b, c, m, x, y, z \in \mathbb{Z})$$

háromismeretlenes lineáris Diophantikus egyenletek *általános* megoldását (a kétismeretlenes egyenletekről tanultak felhasználásával.)

4.3.4.8) Oldja meg az alábbi egyenleteket az egész számok körében:

a) $12x + 30y + 15z = 18$,

b) $4x + 3y = 7z$,

c) $6x + 10y + 15z = 7$.

d) Adja meg a fenti egyenletek *pozitív egész* megoldásait!

4.3.4.9) írja fel a $3x + 4y + 7z = n$ egyenlet összes (egész) gyökét, n függvényében!

4.3.4.10) A McDonald's éttermekben 6-os, 9-es vagy 20-as csomagolásban rendelhetünk Chicken McNuggets-et. (így például kérhetünk 21 darabot, mert $21 = 6 + 6 + 9$, de semmilyen módon nem kaphatunk 19 darabot.) Melyik az a legnagyobb darabszám, amit *nem* tudunk rendelni[32)]?

Érdemes még a 4.2.1.2) f) és 4.2.1.4) g) feladatokat is megtekintenünk. A lineáris Diophantikus egyenletek *kombinatorikai* vonatkozásait illetően az [$SzI'97$] feladatgyűjtemény 8. és 10. fejezeteit ajánlhatjuk.

4.3.5. Kínai maradéktétel

4.3.5.1) Oldja meg az alábbi kongruenciarendszereket:

[31)] Összefoglaló feladatgyűjtemény matematikából, 3946. feladat.

[32)] KöMaL C.625.gyakorlata, ld. 2001/4 szám 231.old., megoldása a 2001/9.szám 527.oldalán.

a) $\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod 9 \\ x \equiv 3 \pmod{11} \end{cases}$, **b)** $\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 2 \pmod{12} \\ x \equiv 3 \pmod{25} \\ x \equiv 0 \pmod{11} \end{cases}$

4.3.5.2) Oldja meg az alábbi kongruenciarendszereket:

a) $\begin{cases} 3x \equiv 4 \pmod 5 \\ 2x \equiv 1 \pmod 3 \end{cases}$, **b)** $\begin{cases} 3x \equiv 2 \pmod 7 \\ 2x \equiv 3 \pmod 9 \end{cases}$,

c) $\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \\ 5x \equiv 4 \pmod{11} \end{cases}$, **d)** $\begin{cases} x \equiv 3 \pmod 4 \\ 2x \equiv 3 \pmod 5 \\ 3x \equiv 2 \pmod 7 \\ 5x \equiv 4 \pmod{11} \end{cases}$

4.3.5.3) Melyik az a legkisebb természetes szám, amely 2 -vel osztva 1 , 3 -mal osztva 2 , 4 -gyel osztva 3 és 5 -tel osztva 4 maradékot ad[33)]?

4.3.5.4) Számítsa ki a következő nagyméretű szorzásokat a Kínai Maradéktétel felhasználásával:

a) $X_1 = 56\,079$, $Z_1 = 58\,144$,

b) $X_2 = 49\,745$, $Z_2 = 55\,846$,

c) $X_3 = 57\,898$, $Z_3 = 48\,653$,

d) $X_3 = 56\,898$, $Z_3 = 49\,866$.

Használja az alábbi modulus-rendszert:

$$\begin{cases} m_1 = 11 \cdot 23 = 253 , \\ m_2 = 8 \cdot 25 = 200 , \\ m_3 = 9 \cdot 29 = 261 , \\ m_4 = 13 \cdot 19 = 247 . \end{cases}$$

4.3.5.5) a) Oldja meg az

$$\begin{cases} x \equiv 3 \pmod 6 \\ x \equiv 7 \pmod{10} \end{cases}$$

[33)] Összefoglaló feladatgyűjtemény matematikából, 3937.feladat

kongruenciarendszert!

b) Adja meg általában az

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \tag{4.1}$$

kongruenciarendszerek megoldását (ahol m_1 és m_2 nem feltétlenül relatív prímek).

4.3.5.6) a) Oldja meg az

i) $\begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 1 \pmod{10} \\ x \equiv 11 \pmod{15} \end{cases}$, **ii)** $\begin{cases} x \equiv 3 \pmod{6} \\ x \equiv 5 \pmod{10} \\ x \equiv 0 \pmod{15} \end{cases}$

kongruenciarendszereket!

b) Adja meg általában az

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \end{cases} \tag{4.2}$$

kongruenciarendszerek megoldását (ahol m_1, m_2 és m_3 nem feltétlenül páronként relatív prímek).

Lásd még a 4.2.1.2) f) és 4.2.1.4) g) feladatokat is.

4.3.6. Magasabbfokú kongruenciák

Az $x^a \equiv b \pmod{m}$ alakú kongruenciák megoldására nincs általános vagy egyszerű módszer, ezen alapszik sok titkosírás.

4.3.6.1) Oldjuk meg az alábbi kongruenciákat:

a) $x^3 = 1 \ (mod\ 13)$

b) $x^{11} = 4 \ (mod\ 91)$

c) $x^{11} = 12 \ (mod\ 221)$

d) $x^{15} = 4 \ (mod\ 391)$

e) $x^{17} = 3 \ (mod\ 143)$

f) $x^{30} = 2 \pmod{1024}$

g) $x^{31} = 6 \pmod{187}$.

A fenti kongruenciák megoldása megtalálható $[SzI'17]$ -ben.

4.4. Polinomok

4.4.1) Végezze el a következő polinomok maradékos osztását a $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$ és $\mathbb{C}[x]$ gyűrűkben.

a) $(x^4 + x^2) : (x - 2)$,

b) $(x^3 + 3x + 5) : (2x^2 - 7x + 9)$,

c) $(4x^5 + 5x - 2) : (2x^3 + 3)$.

4.4.2) Bontsa fel irreducibilis tényezők szorzatára az alábbi polinomokat a $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ és $\mathbb{C}[x]$ struktúrákban:

o) $x^2 - 1$, $x^2 - 5$, $x^2 + 1$, $x^3 - 1$, $x^3 + 1$, $x^4 - 1$, $x^4 + 1$,

a) $x^2 - 3x + 1$, $x^2 + 5x + 7$, $x^2 + x + 1$,

b) $2x^3 - 5x^2 + 3x - 2$, $2x^3 - x^2 - 1$,

c) $x^4 + 2x^3 + 2x^2 + 2x - 1$

d) $x^5 - 2x^4 + 13x^3 - 18x^2 + 22x - 12$.

4.4.3) Bontsa fel[34)] prímtényezőkre az $1,000,000,000,000,001$ (16 jegyű) számot !

4.4.4) írja fel az alábbi polinomokat $(x - 2)$ polinomjaként[35)] :

a) $x^3 - 2x^2 + 2x - 1$,

b) $x^4 + x^2$.

4.4.5) Mit kapunk maradékul, ha az x^{2001} polinomot elosztjuk az $x^2 + 2x + 1$ polinommal[36)]?

[34)] azaz *faktorizálja*

[35)] azaz $p(x) = a_n(x-2)^n + a_{n-1}(x-2)^{n-1} + ... + a_1(x-2) + a_0$ alakban.

[36)] KöMaL B.3426.feladat, 2001/6.szám 355.old., vagy
https://www.komal.hu/verseny/2001-01/B.h.shtml

4.4.6) Határozza meg az alábbi polinomok *legnagyobb közös osztó*ját a $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ és $\mathbb{C}[x]$ struktúrákban:

a) $p(x) = x^3 + 2x^2 - 2x + 1$ és $q(x) = x^2 - x - 2$,

b) $f(x) = x^4 + 3x^3 - x^2 - 4x - 3$ és $g(x) = 3x^3 + 10x^2 + 2x - 3$.

4.4.7) Keresse meg az (összes) olyan $u(x), v(x) \in \mathbb{R}[x]$ polinomokat, amelyekre

$$f(x) \cdot u(x) + g(x) \cdot v(x) = d(x)$$

ahol $f(x) = x^3 - x^2 + 3x - 10$, $g(x) = x^3 + 6x^2 - 9x - 14$

és $d(x) = lnko\,(f(x), g(x))$ a legnagyobb közös osztó.

4.4.8) Hányszoros gyöke

a) $x_0 = 1$ az $f(x) = x^3 + 3x^2 + 2x - 6$ polinomnak ?

b) $x_1 = -2$ a $g(x) = x^7 + 3x^6 - 4x^4 + x^3 + 3x^2 - 4$ polinomnak ?

4.4.9) Négyzetmentesek[37] -e a következő polinomok:

a) $a(x) = x^3 - x^2 - x + 1$,

b) $b(x) = x^4 + x^3 + 4x^2 + x + 3$,

c) $c(x) = x^6 + 2x^5 + 11x^4 + 12x^3 + 39x^2 + 18x + 45$.

4.4.10) Adjon meg szükséges és elégséges feltételt arra, hogy egy *másodfokú* polinomnak egyszeres gyökei legyenek.

4.4.11) Bontsuk fel irreducibilis tényezők szorzatára az alábi polinomokat *a megadott struktúrákban:*

o) $o_1(x) = x^2 + 1$, $o_2(x) = x^2 + x + 1$ $\in \mathbb{Z}_2[x]$,

a) $a(x) = x^7 - 1$ $\in \mathbb{Z}_2[x]$,

b) $b(x) = x^5 - x + 1$ $\in \mathbb{Z}_5[x]$,

c) $c(x) = x^7 - 1$ $\in \mathbb{Z}_7[x]$,

d) $d(x) = 2x^6 + 3x^5 + 5x^3 + 2x^2 + 4$ $\in \mathbb{Z}_7[x]$.

---

[37] **Definíció:** *Egy* $p(x) \in \Gamma[x]$ *polinom* **négyzetmentes**, *ha nincs olyan* $q(x) \in \Gamma[x]$, $q(x) \notin \Gamma$ *polinom, amelyre* $(q(x))^2 \mid p(x)$. □

4.4.12)* Mutassa meg, hogy: ha az egész együtthatós

$$P(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \quad \in \mathbb{Z}[x]$$

polinom értéke minden $x \in \mathbb{Z}$ egész szám esetén egy 7 -tel osztható szám, akkor a polinom összes a_i együtthatója is osztható 7 -tel[38)].

Lásd még az 5. "*Testek*" c. fejezet megfelelő feladatait is.

[38)] Középiskolai Matematikai Lapok F1779.feladat, 1971.

5. fejezet

Testek

5.1.1) Ellenőrizze, hogy a következő halmazok a szokásos műveletekkel testeket alkotnak: $\mathbb{Q}$, $\mathbb{A}$ (=algebrai számok), $\mathbb{R}$, $\mathbb{C}$, $\mathcal{Q}$ (=kvaterniók), $\mathbb{Q}[\beta]$, $\mathbb{Z}_p$ (ha $p \in \mathbb{P}$ prímszám), $\mathbb{R}^{\mathbb{R}}_{Rac}$ (=racionális törtfüggvények).

5.1.2) Ellenőrizze, hogy $\mathbb{Z}_5$ -ben (azaz mod 5) valóban minden számmal (kivéve 0-val) lehet osztani (minden számot).

5.1.3) Számítsa ki a $p(x) \cdot q(x)$ szorzatot a $Z_m[x]/_{(f(x))}$ *faktorgyűrű*-ben, ahol

$$p(x) = \quad 3x^4 + 2x^3 - 4x + 1 \ ,$$
$$q(x) = -4x^4 + x^2 - 3x + 2 \ ,$$
$$f(x) = \qquad 2x^3 + x^2 - x + 4 \qquad \text{és} \qquad m = 5 \ .$$

5.1.4) Adja meg a

$$GF(4) = (\mathbb{Z}_2[x], +, \cdot) \, /_{(x^2+x+1)}$$

faktorhalmaz elemeit és a reprezentánsok közötti műveletek táblázatait! Miért test az így kapott struktúra?

5.1.5) írja fel az alábbi **véges testek**et (alaphalmazát [elemeit] és műveleti tábláit) ! (*Segítség:* $q = p^n$ esetén a $(\mathbb{Z}_p[x], +, \cdot)$ gyűrűt kell faktorizálni egy n -edfokú irreducibilis $f(x) \in \mathbb{Z}_p[x]$ polinommal.)

a) $GF(4) = \mathbb{Z}_2[x]/_{(f_7(x))}$ ahol pl. $f_7(x) = x^2 + x + 1$,

b) $GF(8) = \mathbb{Z}_2[x]/_{(f_{11}(x))}$ ahol pl. $f_{11}(x) = x^3 + x + 1$,

c) $GF(16) = \mathbb{Z}_2[x]/_{(f_{31}(x))}$ ahol pl. $f_{31}(x) = x^4 + x^3 + x^2 + x + 1$,

d) $GF(9) = \mathbb{Z}_3[x]/_{(f_{10}(x))}$ ahol pl. $f_{10}(x) = x^2 + 1$,

e) $GF(27) = \mathbb{Z}_3[x]/_{(f_{34}(x))}$ ahol pl. $f_{34}(x) = x^3 + 2x + 1$,

f) $GF(81) = \mathbb{Z}_3[x]/_{(f_{92}(x))}$ ahol pl. $f_{92}(x) = x^4 + x^2 + 2$,

g) $GF(25) = \mathbb{Z}_5[x]/_{(f_{27}(x))}$ ahol pl. $f(x)_{27} = x^2 + 2$,

h) $GF(125) = \mathbb{Z}_5[x]/_{(f_{131}(x))}$ ahol pl. $f_{131}(x) = x^3 + x + 1$,

i) $GF(625) = \mathbb{Z}_5[x]/_{(f_{627}(x))}$ ahol pl. $f_{627}(x) = x^4 + 2$.

(Ld. még a Függelékben az irreducibilis polinomok táblázatát.)

Lásd még a 4.2.1. "*Alapműveletek a $\mathbb{Z}_m$ maradékosztályokban*" c. fejezet feladatait is.

6. fejezet

Hálók, Boole-algebrák

6.1. Hálók

6.1.1) Vizsgáljuk meg a 1.2.2. "*Rendezések*" c. fejezet 2.18-24 feladataiban szereplő rendezési relációkat: melyek alkotnak közülük hálót.

6.1.2) Legyen $\Re$ egy tetszőleges (elsőrendű algebrai) struktúra, legyen $Sub(\Re)$ $\Re$ részalgebráinak halmaza, és tekintsük a $\mathcal{SUB}(\Re) := (Sub(\Re), \leq)$ struktúrát, ahol $\leq$ a részstruktúra-reláció. Mutassuk meg, hogy $\mathcal{SUB}(\Re)$ háló. Van-e legkisebb, legnagyobb, minimális ill. maximális eleme, és ez melyik részstruktúrája $\Re$-nek? Disztributív háló-e ?

6.2. Boole-algebrák

6.2.1) Az alábbi struktúrákban (kvázi Boole-algebrák) írjuk fel a Boole-algebra axiómákat, és döntsük el, közülük melyek teljesülnek, melyek nem:

(a) $\mathcal{R} := (\mathbb{R}, +, \cdot, -, 1, 0)$ (valós számok szokásos összeadása, szorzása, szorzása (-1) -gyel),

(b) $\mathcal{T} := (\ \{0, \frac{1}{2}, 1\},\ \max, \min, 1 - x, 1, 0,)$ a *háromértékű logika* ($\frac{1}{2}$ = a "*félig*- igazság").

6.2.2) Az alábbi struktúrákban írja fel a Boole-algebrák axiómáit, a De Morgan azonosságokat, és a következő feladatban szereplő azonosságokat:

(a) $\mathcal{P}_X := (\mathcal{P}(X), \cup, \cap, ^- , X, \emptyset)$ (a szokásos *halmazalgebra*) ahol $X \neq \emptyset$ tetszőleges halmaz.

(b) $\mathcal{B}_\mathcal{Y} := (\mathcal{Y}, \cup, \cap, ^- , X, \emptyset)$ ahol $X \neq \emptyset$ tetszőleges halmaz és $\mathcal{Y} \subset \mathcal{P}(X)$ olyan halmazrendszer X *részhalmazaiból* mely **zárt** a halmazműveletekre és $X \in \mathcal{Y}$.

(c) $\mathcal{L} := (H, \vee, \wedge, ^- , i, h)$ ahol $H := \{h, i\}$ és $\vee, \wedge, ^-$ a szokásos *logikai műveletek.*

(d) $\mathcal{P}_\Omega := (H, +, \cdot, ^- , \Omega, \emptyset)$ ahol Ω egy tetszőleges eseménytér, $H := \mathcal{P}(\Omega)$ és $+, \cdot, ^- , \Omega, \emptyset$ rendre az események összegét, szorzatát, tagadását, a biztos- és a lehetelen eseményt jelölik (*eseményalgebra*).

(e) $\mathcal{N}_N := (H, \vee, \wedge, ^- , N, 1)$ ahol $N \in \mathbb{N}$ egy tetszőleges *négyzetmentes* szám[1)], $H := \{N \text{ } osztói\}$, $a, b \in H$ esetén $a \vee b := lnko(a, b)$, $a \wedge b := lkkt(a, b)$, $\overline{a} := \frac{N}{a}$.

(f) $\mathcal{C} :=$ *a színkeverés* algebrája: H a lehetséges színek halmaza, az $\vee$ és $\wedge$ műveletek az additív és szubtraktív keverés, a $\overline{s}$ az s szín komplementer (kiegészítő) színe, $I :=$*fehér* és $\emptyset :=$*fekete.*

(g) *Kapcsoló-* és *csapalgebrák*: villanykapcsolók és vízcsapok soros, párhuzamos ill. fordított működésű kapcsolása, ahol $I =$*állandó áramlás* ("csőtörés") és $\emptyset =$*nincs áram.*

6.2.3) Igazolja az alábi azonosságokat a Boole-algebrák axiómái alapján[2)]:

(a)	$a \vee a = a \ , \ \ a \wedge a = a$	($\vee$ és $\wedge$ idempotensek)
(b)	$\neg\neg a = a$	($\neg$ involúció)
(c)	$a \vee b = \mid$ és $a \wedge b = \circ$ akkor $b = \neg a$	($\neg$ unicitása[3)])
(d)	$\neg(a \vee b) = \neg a \wedge \neg b$	
(e)	$\neg(a \wedge b) = \neg a \vee \neg b$	(De Morgan azonosságok)
(f)	$\neg\mid = \circ$ és $\neg\circ = \mid$	

[1)] *Egy $N \in \mathbb{N}$ szám* **négyzetmentes**, *ha egyik prímtényezője sem szerepel* 1 *-nél magasabb hatványon.* □

[2)] **Augustus De Morgan** (1806-1871) angol matematikus.

[3)] egyértelműsége

II. rész

Megoldások

1. fejezet

Halmazok, relációk, függvények

1.1. Halmazok

1.1.0) a) $= \big(A \cap \overline{B} \cap \overline{C}\big) \cup \big(\overline{A} \cap B \cap C\big)$,

b) $= \big(A \cap B \cap \overline{C}\big) \cup \big(\overline{A} \cap B \cap C\big) \cup \big(A \cap \overline{B} \cap C\big) \cup (A \cap B \cap C)$
vagy rövidebben: $= (A \cap B) \cup (A \cap C) \cup (B \cap C)$

c) $= \big(A \cap \overline{B} \cap \overline{C}\big) \cup \big(\overline{A} \cap B \cap \overline{C}\big) \cup \big(\overline{A} \cap \overline{B} \cap C\big)$

d) $= \big(\overline{A} \cap B \cap \overline{C}\big) \cup \big(\overline{A} \cap B \cap C\big) \cup \big(A \cap \overline{B} \cap C\big)$
vagy rövidebben: $= \big(\overline{A} \cap B\big) \cup \big(A \cap \overline{B} \cap C\big)$.

1.1.2) a) $x \in \{\{x\}, y\}$ pontosan akkor teljesül, ha $x = y$,

b) $V = \{x, \{x\}, y\}$,

c) W elemei: 0, $\{0\}$, $\{0, \{0\}\}$ és $\{0, \{0\}, \{0, \{0\}\}\}$, vagyis W -nek 4 eleme van.

1.1.3) Igaz állítás a), b), d), e) ; Hamis c) .
Az f) állítás pontosan akkor igaz, ha $x = \emptyset$.

1.1.4) Igaz állítás a) és e) második fele ; Hamis b), c), d) és e) első fele.
Az i) állítás pontosan akkor igaz, ha $\emptyset \in X$.

1.1.6) b) $A \triangle \emptyset = A$,

c)

$$\begin{array}{rcl} A\triangle B = \emptyset & \iff & A = B \\ A\triangle C = B\triangle C & \iff & A = B \\ A \cup (B\triangle C) = (A \cup B)\triangle(A \cup C) & \iff & A \subseteq B\triangle C \end{array}$$

Megjegyezzük, hogy *tetszőleges* A, B, C halmazokra

$$(A \cup B)\triangle(A \cup C) = B\triangle C \quad .$$

1.1.10) Vegyük észre, hogy ha $H = A \times B$, akkor A pontosan H elemeinek első komponenseiből állhat, míg hasonlóan B a második komponenseket tartalmazza.

a) Csak $A = \{1, 2, 3\}$ és $B = \{1, 2, 3\}$ lehet.
Ellenőrzés: $H_1 \neq A \times B$, mert $|H_1| = 6$ míg

$$|A \times B| = |A| \cdot |B|$$

alapján esetünkben $|A \times B| = 3 \cdot 3 = 9$ lenne.
Megjegyzés: $H \subseteq A \times B$ minden ilyen esetben mindenképpen teljesül.

b) Hasonlóan csak $A = \{a, b, c\}$ és $B = \{1, 2\}$ lehet.
Könnyen ellenőrizhető, hogy $H_2 = A \times B$.

1.1.12) Legyen
$A_i :=$
$\{$*azon* 0 *és* 31 *közötti egész számok, melyeknek i -dik bináris számjegye* 1 $\}$.

1.2. Relációk

1.2.2) i1) Ekvivalencia reláció.

f2$_1$) (oszthatóság $\mathbb{Z}$ -n): Nem antiszimmetrikus mert pl. $2|-2$ és $-2|2$ de $-2 \neq 2$, tehát az $|$ reláció *nem* rendezés $\mathbb{Z}$ -n. Nem is szimmetrikus mert pl. $3|6$ és $6 \nmid 3$.

f2$_2$) (oszthatóság $\mathbb{N}$ -n): $m|n$ -ből $m \leq n$ következik kivéve ha $m = 0$, vagyis 0 a *legnagyobb* elem, mert $m|0$ minden $m \in \mathbb{N}$ elemre, és hasonlóan 1 a legkisebb elem.

g2$_1$) $m \mid a-b$ pontosan azt jelenti, hogy a és b *ugyanazt a maradékot adják* m -el elosztva, így

$$\mathbb{Z}/_{\equiv m} \cong \mathbb{Z}_m = \{0, 1, ..., m-1\} \quad .$$

$m = 1$ esetén bármely a és b számok kogruensek egymással, így (az előző esettel összhangban)

$$\mathbb{Z}/_{\equiv 1} \cong \mathbb{Z}_1 = \{0\} \quad .$$

(Más szavakkal: az $\equiv_1$ reláció szerinti parrtíció *egyetlen* osztályból áll: $\mathbb{Z}$.)

$m = 0$ esetén minden szám csak *önmagával* kongruens, vagyis $\equiv_0$ a (jólismert) "egyenlőség" reláció:

$$\equiv_0 \quad = \quad " = " \quad .$$

g2$_2$) $a \bowtie b$ pontosan akkor teljesül, ha $\mathfrak{p}(a)$ és $\mathfrak{p}(b)$ ugyanazt a *véges* részhalmazát jelöli a prímszámok $\mathbb{P}$ halmazának. Vagyis

$$\mathbb{Z}/_{\bowtie} \cong \mathbb{P}^* \cup \{\bullet\}$$

ahol $\mathbb{P}^*$ jelöli $\mathbb{P}$ összes *véges* részhalmazának összességét, és $\bullet$ a $0 \in \mathbb{Z}$ szám ekvivalencia osztálya. Megjegyezzük még, hogy $\emptyset$ az $1 \in \mathbb{Z}$ szám ekvivalencia osztálya.

i2$_1$) Szimmetrikus de *nem* reflexív és *nem* tranzitív.

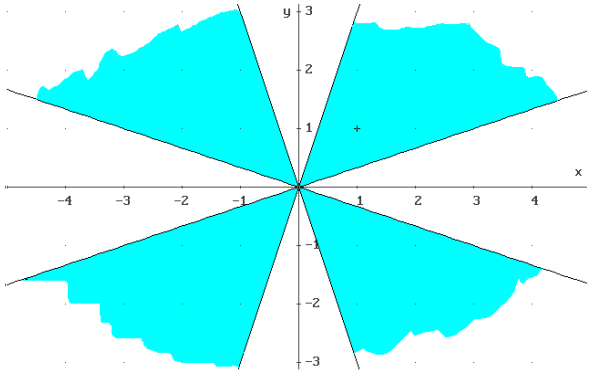
j2) (párhuzamos egyenesek) Egy lehetséges reprezentáns rendszer síkban: egy ponton átmenő összes egyenes (egyenesserreg/sugársor),

k2) A $\shortparallel$ reláció köztudottan reflexív és szimmetrikus. V -n nem tranzitív mert $\underline{0}$ minden vektorral párhuzamos, de $V \backslash \{\underline{0}\}$ -n már tranzitív.

m2) A mátrixok hasonlósága *ekvivalencia* reláció.

q2$_1$) Ekvivalencia mert: reflexiót bármely $c > 1$ szám igazolja, a szimmetria nyilvánvaló, a tranzitivitáshoz pedig elég meggondolnunk, hogy ha $|\frac{a}{b}| < c_1$ és $|\frac{b}{d}| < c_2$ akkor $|\frac{a}{d}| = |\frac{a}{b}| \cdot |\frac{b}{d}| < c_1 \cdot c_2$, vagyis $c_1 \cdot c_2$ igazolja $a \sim_0 d$ -t.

q2$_2$) Az előző pontban írtak alapján $a \sim_c b$ mindig szimmetrikus, de csak $c > 1$ esetén reflexív, és csak $c^2 < c$ (azaz $c < 1$) esetén tranzitív. Vagyis egyetlen $c > 0$ valós számra sem ekvivalencia reláció.



1.2.2) q2_2) feladat

1.2.9) Egy reláció pontosan akkor *reflexív*, ha gráfja tartalmazza az $y = x$ egyenest.

A reláció *szimmetrikus*, ha gráfja (tengelyesen) szimmetrikus az $y = x$ egyenesre.

A reláció *teljes*, ha $\Gamma \cup \Gamma' = \mathbb{R}^2$ ahol Γ a reláció gráfja és Γ' a gráf tükörképe az $y = x$ egyenesre.

A reláció *antiszimmetrikus*, ha $\Gamma \cup \Gamma' \subsetneqq \{y = x\}$.

1.2.1. Ekvivalenciák

1.2.15) a) $\equiv_1 = \Delta = \mathbb{Z}^2$ (bármely két elem kongruens),

$\equiv_0$ a (jólismert) "egyenlőség" reláció

$=$ (az egyenlőség) csak $\equiv_\infty$ lehetne, *nincs* olyan $m \in \mathbb{N}$ amelyre $=$ azonos lenne $\equiv_m$-el.

$\mathbb{Z}/_{=} \cong \mathbb{Z}$, $\mathbb{Z}/_{=_1} \cong \mathbb{Z}_1 = \{0\}$, $\mathbb{Z}/_{=_m} \cong \mathbb{Z}_m$.

$\equiv_n$ pontosan akkor finomabb $\equiv_m$ -nél, ha $m|n$, és $=$ a legfinomabb reláció.

b) $\sim_A$ pontosan akkor reflexív ha $0 \in A$.
$\sim_A$ pontosan akkor szimmetrikus ha A szimmetrikus 0 -ra, azaz $a \in A$ esetén $-a \in A$ is teljesül.

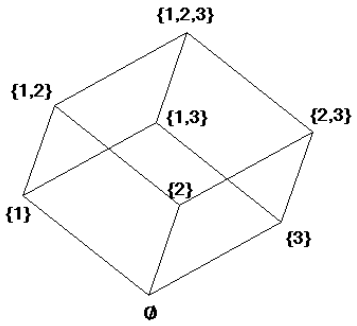
$\sim_A$ végül pontosan akkor tranzitív, ha A zárt az összeadásra: $a, b \in A$ esetén $a + b \in A$ is teljesül.

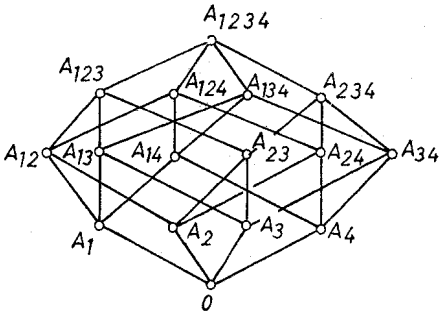
1.2.17) A szimmetria és a reflexivitás minden esetben nyilvánvaló.

1.2.2. Rendezések

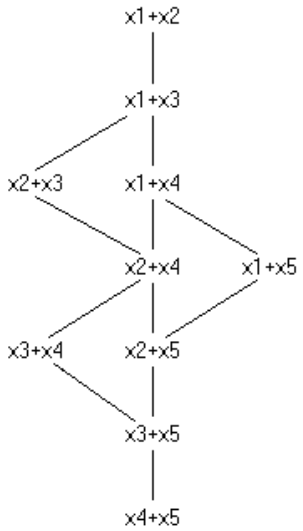
1.2.18) c) $|_{\mathbb{Z}} \subseteq \mathbb{Z}^2$ nem szimmetrikus és nem antiszimmetrikus.

1.2. 20) a) A három- és négydimenziós kockák élgráfjait kapjuk (az $\mathbf{A}_{uv...}$ csúcsok az $\{u, v, ...\}$ részhalmazokat jelölik):





1.2.21)



1.2.22) Például: "*minden páros* $<$ *minden páratlan*" $\mathbb{N}$ ill. $\mathbb{Z}$ -ben.

Vagy: válasszunk egy tetszőleges $p \in \mathbb{N}$, $p \geq 2$ számot, és legyen $n \preccurlyeq m$ **ha** p alapú számrendszerben felírva n lexikografikusan (betűrendben) megelőzi m -et.

1.2.23) $|_{\mathbb{N}\setminus\{0\}} \subset \leq_{\mathbb{N}\setminus\{0\}}$ míg $|_{\mathbb{N}} \not\subseteq \leq_{\mathbb{N}}$, hiszen például $(\mathbb{N}, |)$ -ban 0 maximális, 1 minimális elem. Vagyis $|_{\mathbb{N}\setminus\{0\}}$ teljessé tehető, de $|_{\mathbb{N}}$ nem.

1.2.24) $(\mathbb{N}, |)$ -ben:

$$\inf\{a_1, ..., a_k\} = lnko\{a_1, ..., a_k\}$$

és

$$\sup\{a_1, ..., a_k\} = lkkt\{a_1, ..., a_k\} \quad .$$

1.2.25) pl. 6, 10 és 15 .

1.2.26) a) $(\mathbb{R}, \leq)$ -ben $H_{\leq}(a) = (-\infty, a]$ félegyenes,

$H_{\leq}(\min(a,b)) = H_{\leq}(a) \cap H_{\leq}(b)$, $H_{\leq}(\max(a,b)) = H_{\leq}(a) \cup H_{\leq}(b)$

és $a \leq b \Leftrightarrow H_{\leq}(a) \subseteq H_{\leq}(b)$.

b) $(\mathbb{N}, \mid)$ -ben nyilván $H_{|}(a) = \{a \text{ osztói}\}$, $1, a \in H(a)$, továbbá

$$\begin{array}{ccc} a|b & \Leftrightarrow & a \in H(b) \quad \Leftrightarrow \quad H(a) \subseteqq H(b) \\ H_{|}(lnko(a,b)) & = & H_{|}(a) \cap H_{|}(b) \\ H_{|}(lkkt(a,b)) & \subseteqq & H_{|}(a) \cup H_{|}(b) \ . \end{array}$$

1.2.27) a) $\lhd$ nyilván reflexív. A tranzitivitás is könnyen látható: ha $f \lhd g$ és $g \lhd h$ (melyeket $n_{f,g}$ és $n_{g,h}$ igazol), akkor $n_0 := \max\{n_{f,g}; n_{g,h}\}$ és $n_0 \leq n$ esetén nyilván $f(n) \leq g(n) \leq h(n)$, vagyis valóban $f \lhd h$.

$\lhd$ nem szimmetrikus. Ha ugyanis $f \lhd g$ és $g \lhd f$ (melyeket $n_{f,g}$ és $n_{g,f}$ igazol), akkor csak annyit tudunk, hogy az $n_0 := \max\{n_{f,g}; n_{g,f}\}$ *küszöbtől kezdve* $f(n) \leq g(n)$ és $g(n) \leq f(n)$, azaz $n_0 \leq n$ esetén $f(n) = g(n)$; f és g értékeiről $n \leq n_0$ esetén semmit sem tudunk.

Azonban, tekintsük az $\mathcal{A}$ halmazon a következő *ekvivalencia* relációt (HF): legyen $f, g \in \mathcal{A}$ esetén $f \stackrel{\circ}{=} g$ ha valamely $n_0 \in \mathbb{N}$ küszöbtől kezdve $f(n) = g(n)$. Ekkor az $\mathcal{A}/\stackrel{\circ}{=}$ faktorhalmazon $\lhd$ már (igazi) rendezés lesz! Sőt, az $\trianglelefteq$ jelölés még kifejezőbb lenne.

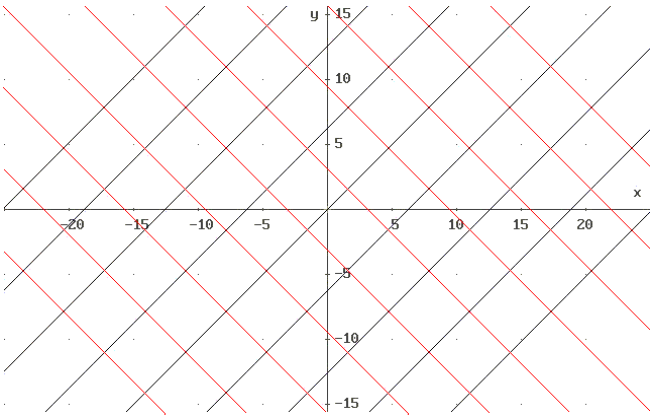
$\lhd$ nem teljes reláció, mert az $f(n) = 1+(-1)^n = 2,0,2,0,2,...$ és $f(n) = 1-(-1)^n = 0,2,0,2,0,...$ függvények összehasonlíthatatlanok (sem $f \lhd g$ sem $g \lhd f$ sem $f = g$, még az $\mathcal{A}/\stackrel{\circ}{=}$ faktorhalmazon sem).

b) Például $h(n) := \min\{f(n), g(n)\}$ és $k(n) := \max\{f(n), g(n)\}$ esetén $h \lhd f$, $h \lhd g$, $f \lhd k$ és $g \lhd k$. Tehát *bármely* $f, g \in \mathcal{A}$ *kompatibilis* alulról és felülről $\lhd$ szerint.

1.3. Függvények, műveletek

1.3.4) a)

$$Ker(\varphi) = \{\ (x,y) \in \mathbb{R}^2\ :\ \sin(x) = \sin(y)\ \}$$
$$= \bigcup_{k\in\mathbb{Z}} \left\{(x,y) \in \mathbb{R}^2 : y = x + 2k\pi\right\} \cup \left\{(x,y) \in \mathbb{R}^2 : y = (2k-1)\pi - x\right\}.$$



1.3.4) a) feladat

1.3.6) Műveletről eleve csak akkor beszélhetünk, ha minden $x, y \in \mathbb{R}_+$ számpárra $x * y \in \mathbb{R}_+$ is teljesül, azaz

$$x * y = x + y + t\sqrt{xy} > 0\ , \quad \text{vagyis} \quad t > -\left(\sqrt{\frac{x}{y}} + \sqrt{\frac{y}{x}}\right) \quad .$$

Ez pontosan akkor teljesül minden $x, y \in \mathbb{R}$ számra, ha $t > -2$.

A kívánt $(x * y) * z = x * (y * z)$ azonosság nyilván fennáll, ha $t = 0$. Ha $t \neq 0$, akkor pedig ekvivalens a

$$\sqrt{xy} + \sqrt{xz + yz + t\sqrt{xyz}} = \sqrt{yz} + \sqrt{xy + xz + t\sqrt{yzx}}$$

azonossággal. Az $x = 4$, $y = z = 1$ értékekkel tesztelve a $t^2 = 4$ egyenlethez jutunk. Tehát $t = 0$ mellett csak $t = 2$ jöhet szóba. Az utóbbi esetben

$$x * y = x + y + 2\sqrt{xy} = (\sqrt{x} + \sqrt{y})^2 \quad ,$$

így valóban

$$(x * y) * z = (\sqrt{x} + \sqrt{y} + \sqrt{z})^2 = x * (y * z) \quad .$$

A feladat követelményeit tehát csak a $t = 0$ és $t = 2$ értékek elégítik ki.

1.3.7) b) A kommutativitás és asszociativitás nyilvánvaló.

A $\boxtimes$ művelet könnyen láthatóan *idempotens, hiszen* tetszőleges $r = \frac{a}{b} \in \mathbb{Q}$ számra

$$r \boxtimes r = \frac{a}{b} \boxtimes \frac{a}{b} = \frac{2a}{2b} = \frac{a}{b} = r \quad .$$

1.3.8) A válasz: **nem**. Legyen $f(x) = x$ és

$$g(x) = \begin{cases} x - 3 & ha \quad x \leq 1 \\ -2/x & ha \quad 1 < x < 2 \\ x - 3 & ha \quad 2 \leq x \end{cases} \quad ,$$

ekkor belátható, hogy $f, g \in \mathbb{Q}_{növ}$ de az $f(x) + g(x) = 0$ egyenletnek nincs megoldása[1)], vagyis $f + g \in \mathbb{Q}_{növ}$.

1.3.9) Az $y = x^3$ görbe pontjait *egyértelműen* jellemezhetjük az abcisszájukkal. Legyen $^\circ$ az a művelet, amely a görbe a és b abszcisszájú A és B pontjai esetén $a^\circ b$-nek az $A * B$ pont abszcisszáját felelteti meg. Ekkor a pontokon értelmezett $*$ művelet pontosan akkor asszociatív, ha a valós

[1)] a részletes indoklás megtalálható a KöMaL 2000/6. számának 352.oldalán, az A.228 feladat megoldásánál, vagy: https://www.komal.hu/verseny/2000-01/A.h.shtml

számokon értelmezett $^\circ$ művelet az. Megmutatjuk, hogy $^\circ$ éppen az összeadás, amiből feladatunk állítása nyilván következik.

Az AB egyenes egyenlete $a \neq b$ esetén

$$(b-a)(y-a^3) = (b^3-a^3)(x-a) \quad ,$$

ami rendezés után

$$y = (b^2+ab+a^2)\cdot x - (b^2a+a^2b) \tag{1.1}$$

alakba írható. Könnyen ellenőrizhető, hogy az (1.1) egyenlet $b=a$ esetén az $y=x^3$ görbe (a,a^3) pontbeli érintőjének az egyenlete. Az (1.1) egyenletű egyenes és az $y=x^3$ görbe metszéspontjainak abszcisszái kielégítik az

$$x^3 = (b^2+ab+a^2)\cdot x - (b^2a+a^2b)$$

egyenletet. Ebben az x-re nézve harmadfokú egyenletben x^2 együtthatója 0, ezért a három gyök *összege*[2] is 0. így, mivel az egyenlet két gyöke a és b , a harmadik gyöke $-(a+b)$.

Vagyis a harmadik metszéspont a $(-(a+b),-(a+b)^3)$ pont, tehát az $A*B$ pont az $((a+b),(a+b)^3)$ pont, ami azt jelenti, hogy $a^\circ b = a+b$. (Könnyen ellenőrizhető, hogy ez az $a=b$ esetben is érvényes.)

Megjegyzés: Megoldásunkból az is látszik, hogy az $y = x^3 + k\cdot x$ egyenletű görbére is igaz a feladat állítása[3].

1.3.10) Vizsgáljuk az $(x\bullet y) - x + (y\bullet z) - y$ mennyiséget! **c)** és **b)** alapján:

$$\begin{aligned}(x\bullet y) - x + (y\bullet z) - y &= (x-x)\bullet(y-x) - (y-y)\bullet(x-y)\\ &= (-1)\,(0\bullet(x-y)) - 0\bullet(x-y) = 0 \quad .\end{aligned}$$

Végül **a)** felhasználásával $\bullet$ *csak* a következő lehet:

$$x\bullet y = \frac{x+y}{2} \ .$$

---

[2] A másodfokú egyenletekre megismert Viéta formulákhoz hasonló, a harmad- (és magasabb-) fokú egyenletekre való általánosításáról van szó: *Ha az* $a_nx^n+...+a_1x+a_0=0$ *egyenlet (nem feltétlenül különböző) gyökei* $x_1,...,x_n$, *akkor* $x_1+...+x_n = -a_{n-1}/a_n$, $x_1\cdot...\cdot x_n = (-1)^n\cdot a_{n-1}/a_n$, *stb.* □ (Bővebb részletekért ajánljuk a www.mathworld.wolfram.com címet, ahol egy matematikai kislexikont találunk.)

[3] KöMaL 2000/1. szám 28.oldal F.3278 feladat.

Ellenőrizhető (ellenőrizendő), hogy ez a $\bullet$ művelet teljesíti az a),b),c) tulajdonságokat. $\square$

1.3.11) Ha $x = y$ és $z = 0$, akkor a feltétel szerint

$$x * x = x * x + 0 * x \quad ,$$

azaz

$$0 * x = 0 \qquad (\forall x \in \mathbb{R}) \, . \tag{1.2}$$

Ha most x és y tetszőlegesek de $z = 0$, akkor

$$x * y = x * (y + 0) = (y * x) + (0 * x) = (y * x) + 0$$

ami (1.2) alapján azt jelenti, hogy

$$x * y = y * x$$

vagyis $*$ valóban kommutatív. $\square$

Megjegyzés: A $*$ művelet fenti tulajdonságaiból (kommutatív és disztributív) még nem következik, hogy csak a szorzás lehetne. Például az

$$x * y := 0 \; (\forall x, y \in \mathbb{R})$$

műveletre is teljesülnek a feladatban megismert tulajdonságok.

1.3.12) Teljes indukcióval igazolható, hogy minden $y \geq 0$ és tetszőleges $x \in \mathbb{Z}$ számra

$$x \# y = x(y + 1) - y \, . \tag{1.3}$$

Ezután, egy újabb teljes indukcióval igazolható, hogy (1.3) teljesül *tetszőleges* $y, x \in \mathbb{Z}$ számokra. $\square$

1.3.13)* Az $x, 0, y$ számokra ii) alapján $x \boxtimes (0 \boxtimes y) = y \boxtimes (0 \boxtimes x)$, tehát i) alapján $x \boxtimes y = y \boxtimes x$, vagyis a $\boxtimes$ művelet kommutatív. Ekkor ii) -re alkalmazva a kommutativitást $a \boxtimes (b \boxtimes c) = c \boxtimes (b \boxtimes a) = (b \boxtimes a) \boxtimes c = (a \boxtimes b) \boxtimes c$.

1.3.14) Könnyen adható olyan művelet, amelyre **a), b), c)** teljesül de az *egyszerűsítési szabály nem*: legyen

$1 \circ x = x \circ 1 := x$ és $x \circ y := 0$ minden más esetben.

1.3.15) A * művelet nem asszociatív, nem kommutatív, jobbról egy elemmel sem lehet egyszerűsíteni, de balról minden elemmel lehet egyszerűsíteni.

2. fejezet

Általános struktúrák

2.1. Algebrai struktúrák (Algebrák)

2.1.3) a) $(\mathbb{Z}_p, +)$ -nak nincs valódi részstruktúrája (csak $\{0\}$ és önmaga), mert ha $H \leq \mathbb{Z}_p$ és $a \in H$, $a \neq 0$, akkor

$$H \supseteq \{k \cdot a \mid k = 0, ..., p-1\} =: L \quad ,$$

de p prímtulajdonsága miatt L elemei mind különbözőek:

$$k_1 a \equiv_p k_2 a \quad \Leftrightarrow \quad p \mid (k_1 - k_2) \cdot a \quad \Leftrightarrow \quad k_1 = k_2$$

hiszen a, k_1 , $k_2 \leq p$. Vagyis L -nek és H -nak ugyanannyi eleme (p db) van, mint $\mathbb{Z}_p$ -nek, vagyis $L = H = \mathbb{Z}_p$.

b) Legyen $m \in \mathbb{N}$ összetett szám és legyen $H \subseteq \mathbb{Z}_m$ részstruktúrája $(\mathbb{Z}_m, +)$ -nek, $H \neq \{0\}$.

Ha van olyan $a \in H$ amely relatív prím m -hez, akkor az a) -beli gondolatmenetet megismételhetjük, vagyis ez esetben $H = \mathbb{Z}_m$.

2.1.4) Elég a (függvény-) halmazok zártságát ellenőrizni a $\circ$ (kompozíció) műveletére.

2.1.5) Például $(\mathbb{Z}_p, +)$ vagy $(\{i, h\}, \rceil)$ (tagadás).

2.1.6) a) $[2]_+ = \{2, 4, 0, ...\} = \{0, 2, 4\}$

és $[2]. = \{2, 2^2, 2^3, 2^4, ...\} = \{2, 4, 2, 4, ...\} = \{2, 4\}$

b) Mivel $10 \equiv -2 \pmod{12}$, ezért számolásainkat rövidebben is írhatjuk:

$$[10]_+ = [-2]_+ = \{-2,-4,-6,-8,-10,-12,...\} \equiv \{10,8,6,4,2,0\} =$$
$$= \{0,2,4,6,8,10\}$$

illetve

$$[10]. = [-2]. = \{-2,(-2)^2,(-2)^3,(-2)^4,...\} = \{-2,4,-8,16,-32,...\} \equiv$$
$$\equiv \{10,8,4,4,...\} = \{4,8,10\} \ .$$

2.1.7) Lásd a 2.1.3) feladat megoldását.

2.1.8) a) Minden *véges* struktúra természetesen végesen generált.

$(\mathbb{Z}_{12},+) = [1]$, tehát ciklikus. Sőt, általában $(\mathbb{Z}_m,+) = [1]$ minden $m \in \mathbb{N}$ -re, vagyis *mindegyik* $(\mathbb{Z}_m,+)$ struktúra ciklikus.

Mivel $(\mathbb{Z}_{12},+) \times (\mathbb{Z}_{12},+) \ncong (\mathbb{Z}_{144},+)$ és mindkettőnek ugyanannyi (144 db) eleme van, továbbá $(\mathbb{Z}_{144},+) = [1]$ ciklikus, ezért $(\mathbb{Z}_{12},+) \times (\mathbb{Z}_{12},+)$ **nem** lehet ciklikus.

b) $(\mathbb{Z},+) = [1,-1]$, tehát végesen generált.

Azonban, minden $x \in \mathbb{Z}$ egész számra

$$[x] = \{x \cdot n : n \in \mathbb{N}\} \quad ,$$

tehát $(\mathbb{Z},+)$ *nem* ciklikus.

$(\mathbb{R},+)$ nem megszámlálható halmaz *G.Cantor tétele* miatt , így a fentiek alapján $(\mathbb{R},+)$ *nem* végesen generált (és így persze *nem* is ciklikus).

2.2. Homomorfizmusok, kongruenciák, faktorok

2.2.1)e) Nem homomorfizmus, mert $\varepsilon(1,5) = 5$, $\varepsilon(2,5) = 10$, $(1,5)+(2,5) = (3,10)$ és $\varepsilon(3,10) = 30$, de $5+10 = 15 \neq 30$ miatt

$$\varepsilon((1,5)+(2,5)\ ) = \varepsilon((3,10)\ ) = 30 \neq 15 = 5+10 = \varepsilon(1,5)+\varepsilon(2,5) \ .$$

Bár $\varepsilon((1,5)\cdot(2,5)) = 50 = \varepsilon(1,5)\cdot\varepsilon(2,5)$, de például

$$\varepsilon((4,7)\cdot(5,8)\ ) = \varepsilon((2,2)\ ) = 4 \neq 40 \equiv 28\cdot 40 = \varepsilon(4,7)\cdot\varepsilon(5,8)$$

mert $4 \cdot 5 \equiv 2 \pmod{\mathbb{Z}_6}$, $7 \cdot 8 \equiv 2 \pmod{\mathbb{Z}_9}$ és $28 \cdot 40 \equiv 40 \pmod{\mathbb{Z}_{54}}$.

2.2.2) Izomorfizmusok: c), d) ;

Nem izomorfizmusok: a), e) /nem injektív/, b) /nem szürjektív/ ,

f) pontosan akkor izomorfizmus, ha $X = \{a\}$ egyelemű halmaz.

2.2.4) Tétel: $((\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +)) \cong (\mathbb{Z}_{m \cdot n}, +)$ *pontosan akkor ha* $lnko(n, m) = 1$ *(azaz n és m relatív prímek).* □

2.2.5) a)

$$\mathbb{Z}/_{(\equiv_m)} \cong \mathbb{Z}_m \quad \text{és} \quad (\mathbb{Z}, +, \cdot)\,/_{(\equiv_m)} \cong (\mathbb{Z}_m, +, \cdot) \quad .$$

b) $\bowtie$ *nem* kongruencia reláció.

3. fejezet

Félcsoportok és csoportok

3.1. Gruppoidok, félcsoportok

3.1.1) o) A valós számok kivonása és osztása nem kommutatív és nem asszociatív, a halmazok kivonása úgyszintén.

A szimmetrikus differencia nyilvánvalóan kommutatív.

Az asszociativitást könnyen beláthatjuk Venn-diagramokkal:

$$A \triangle (B \triangle C) = (A \backslash B \backslash C) \cup (B \backslash C \backslash A) \cup (C \backslash A \backslash B) \cup (A \cap B \cap C) =$$
$$= A \triangle (B \triangle C) \ .$$

a) $\diamond$ nyilván kommutatív, az asszociativitás közvetlenül számolható:

$$(x \diamond y) \diamond z = (x + y + xy) \diamond z = x + y + xy + z + (x + y + xy)\, z =$$
$$= x + y + xy + z + xz + yz + xyz \ ,$$

$$x \diamond (y \diamond z) = x \diamond (y + z + yz) = x + y + z + yz + x\,(y + z + yz) =$$
$$= x + y + z + yz + xy + xz + xyz \ .$$

Látható, hogy a két mennyiség azonos.

(Lásd még a 3.2.4) feladatot is.)

b) $[1, \infty)$ először is *zárt-e* a $\otimes$ műveletre? Ha $a, b \geq 1$, akkor nyilván $a \otimes b \geq a \cdot b \geq 1$, vagyis OK.

$\otimes$ nyilván kommutatív. Az asszociativitás közvetlen (kissé hosszadalmas) számolással is ellenőrizhető, vagy az alábbi észrevétel alapján: $a, b, c \geq 1$ esetén vannak olyan $x, y, z \in \mathbb{R}$ valós számok, amelyekre $a = ch(x)$, $b = ch(y)$ és $c = ch(z)$. Ekkor pedig (a hiperbolikus függvényekre

érvényes azonosságok alapján)

$$a \otimes b = ch(x) \otimes ch(y) = ch(x+y)$$

ami alapján[1)]

$$\begin{aligned}(a \otimes b) \otimes c &= ch(x+y) \otimes ch(z) = ch(x+y+z) = \\ &= ch(x) \otimes ch(y+z) = a \otimes (b \otimes c) \quad .\end{aligned}$$

c) Először a művelet zártságát ellenőrizzük: $0 < a, b < 1$ esetén teljesül-e $0 < \frac{a+b}{1-ab} < 1$? A kifejezés nyilván pozitív, így csak $\frac{a+b}{1-ab} < 1$ kell. Ez pedig

$\Leftrightarrow \quad a + b < 1 - ab$

$\Leftrightarrow \quad a - ab - +b - 1 < 0$

$\Leftrightarrow \quad (a-1)(1-b) < 0$.

Vagyis a $(0,1)$ halmaz zárt a $\boxtimes$ műveletre nézve.

Belátjuk, hogy $\boxtimes$ asszociatív:

$$\begin{aligned}(a \boxtimes b) \boxtimes c &= \frac{a+b}{1-ab} \boxtimes c = \frac{\frac{a+b}{1-ab} + c}{1 - \frac{a+b}{1-ab} \cdot c} \\ &= \frac{a+b+c\,(1-ab)}{(1-ab) - (a+b)\,c} \\ &= \frac{a+b+c-abc}{1-ab-ac-bc}\end{aligned}$$

míg

$$\begin{aligned}a \boxtimes (b \boxtimes c) &= a \boxtimes \frac{b+c}{1-bc} = \frac{a + \frac{b+c}{1-bc}}{1 - a \cdot \frac{b+c}{1-bc}} \\ &= \frac{a - abc + b + c}{1 - bc - ab - ac} \\ &= \frac{a+b+c-abc}{1-ab-ac-bc} \quad .\end{aligned}$$

[1)] A részleteket megtalálhatjuk a *Középiskolai Mat. Lapok* 2000.februári számában a 90. oldalon, az F.3185 feladat megoldásánál.

$a \boxtimes b := \frac{a+b}{1-ab}$ szemmel láthatóan kommutatív.

d) $lnko(m,n)$ nyilván kommutatív. Asszociatív is: a legnagyobb közös osztó definícióját kell csak alaposan átgondolnunk.

e) Az

$$lkkt(m,n) = \frac{m \cdot n}{lnko(m,n)}$$

összefüggés alapján $lkkt$ nyilván kommutatív. Asszociatív is: a legkisebb közös többszörös definícióját kell csak alaposan átgondolnunk.

f) $A \backslash B$ nem kommutatív és nem asszociatív.

g) $\max(x,y)$ és $\min(x,y)$ nyilván kommutatív. Asszociatív is, könnyen meggondolható: mindössze csak három, tetszőleges szám *összes* lehetséges sorrendjét (ez mennyi is?) kell megvizsgálnunk.

3.1.2) a), b), d), e), g) igen; c), f), i), j), h) nem.

3.1.6) b) $\mathbb{R}^{\mathbb{R}}_{Lin}$ zárt a $\circ$ (kompozíció) műveletére:

$f(x) = ax + b$ és $g(x) = cx + d$ esetén

$$(f \circ g)(x) = a \cdot (cx + d) + b = (ac) \cdot x + (ad + b) \ ,$$

így $\left(\mathbb{R}^{\mathbb{R}}_{Lin}, \circ\right)$ rész-félcsoportja $\left(\mathbb{R}^{\mathbb{R}}, \circ\right)$ -nek.

$\underset{\sim}{0} := 0 \cdot x + 0$ zéruselem, vagyis nincs inverze, $\mathbb{R}^{\mathbb{R}}_{Lin} \backslash \{\underset{\sim}{0}\}$ azonban már csoport.

$\mathbb{R}^{\mathbb{R}}_{LinRac}$ is zárt a $\circ$ (kompozíció) műveletére:

$f(x) = \frac{ax+b}{cx+d}$ és $g(x) = \frac{\alpha x+\beta}{\gamma x+\delta}$ esetén

$$(f \circ g)(x) = \frac{a\frac{\alpha x+\beta}{\gamma x+\delta} + b}{c\frac{\alpha x+\beta}{\gamma x+\delta} + d} = \frac{(a\alpha + b\gamma) \cdot x + (a\beta + b\delta)}{(c\alpha + d\gamma) \cdot x + (c\beta + d\delta)} \quad \in \mathbb{R}^{\mathbb{R}}_{LinRac}$$

hiszen

$|c\alpha + d\gamma| + |c\beta + d\delta| \neq 0$ mert $|c| + |d| \neq 0$ és $|\gamma| + |\delta| \neq 0$.

c) $\mathbb{R}^{\mathbb{R}}_{Lin}$ könnyen láthatóan zárt a + műveletre:

$$(ax + b) + (cx + d) = (a + c) \cdot x + (b + d) \quad ,$$

míg $\mathbb{R}^{\mathbb{R}}_{LinRac}$ nem:

$$\frac{ax+b}{cx+d}+\frac{\alpha x+\beta}{\gamma x+\delta}=.... \quad \text{(HF)} \ .$$

3.1.8) a) Mivel a mátrixok szorzása *nem* kommutatív, ezért általában csak annyit tudunk, hogy

$$(A\cdot B)^5=A\cdot B\cdot A\cdot B\cdot A\cdot B\cdot A\cdot B\cdot A\cdot B \ ,$$

és általában $(A\cdot B)^5\neq A^5\cdot B^5$!
Természetesen *konkrét mátrixoknál* használhatjuk a következő módszert[2)]:

$$\left(\left[\begin{array}{cc}2&5\\3&4\end{array}\right]\cdot\left[\begin{array}{cc}7&1\\6&8\end{array}\right]\right)^5=\left[\begin{array}{cc}44&42\\45&35\end{array}\right]^5=$$

$$=\left[\begin{array}{cc}44&42\\45&35\end{array}\right]\cdot\left[\begin{array}{cc}44&42\\45&35\end{array}\right]\cdot\left[\begin{array}{cc}44&42\\45&35\end{array}\right]\cdot\left[\begin{array}{cc}44&42\\45&35\end{array}\right]\cdot\left[\begin{array}{cc}44&42\\45&35\end{array}\right] \ .$$

b) Mivel a függvények kompozíciója sem kommutatív, ezért általában csak annyit tudunk, hogy ("kompozícióhatványok")

$$(f\circ g)^5=f\circ g\circ f\circ g\circ f\circ g\circ f\circ g\circ f\circ g$$

vagyis

$$(f\circ g)^5(x)=f\left(g\left(f\left(g\left(f\left(g\left(f\left(g\left(f\left(g\left(x\right)\right)\right)\right)\right)\right)\right)\right)\right)\right) \ ,$$

például

$$(\sin\circ\lg)^5(x)=\sin\left(\lg\left(\sin\left(\lg\left(\sin\left(\lg\left(\sin\left(\lg\left(\sin\left(\lg\left(x\right)\right)\right)\right)\right)\right)\right)\right)\right)\right) \ ,$$

vagy

$$\left(\cos\circ\sqrt{\ }\right)^3=\cos\circ\sqrt{\ }\circ\cos\circ\sqrt{\ }\circ\cos\circ\sqrt{\ } \ ,$$

azaz

$$\left(\cos\circ\sqrt{\ }\right)^3(x)=\cos\left(\sqrt{\cos\left(\sqrt{\cos\left(\sqrt{x}\right)}\right)}\right) .$$

[2)] **Diagonalizálható mátrixok** [amelyek hasonlóak egy diagonális mátrixhoz, lásd az 1.2.2) m_2) feladatot] magasabb hatványai könnyen kiszámolhatók, sajátvektoraik és sajátvektoraik segítségével. Ennek részleteit megtaláljuk például a [$SzI'01$] könyv "*Magasabbrendű rekurziók*" fejezetében.

c) Ha $p(x) = x^2 + 4x - 5$ akkor (ismét "kompozícióhatványok")

$$\begin{aligned}(p \circ p)(x) &= p(p(x)) = \left(x^2+4x-5\right)^2 + 4 \cdot \left(x^2+4x-5\right) - 5 = \\ &= x^4 + 8x^3 + 10x^2 - 24x\end{aligned}$$

és

$$\begin{aligned}(p \circ p \circ p)(x) &= p(p(p(x))) = \\ &= \left[\left(x^2+4x-5\right)^2 + 4\left(x^2+4x-5\right) - 5\right]^2 + \\ &\quad +4 \cdot \left[\left(\left(x^2+4x-5\right)\right)^2 + 4\left(\left(x^2+4x-5\right)\right) - 5\right] - 5 \\ &= x^8 + 16x^7 + 84x^6 + 112x^5 - 280x^4 - 448x^3 + 616x^2 - 96x - 5\ ,\end{aligned}$$

továbbá

$$\begin{aligned}(p \circ q)(x) &= p(q(x)) = (7-9x)^2 + 4 \cdot (7-9x) - 5 = \\ &= 81x^2 - 162x + 72\ ,\end{aligned}$$

és

$$\begin{aligned}(p \circ q)^2(x) &= (p \circ q \circ p \circ q)(x) = p(q(p(q(x)))) = \\ &= \left[7 - 9\left((7-9x)^2 + 4 \cdot (7-9x) - 5\right)\right]^2 + \\ &\quad +4 \cdot \left[7 - 9\left((7-9x)^2 + 4 \cdot (7-9x) - 5\right)\right] - 5 \\ &= 531\,441x^4 - 2125\,764x^3 + 3057\,426x^2 - 1863\,324x + 408\,312\ .\end{aligned}$$

d) Mivel $\cdot$ a "szokásos" szorzás, ami ráadásul kommutatív, ezért $\mathbb{R}[x]$ -ben $(p(x))^3 = p(x) \cdot p(x) \cdot p(x)$ és (például) $(p(x) \cdot q(x))^5 = p(x)^5 \cdot q(x)^5$.

A c) -beli polinomokkal:

$$\begin{aligned}\left(x^2+4x-5\right)^3 &= \left(x^2+4x-5\right) \cdot \left(x^2+4x-5\right) \cdot \left(x^2+4x-5\right) \\ &= x^6 + 12x^5 + 33x^4 - 56x^3 - 165x^2 + 300x - 125\end{aligned}$$

és

$$\begin{aligned}\left(\left(x^2+4x-5\right) \cdot (7-9x)\right)^5 &= \left(-9x^3 - 29x^2 + 73x - 35\right)^5 \\ &= -59\,049x^{15} - 951\,345x^{14} - 3736\,125x^{13} + ...\end{aligned}$$

vagy másképpen

$$\begin{aligned} &= \big(\big(x^2+4x-5\big)\cdot(7-9x)\big)^5 = \big(x^2+4x-5\big)^5\cdot(7-9x)^5 \\ &= \big(x^{10}+20x^9+135x^8+...\big)\cdot\big(-59\,049x^5+229\,635x^4-357\,210x^3+...\big) \\ &= -59\,049x^{15}-951\,345x^{14}-3736\,125x^{13}+... \end{aligned}$$

e) $\mathbb{C}[x]$ -ben is kommutatív a (szokásos) $\cdot$ szorzás, ezért $u^5 = u\cdot u\cdot u\cdot u\cdot u$ és $(uv)^5 = u^5v^5$. Tehát például

$$\begin{aligned} (2+i)^5 &= (2+i)\cdot(2+i)\cdot(2+i)\cdot(2+i)\cdot(2+i) \\ &= -38+41i \end{aligned}$$

és

$$((2+i)\cdot(5-3i))^5 = (2+i)^5\cdot(5-3i)^5 = 349\,388-141\,116i\ ,$$

vagy másképpen:

$$((2+i)\cdot(5-3i))^5 = (13-i)^5 = 349\,388-141\,116i\ .$$

Lásd még a 3.4."*Szimmetria- és szimmetrikus csoportok*" fejezetben a permutációk hatványaira és felcserélhetőségére vonatkozó feladatokat is.

3.2. Speciális elemek félcsoportokban

3.2.2) a) $\mathcal{A}_\circ := (A^A, \circ)$ -ban: id_A kétoldali *egységelem*,

a $\underset{\sim}{c}$ konstans függvények a baloldali zéruselemek, jobboldali *zéruselem* nincs,
$f : A \to A$ pontosan akkor *baloldali* nullosztó ha *nem* injektív,
$g : A \to A$ pontosan akkor *jobboldali* nullosztó ha *nem* szürjektív.

Az $f : A \to A$ függvénnyel pontosan akkor lehet balról *egyszerűsíteni*, ha injektív, jobbról pontosan akkor ha szürjektív.

Baloldali *inverze* pontosan csak az injektív függvényeknek van, jobboldali pedig pontosan a szürjektíveknek. Csak a bijekcióknak (=permutációknak) van egyértelmű (bármely oldali) inverze, ami egyúttal kétoldali inverz is.

3.2.4) a) A $\diamond$ művelet nyilván kommutatív. Az asszociativitást az 1.1)a) feladatban már beláttuk.

b) e *egységelem*, ha $e \diamond x = x$, azaz $e + x + ex = x$ *minden* x valós számra. Csak $e = 0$ jó megoldás, azaz $(\mathbb{R}, \diamond)$ egységeleme: $e = 0$.

z *zéruselem*, ha $z \diamond x = z$, azaz $z + x + zx = z$ *minden* x valós számra. Ennek megoldása: $z = -1$.

$a \in \mathbb{R}$ *nullosztó*, ha $a \neq -1$ és van olyan $b \in \mathbb{R}$, $b \neq -1$, amelyre

$$a \diamond b = a + b + ab = a\,(1 + b) + b = -1 \ ,$$

amely egyenlőség csak $a = \frac{-1-b}{1+b} = -1$ esetén teljesülne, vagyis $(\mathbb{R}, \diamond)$ -ben *nincs nullosztó.*

$a \neq -1$ esetén a *inverze* $b \neq -1$ akkor, ha $a \diamond b = e$, azaz

$$a \diamond b = a + b + ab = a + (1 + a)b = 0$$

vagyis

$$a^{-1} = b = \frac{-a}{1 + a} \quad .$$

c) Az előzőek alapján csak azt kell ellenőriznünk, hogy az $\mathbb{R}\backslash\{-1\}$ halmaz zárt a $\diamond$ műveletre. Vagyis azt kell megmutatnunk, hogy $x, y \neq -1$ esetén $x \diamond y \neq -1$.

Márpedig, ha $x \neq -1$, akkor könnyen ellenőrizhető, hogy

$$x \diamond y = x + y + xy = x + (1 + x)y = -1$$

pontosan akkor teljesül, ha

$$y = \frac{-1 - x}{1 + x} = -1 \quad .$$

Vagyis a $(\mathbb{R}\backslash\{-1\}, \diamond)$ struktúra valóban Abel csoport, egységeleme $e = 0$.

3.2.5) o) $(2 \cdot \mathbb{Z}, \cdot)$ -ben nincs *idempotens* elem.

a) Például $(\mathbb{Z}_{10}, \cdot)$ -ben: 0, 1, 5, 6 .

b) $(\mathbb{R}^{n\times n},\cdot)$ -ben például olyan átlós (diagonális) mátrixok amelynek főátlójában csak 0 vagy 1 áll; vagy egy olyan mátrix, amelynek minden eleme 0 kivéve egyetlen sorát vagy oszlopát amelyben csupa 1 áll.

c) $\left(\mathbb{R}^{\mathbb{R}},\circ\right)$ vagy általában $\left(A^A,\circ\right)$ -ben $f\in A^A$ idempotens például akkor, ha f felcseréli A két pontját: $f(a)=b$ és $f(b)=a$, továbbá f fixen hagyja A többi elemét: $f(x)=x$.

Általában pedig $f\in A^A$ pontosan akkor idempotens, ha $A=\bigcup_{i\in I}\{x_i,y_i\}$ (legfeljebb) kételemű halmazokra partícionálható, amelyekre $f(x_i)=y_i$ és $f(y_i)=x_i$ minden $i\in I$ esetén.

d) $\mathcal{S}_n$ -ben egy elem (permutáció) pontosan akkor idempotens, ha felbomlik *diszjunkt transzpozíciók* szorzatára.

e) $\left(\left(\mathbb{R}^2\right)^{\left(\mathbb{R}^2\right)},\circ\right)$ -ben (=geometriai leképezések csoportja) például: egyenesre vagy pontra való tükrözés, inverzió, stb.

f) X *minden* részhalmaza idempotens mindkét műveletre nézve, hiszen $A\cup A=A$ és $A\cap A=A$.

g) Bármely $(G,\cdot)$ *csoportban* csak az egységelem idempotens, hiszen az $x\cdot x=x$ egyenletet x^{-1} -el szorozva kapjuk, hogy $x=e$.

3.2.6) Például: $P(X)$ -ben: $\bar{X}$ (komplementer), $\mathbb{C}$ -ben: $\bar{z}$ (konjugált), $\mathbb{R}$ -ben: $x\mapsto(-x)$, .stb.

3.2.7) $f\in A^A$ önmaga inverze például akkor, ha f felcseréli A két elemét: $f(x)=y$ és $f(y)=x$, és A többi elemét fixen hagyja (azaz $f(a)=a$) .

Általában pedig $f\in A^A$ pontosan akkor önmaga inverze, ha

$$A=\bigcup_{i\in I}\{x_i,y_i\}$$

(legfeljebb) kételemű halmazokra partícionálható (vagyis $x_i=y_i$ is megengedett), amelyekre

$$f(x_i)=y_i \text{ és } f(y_i)=x_i \quad \forall i\in I\ .$$

3.2.8) Az egységelemek id_A és $E\in\mathbb{R}^{n\times n}$, sőt λE is *minden* elemmel kommutálnak.

A diagonális mátrixok *egymással* kommutálnak, hiszen

$$\begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & ... & 0 \\ 0 & 0 & \lambda_n \end{bmatrix} \cdot \begin{bmatrix} \mu_1 & 0 & 0 \\ 0 & ... & 0 \\ 0 & 0 & \mu_n \end{bmatrix} = \begin{bmatrix} \lambda_1\mu_1 & 0 & 0 \\ 0 & ... & 0 \\ 0 & 0 & \lambda_n\mu_n \end{bmatrix} .$$

3.3. Csoportok

3.3.1) Csoportok: b), c), f), g2), h), nem csoportok: a), d), e), g1) .

Speciálisan: f) -ben $\emptyset$ az egységelem, és minden $A \subseteq X$ halmaz "inverze" önmaga: $A \triangle A = \emptyset$.

3.3.2) Általában: $(\mathbb{Z}_m, +)$ *csoport minden* $m \in \mathbb{N}$ *számra, míg* $(\mathbb{Z}_m, \cdot)$ pontosan akkor *csoport, ha* $m \in \mathbb{P}$ *prímszám.* $\square$

3.3.5) e) Általában: Legyen $m, n \in \mathbb{Z}$ tetszőleges, relatív prím számok, azaz $n \in \mathbb{Z}_m^*$. n multiplikatív inverze olyan $x \in \mathbb{Z}_m^*$ szám, amelyre $nx \equiv 1 \pmod{m}$, azaz $nx - my = 1$. A 4.3.4 "*Lineáris Diophantikus egyenletek*" c. fejezetben megtaláljuk a folytatást: x és y léteznek, sőt könnyen (gyorsan) ki is számolhatók.

3.3.7) a) a komplex egységgyökök: $z^n = 1$ megoldásai ahol $n \in \mathbb{N}$ tetszőleges természetes szám.

b) csak $id_{[0,1]}$.

3.3.8) Igen.

3.3.9) c) Az egyenleteket a szokásos "*mérleg-elv*[3)]" segítségével oldhatjuk meg:

$$\begin{aligned} axbcx &= abx \qquad / \cdot x^{-1} \text{ jobbról} \\ axbc &= ab \qquad / \cdot a^{-1} \text{ balról} \\ xbc &= b \qquad / \cdot (bc)^{-1} \text{ jobbról} \\ x &= b \cdot (bc)^{-1} \\ \text{átalakítva} \quad x &= b \cdot c^{-1} \cdot b^{-1} \end{aligned}$$

[3)] ld. az általános iskola alsó tagozat matek tananyagot.

illetve

$$\begin{aligned} yay &= bba^{-1} \qquad / \cdot a \text{ jobbról} \\ (ya)^2 &= b^2 \\ \textit{egyik gyök} \quad ya &= b \\ \text{vagyis} \quad y &= ba^{-1} \quad . \end{aligned}$$

a) és **b)** A fentiek alapján

$X = B(BC)^{-1} = BC^{-1}B^{-1}$, $f = b \circ (b \circ c)^{-1} = b \circ c^{-1} \circ b^{-1}$

illetve

$Y = BA^{-1}$ és $g = b \circ a^{-1}$.

3.3.11) d) Általában: $(\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +) \cong (\mathbb{Z}_{mn}, +)$ pontosan akkor ha $lnko(m, n) = 1$ (azaz m és n relatív prímek).

3.3.12) Alkalmazzuk az előző (3.11)d)) feladat eredményét és az *Abel csoportok Alaptételét*[4)].

12 eleműek $(\mathbb{Z}_{12}, +)$ és $(\mathbb{Z}_2, +) \times (\mathbb{Z}_6, +)$,

15 elemű csak $(\mathbb{Z}_{15}, +)$ (mert 3 és 5 relatív prímek),

19 elemű csak $(\mathbb{Z}_{19}, +)$ (mert 19 prímszám),

20 eleműek $(\mathbb{Z}_{20}, +)$ és $(\mathbb{Z}_2, +) \times (\mathbb{Z}_{10}, +)$,

27 eleműek $(\mathbb{Z}_{27}, +)$, $(\mathbb{Z}_3, +) \times (\mathbb{Z}_9, +)$ és $(\mathbb{Z}_3, +) \times (\mathbb{Z}_3, +) \times (\mathbb{Z}_3, +)$,

30 elemű csak $(\mathbb{Z}_{30}, +)$.

Általában: *Négyzetmentes*[5)] $n \in \mathbb{N}$ *számok esetén csak egyetlen* n *-elemű Abel csoport van:* $(\mathbb{Z}_n, +)$ □

[4)] **Abel csoportok Alaptétele:** *Tetszőleges* $(G, \cdot)$ *Abel-csoport izomorf prímhatvány rendű ciklikus csoportok* (*azaz* $(\mathbb{Z}_q, +)$ ahol $q = p^\alpha$) *direkt szorzatával.* □

Véges sok struktúra *direkt szorzata* megegyezik a Descartes -szorzatukkal.

[5)] **Definíció:** *Az* $n \in \mathbb{N}$ *szám* **négyzetmentes**, *ha nincs négyzetszám osztója:* nincs *olyan* $x \in \mathbb{N}$ *amelyre* $x^2 \mid n$ *lenne.* □

n nyilván akkor és csak akkor négyzetmentes, ha minden prímosztója első hatványon szerepel: $n = p_1 p_2 ... p_t$ ahol p_i különböző prímszámok. □

3.3.14) Bizonyítás nélkül felsorolunk pár idevágó tételt:

i) TÉTEL: *Prímrendű csoport ($n = p$ prímszám) mindig ciklikus, azaz csak $\mathbb{Z}_p$ lehet.* □

ii) TÉTEL: *Minden prímnégyzetrendű csoport ($n = p^2$) kommutatív.*□

iii) TÉTEL: $n = 2p$ ($p \in \mathbb{P}$ *páratlan prímszám*) - *rendű csoport csak* $\mathbb{Z}_{2p}$ *vagy* $\mathbb{D}_p$ (*diédercsoport*) *lehet.* □

iv) TÉTEL: 8 -*adrendű nemkommutatív csoport csak* D_4 *vagy* $\mathcal{Q}$ *(a kvaterniócsoport) lehet.* □

v) TÉTEL: 12 -*drendű csoport csak* $\mathbb{Z}_{12}$, $\mathbb{Z}_2 \times \mathbb{Z}_6$, A_4 (*alternáló csoport*), D_6 *vagy a következő*

$$[\, a, b \,:\, a^3 = b^2 \neq 1, b^4 = baba = 1 \,]$$

csoport lehet. □

vi) TÉTEL: 15 -*drendű csoport csak* $\mathbb{Z}_{15}$ *(a ciklikus csoport) lehet.* □

vii) TÉTEL: 16 -*drendű (páronként nem izomorf) csoport* 14 -*féle van: öt kommutatív, a nemkommutatívak közül öt exponense* 4*, négynek az exponense* 8 . □

viii) TÉTEL: 18 -*rendű (páronként nem izomorf) csoport* 5-*féle van.*□

3.4. Szimmetria- és szimmetrikus csoportok

3.4.0) Könyveket, tárgyakat pakolgatunk a polcon, a lakásban, a raktárban; kártyalapokat a kezünkben vagy pakliban (megkeverjük), az asztalon; gyermekek labdákat, virágokat dobálgatnak egymásnak; egy *teljes* irányított gráf, amin bábukkal lépegetünk, stb. Egy rögzített H halmaz egy tetszőleges $f : H \to H$ *bijekciója* esetén az $x \longmapsto y$ hozzárendelések.

Hangsúlyozzuk, hogy minden esetben csak az a lényeg: *melyik helyről melyik másik helyre* tesszük az éppen ott levő (bármilyen) tárgyakat, és az lényegtelen, hogy mik ezek a tárgyak! Természetesen minden helyen pontosan egy tárgy lehet, és minden tárgynak valamelyik helyen lennie kell. Tehát az $f(x) = y$ azaz $x \longmapsto y$ hozzárendelés azt jelenti, hogy az x *helyről* rakunk valamit (nem érdekes, hogy mit) az y *helyre*!

A számítógép működés közben memóriarekeszeinek tartalmát "pakolgatja". Sajnos ez nem igazi permutáció, mert például az A:=B utasításkor az A rekesz *tartalma* törlődik. Ha azonban úgy képzeljük a számítógépet, hogy az ilyen esetekben az A rekesz tartalma valamely C rekeszbe kerülne át (és C tartalma egy D -be, ...), akkor egy programunk is permutáció lenne. Ismét nem az a lényeg, hogy mit teszünk odébb, hanem az, hogy *honnan hová*, de ezt előre, a program írásakor még nem is tudjuk! Tehát a permutációcsoportokról tanultak jó közelítéssel a számítógép programokra is igazak.

3.4.1) a) A szabályos n -szög szimmetriacsoportja a D_n ún. **diéder csoport** :

$$D_n := [\{f, t\}] = \{id, f, f^2, ..., f^{n-1}, t, tf, tf^2, ..., tf^{n-1}\}$$

ahol f egy n -edrendű forgatás és t egy (másodrendű) tengelyes tükrözés, és D_n ezen két elem által generált csoport.

Vegyük észre, hogy D_n elemeinek száma: $|D_n| = 2n$.

b) A *kör* transzformációcsoportja

$$D_\infty := [\{f, t\}] = \{f^r, tf^r : r \in \mathbb{R}\}$$

ahol f egy ∞ -edrendű forgatás és t egy (másodrendű) tengelyes tükrözés, és D_∞ e két elem által generált csoport, a ∞ -rendű **diédercsoport**,

3.4.2) a) Például a *téglalap* transzformációcsoportja (ha a csúcsait körbejárva számozzuk 1,2,3,4 -gyel):

$$\mathcal{T}\left(\begin{smallmatrix}1&&2\\4&&3\end{smallmatrix}\right) = \left\{id, \begin{pmatrix}1234\\4321\end{pmatrix}, \begin{pmatrix}1234\\2143\end{pmatrix}, \begin{pmatrix}1234\\3412\end{pmatrix}\right\}$$

amely elemek rendre megfelelnek[6)] a helybenhagyásnak, a vízszintes- és függőleges tengelyre való tükrözésnek, és a 180^o -os elforgatásnak. Tehát $\mathcal{T}$ egy 4 -elemű részcsoportja S_4 -nek: $\mathcal{T} \leq S_4$.

A *négyzet* transzformációcsoportja (hasonló számozással) egy 8 -elemű részcsoportja S_4 -nek:

$$\begin{aligned}\mathcal{T}\left(\begin{smallmatrix}1&&2\\4&&3\end{smallmatrix}\right) &= D_4 = \\ &= \left\{id, \begin{pmatrix}1234\\4123\end{pmatrix}, \begin{pmatrix}1234\\3412\end{pmatrix}, \begin{pmatrix}1234\\2341\end{pmatrix}, \begin{pmatrix}1234\\4321\end{pmatrix}, \begin{pmatrix}1234\\3214\end{pmatrix}, \begin{pmatrix}1234\\2143\end{pmatrix}, \begin{pmatrix}1234\\1432\end{pmatrix}\right\}.\end{aligned}$$

[6)] Az $\left(\begin{smallmatrix}...i...\\...j...\end{smallmatrix}\right)$ permutáció azt rövidíti, hogy az i jelű csúcs a j jelű csúcs helyére kerül.

Vegyük észre, hogy

$$\mathcal{T}\left(\begin{smallmatrix}1&&&2\\4&&&3\end{smallmatrix}\right) \leq \mathcal{T}\left(\begin{smallmatrix}1&\square&2\\4&&3\end{smallmatrix}\right) \leq S_4$$

egymás részcsoportjai.

b) A permutáció az **1** és **3** csúcsokat helybenhagyja, a **2** és **4** csúcsokat felcseréli, tehát az **1-3** átlóra való tükrözésre gondolhatnánk. Azonban egy általános téglalap *nem* szimmetrikus egyik átlójára sem, vagyis $\left(\begin{smallmatrix}1&2&3&4\\1&4&3&2\end{smallmatrix}\right)$ **nem** szimmetriája a téglalapnak, azaz $\left(\begin{smallmatrix}1&2&3&4\\1&4&3&2\end{smallmatrix}\right) \notin \mathcal{T}\left(\begin{smallmatrix}1&&&2\\4&&&3\end{smallmatrix}\right)$.

Négyzet esetében azonban $\left(\begin{smallmatrix}1&2&3&4\\1&4&3&2\end{smallmatrix}\right)$ valóban az **1-3** átlóra való tükrözés, vagyis $\left(\begin{smallmatrix}1&2&3&4\\1&4&3&2\end{smallmatrix}\right) \in \mathcal{T}\left(\begin{smallmatrix}1&\square&2\\4&&3\end{smallmatrix}\right)$.

3.4.3) a) b) $\mathcal{S}_3 = \left\{\left(\begin{smallmatrix}123\\123\end{smallmatrix}\right), \left(\begin{smallmatrix}123\\132\end{smallmatrix}\right), \left(\begin{smallmatrix}123\\213\end{smallmatrix}\right), \left(\begin{smallmatrix}123\\231\end{smallmatrix}\right), \left(\begin{smallmatrix}123\\312\end{smallmatrix}\right), \left(\begin{smallmatrix}123\\321\end{smallmatrix}\right)\right\}$

ahol $\left(\begin{smallmatrix}123\\123\end{smallmatrix}\right) = id$,

kételemű ciklusok (transzpozíciók): $\left(\begin{smallmatrix}123\\132\end{smallmatrix}\right) = (2,3) = (3,2) = a$,

$\left(\begin{smallmatrix}123\\213\end{smallmatrix}\right) = (1,2) = (2,1) = b$, $\left(\begin{smallmatrix}123\\321\end{smallmatrix}\right) = (1,3) = (3,1) = e$,

háromelemű ciklusok: $\left(\begin{smallmatrix}123\\231\end{smallmatrix}\right) = (1,2,3) = c$ $(= (2,3,1) = (3,1,2))$

és $\left(\begin{smallmatrix}123\\312\end{smallmatrix}\right) = (1,3,2) = d = \left(\begin{smallmatrix}123\\231\end{smallmatrix}\right)^{-1} = (3,2,1)$ $(= (2,1,3))$,

$\circ$	id	$(2,3)$	$(1,2)$	$(1,2,3)$	$(3,2,1)$	$(1,3)$
id	id	$(2,3)$	$(1,2)$	$(1,2,3)$	$(3,2,1)$	$(1,3)$
$(2,3)$	$(2,3)$	id	$(1,3,2)$	$(1,3)$	$(2,1)$	$(1,2,3)$
$(1,2)$	$(1,2)$	$(2,3,1)$	id	$(2,3)$	$(2,3)$	$(1,3,2)$
$(1,2,3)$	$(1,2,3)$	$(2,1)$	$(1,3)$	$(1,3,2)$	id	$(2,3)$
$(3,2,1)$	$(3,2,1)$	$(3,1)$	$(2,3)$	id	$(3,1,2)$	$(1,2)$
$(1,3)$	$(1,3)$	$(2,1,3)$	$(1,2,3)$	$(1,2)$	$(3,2)$	id

(Ne feledjük: függvények kompozíciójánál

$$(f \circ g)(x) = f(g(x)) \quad ,$$

vagy algebrai jelöléssel ugyanez: $x(g \cdot f) = xgf = (xg)f$.

Ha az

$$\mathcal{S}_3 = \{id, a, b, c, d, e\} \tag{3.1}$$

jelölést kívánjuk használni, akkor

$\circ$	id	a	b	c	d	e
id	id	a	b	c	d	e
a	a	id	d	e	b	c
b	b	c	id	a	e	d
c	c	b	e	d	id	a
d	d	e	a	id	c	b
e	e	d	c	b	a	id

.

Látható, hogy $\mathcal{S}_3$ *nem* kommutatív.

c) Jelölje σ a $\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)$ permutációt, azaz legyen $H := \{id, \sigma\}$. Nyilván csak azt kell ellenőriznünk, hogy $\sigma^2 \in H$, de $\sigma^2 = id \in H$, tehát H valóban részcsoportja $\mathcal{S}_3$ -nak (zárt a kompozíció műveletére).

d) Természetesen

$$H \cdot id = id \cdot H = H$$

és $\sigma^2 = id$ miatt

$$H \cdot \sigma = \sigma \cdot H = H \quad .$$

A többi jobboldali mellékosztály:

$$\begin{aligned} J_1 &= H \cdot \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right) = H \cdot \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right) = \left\{\left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right)\right\} \ , \\ J_2 &= H \cdot \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) = H \cdot \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right) = \left\{\left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)\right\} \ , \end{aligned}$$

baloldali mellékosztályok:

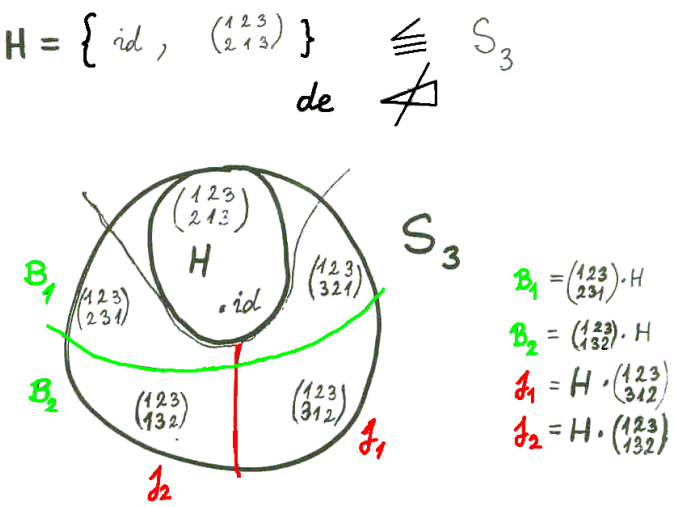
$$\begin{aligned} B_1 &= \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) \cdot H = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right) \cdot H = \left\{\left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)\right\} \ , \\ B_2 &= \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right) \cdot H = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right) \cdot H = \left\{\left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)\right\} \ , \end{aligned}$$

vagy az (3.1) jelölést használva

$$\begin{aligned} B_1 &= c \circ H = \{c, e\} = e \circ H \ , \\ B_2 &= a \circ H = \{a, d\} = d \circ H \end{aligned}$$

és

$$\begin{aligned} J_1 &= H \circ d = \{d, e\} = H \circ e \ , \\ J_2 &= H \circ a = \{a, c\} = H \circ c \ . \end{aligned}$$



S_3 mellékosztályai

Látható, hogy H *nem* normálosztója $\mathcal{S}_3$ -nak.

3.4.4)

$$A_4 = \{\, id,\ (12)(34),\ (13)(24),\ (14)(23),\ (123),\ (132),\ (124),\ (142),\ (134),\ (143),\ (234),\ (243) \,\}$$

és A_n mindig $n!/2$ elemű részcsoportja S_n -nek.

3.4.5) $\sigma_1 = (1,5,4,3,2)$, minden elem pályája az $\{1,2,3,4,5\}$ halmaz,

$\sigma_2 = (1,3)\circ(4,5)$, az $1,3$ elemek pályája az $\{1,3\}$ halmaz, a $4,5$ elemek pályája az $\{4,5\}$ halmaz, a 2 elem fixpont, így pályája a $\{2\}$ egyelemű halmaz (singleton[7]),

$\sigma_3 = (1,4,3)\circ(5,6)$,

$\sigma_4 = (1,5,3,2)\circ(4,6)$,

$\sigma_5 = (1,5,4,6,2)\circ(3,8)\circ(7,14,11,15,9)\circ(10,12)\circ(13)$,

az $1,2,4,5,6$ elemek pályája az $\{1,2,4,5,6\}$ halmaz,

[7] **singleton** = egyelemű halmaz (single (ang.), azaz "szingli")

a $3, 8$ elemek pályája a $\{3, 8\}$ halmaz,

a $7, 9, 11, 14, 15$ elemek pályája a $\{7, 9, 11, 14, 15\}$ halmaz,

a $10, 12$ elemek pályája a $\{10, 12\}$ halmaz, $\qquad T_{\sigma_5}(3) = \{3\}$,

$\sigma_6 = (1, 2, 4, 5, 8, 9, 6, 3) \circ (7, 10)$,

$\sigma_7 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 3\,2\,7\,1\,6\,4\,5 \end{pmatrix}$,

$\sigma_8 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 3\,4\,2\,1\,5\,6\,8\,7 \end{pmatrix}$,

$\sigma_9 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 2 & 5 & 1 & 3 & 10 & 11 & 7 & 16 & 14 & 4 & 8 & 9 & 17 & 18 & 12 & 19 & 13 & 20 & 6 & 15 \end{pmatrix}$,

$\sigma_{10} = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 3\,4\,2\,1\,5\,6\,8\,7 \end{pmatrix}$.

3.4.6) Minden ciklus = egy (leglább kételemű) részhalmaz valamilyen sorrendben - körben. A lehetőségek száma:

$$\sum_{k=2}^{n} \binom{n}{k} \frac{k!}{k} \quad .$$

3.4.7) "Mindössze" csak a permutáció *értelmezési tartományát* (felső sor) és *értékkészletét* (alsó sor) kell felcserélnünk (és persze az új értelmezési tartományt sorba rakni). Például, σ_5 esetében:

$$(\sigma_5)^{-1} = \begin{pmatrix} 5\,1\,8\,6\,4\,2\,14\,3\,7\,12\,15\,10\,13\,11\,9 \\ 1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15 \\ 2\,6\,8\,5\,1\,4\,9\,3\,15\,12\,14\,10\,13\,7\,11 \end{pmatrix} .$$

Más lehetőség: ciklusokra bontás után csak megfordítjuk a ciklusok belsejét (a nyilakat)[8] (vagyis a labdát visszafelé dobják a gyerekek)**:**

$\sigma_5 = (1, 5, 4, 6, 2) \circ (3, 8) \circ (7, 14, 11, 15, 9) \circ (10, 12) \circ (13)$

és

$\sigma_5^{-1} = (2, 6, 4, 5, 1) \circ (3, 8) \circ (9, 15, 11, 14, 7) \circ (10, 12)$.

Ne feledjük, hogy tetszőleges $\quad \tau = (i, j) \quad$ transzpozícióra[9]

$$\tau = \tau^{-1} = (i, j) = (j, i)$$

és egyelemű ciklusokat nem szoktunk kiírni[10] .

---

[8] Vegyük észre, hogy *diszjunkt* permutációk (ciklusok) esetében $\circ$ és $\cdot$ közül bármelyiket írhatjuk, és a *diszjunkt* permutációk sorrendje is lényegtelen, hiszen ezek a permutációk kommutálnak (felcserélhetők).

[9] **Def.**: **transzpozíció** *:= kételemű ciklus.* □

[10] hiszen minden egyelemű ciklus $\quad (i) = id$.

3.4.8) Mivel $\rho = (1,3,7,5,6,4) \circ (2)$, ezért (kis fejszámolás után)

$\rho^1 = (1,3,7,5,6,4)$, $\rho^{-1} = (1,4,6,5,7,3)$,
$\rho^2 = (1,7,6) \circ (3,5,4)$, $\rho^{-2} = (1,6,7) \circ (3,4,5)$,
$\rho^3 = (1,5) \circ (3,6) \circ (4,7)$, $\rho^{-3} = (1,5) \circ (3,6) \circ (7,4)$,
$\rho^4 = (1,6,7) \circ (3,4,5)$, $\rho^{-4} = (1,7,6) \circ (3,5,4)$,
$\rho^5 = (1,4,6,5,7,3)$, $\rho^{-5} = (1,3,7,5,6,4)$,

továbbá

$$\rho^6 = id \quad \textit{és} \quad \rho^{6k+i} = \rho^i \qquad (\forall k, i \in \mathbb{Z}) \tag{3.2}$$

mert

$$\rho^{6k+i} = \left(\rho^6\right)^k \circ \rho^i = (id)^k \circ \rho^i = \rho^i \qquad (\forall k, i \in \mathbb{Z}) \quad .$$

Tehát ρ *rendje* $o(\rho) = 6$.

Vegyük észre továbbá, hogy pl. $\rho^2 = \rho^{-4}$, $\rho^5 = \rho^{-1}$, $\rho^3 = \rho^{-3}$, s.í.t., hiszen $\rho^6 = id_6$, és így általában

$$\rho^i = \rho^{i-6} \quad (\forall i \in \mathbb{Z}) \tag{3.3}$$

tetszőleges $i \in \mathbb{N}$ kitevőre. Ez amiatt van, mert (3.2) szerint $\rho^i \circ \rho^{6-i} = id$, és ha az egyenlőség mindkét oldalát beszorozzuk ρ^{6-i} inverzével, akkor éppen a (3.3) egyenlőséget kapjuk, hiszen ρ^{6-i} inverze éppen

$(\rho^{6-i})^{-1} = \rho^{-1\cdot(6-i)} = \rho^{i-6}$.

Általában pedig, ha $\rho \in S_n$ rendje[11] $o(\rho) = r$, akkor

$$\rho^{r\cdot k+i} = \rho^i \qquad (\forall k, i \in \mathbb{Z})$$

és

$$\rho^i = \rho^{i-r} \quad (\forall i \in \mathbb{Z}) \quad .$$

Ne feledjük, hogy Lagrange tétele[12] alapján $o(\rho) \mid n!$.

3.4.9)

$$\tau^{25} = (1,2)^{25} \circ (3,5,4)^{25} = (1,2)^{12\cdot 2+1} \circ (3,5,4)^{8\cdot 3+1} = (1,2)^1 \circ (3,5,4)^1 = \tau,$$

---

[11] **Def.:** *Tetszőleges* $(G,\cdot)$ *csoport* $g \in G$ *elemének* **rendje** $o(g) :=$ *a legkisebb olyan* $r \in \mathbb{N}$ *amelyre* $g^r = 1$, ha *létezik ilyen kitevő.* Ha *ilyen* r *kitevő nincs, akkor* $o(g) := \infty$. □

[12] **Lagrange Tétele:** *Ha* G *véges csoport, akkor tetszőleges* $g \in G$ *elemének rendje osztója a csoport rendjének, azaz* $o(g) \mid |G|$. □

$\tau^{26} = (1,2)^{26} \circ (3,5,4)^{26} = (1,2)^{13\cdot 2} \circ (3,5,4)^{9\cdot 3-1} = id \circ (3,5,4)^{-1} = (4,5,3).$

3.4.10) Először bontsuk fel σ -t diszjunkt ciklusok szorzatára:

$\sigma = (1,2,5,10,4,3) \circ (6,11,16,19) \circ (7) \circ (8,12,9,14,18,20,15) \circ (13,17).$

Ekkor már könnyebben ki tudjuk számolni a kisebb hatványokat (hasonlóan ahhoz, amikor a gyerekek körben állnak, és a 2. vagy 5. , ... labdamenet utáni állapotot kérdezzük):

a)

$\sigma^2 = (1,2,5,10,4,3)^2 \circ (6,11,16,19)^2 \circ (8,12,9,14,18,20,15)^2 \circ (13,17)^2$
$= (1,5,4) \circ (2,10,3) \circ (6,16) \circ (11,19) \circ (8,9,18,15,12,14,20) \circ id$,

$\sigma^5 = (1,2,5,10,4,3)^5 \circ (6,11,16,19)^5 \circ (8,12,9,14,18,20,15)^5 \circ (13,17)^5$
$= (1,2,5,10,4,3)^5 \circ (6,11,16,19)^{4+1} \circ (8,12,9,14,18,20,15)^5 \circ (13,17)^{2\cdot 2+1}$
$= (1,3,4,10,5,2) \circ (6,11,16,19) \circ (8,20,14,12,15,18,9) \circ (13,17)$,

Ha tudjuk, hogy $(1,2,5,10,4,3)^{-1} = (3,4,10,5,2,1)$, akkor az $(1,2,5,10,4,3)^5$ tényezőt gyorsabban is kiszámolhatjuk:

$(1,2,5,10,4,3)^5 = (1,2,5,10,4,3)^{6-1} = (1,2,5,10,4,3)^{-1} = (1,3,4,10,5,2),$

$\sigma^{18} = (1,2,5,10,4,3)^{18} \circ (6,11,16,19)^{18} \circ (8,12,9,14,18,20,15)^{18} \circ (13,17)^{18} =$
$= (1,2,5,10,4,3)^{3\cdot 6} \circ (6,11,16,19)^{4\cdot 4+2} \circ (8,12,9,14,18,20,15)^{2\cdot 7+4} \circ$
$\circ (13,17)^{9\cdot 2} =$
$= id \circ (6,11,16,19)^2 \circ (8,12,9,14,18,20,15)^4 \circ id =$
$= (6,16) \circ (11,19) \circ (8,18,12,20,9,15,14)$,

hasonlóan

$\sigma^{83} = (1,2,5,10,4,3)^{14\cdot 6-1} \circ (6,11,16,19)^{21\cdot 4-1} \circ (8,12,9,14,18,20,15)^{12\cdot 7-1} \circ$
$\circ (13,17)^{41\cdot 2+1} =$
$= (1,2,5,10,4,3)^{-1} \circ (6,11,16,19)^{-1} \circ (8,12,9,14,18,20,15)^{-1} \circ (13,17)$
$= (3,4,10,5,2,1) \circ (19,16,11,6) \circ (15,20,18,14,9,12,8) \circ (13,17)$.

A számolásoknál felhasználtuk, hogy egy k elemű *ciklus* rendje k :
$\sigma^k = id$ ha $\sigma \in S_n$ egy k -elemű ciklus.
Nagyobb hatványkitevők esetén érdemes előbb σ rendjét kiszámolni[13)]:

[13)] **Állítás:** Könnyen belátható, hogy tetszőleges $\sigma \in S_n$ permutáció rendje

b)

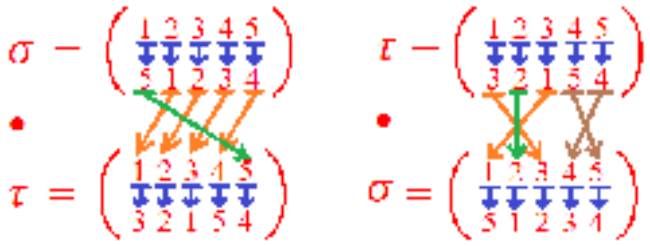
$$o(\sigma) = lkkt(6,4,2,7) = 3 \cdot 2^2 \cdot 7 = 84$$

mert σ felbontásában csak $6,4,2,7$ -elemű (diszjunkt) ciklusok szerepelnek.

a) folytatása: Ennek alapján

$\sigma^{547} = \sigma^{6\cdot 84+43} = \sigma^{43} =$
$= (1,2,5,10,4,3)^{43} \circ (6,11,16,19)^{43} \circ (8,12,9,14,18,20,15)^{43} \circ (13,17)^{43}$
$= (1,2,5,10,4,3)^{7\cdot 6+1} \circ (6,11,16,19)^{11\cdot 4-1} \circ (8,12,9,14,18,20,15)^{6\cdot 7+1} \circ (13,17)^{2\cdot 21+1}$
$= \ldots$ (HF.)

3.4.12) a) Például $\sigma(1) = 5$ és így $(\tau \circ \sigma)(1) = \tau(\sigma(1)) = \tau(5) = 4$. Ugyanez algebrai jelöléssel: $1\sigma = 5$ és $1\sigma\tau = 1(\sigma\tau) = (1\sigma)\tau = 5\tau = 4$. Tehát a $\tau \circ \sigma$ (azaz $\sigma \bullet \tau$) összetett permutáció, az elemek mozgatását részletesen megjelölve (kövessük a nyilakat):



$\sigma \cdot \tau$ és $\tau \cdot \sigma$

vagyis $\tau \circ \sigma = \sigma \bullet \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$.

Hasonlóan: $\tau(1) = 3$ és $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(3) = 2$,
és $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$.

c) Vigyázat: A ciklusok most nem diszjunktak! Nyilván

$\sigma^{-1} = (1,3)^{-1} \circ (2,5,4)^{-1} \circ (1,5,3,2)^{-1} = (3,1) \circ (4,5,2) \circ (2,3,5,1)$
és
$\tau^{-1} = (3,1,4)^{-1} \circ (1,3,2)^{-1} \circ (4,3,1)^{-1} = (4,1,3) \circ (2,3,1) \circ (1,3,4)$.

$o(\sigma) = lkkt(k_1,\ldots,k_t)$ ahol $k_1,\ldots,k_t$ jelölik σ diszjunkt ciklusokra való felbontásában a ciklusok hosszait. □

Vigyázat: a tényezők sorrendje lényeges, mert nem diszjunktak[14)]!

Ugyanez algebrai jelöléssel:

$$\sigma = (1,3)\,(2,5,4)\,(1,5,3,2)\ ,$$

$$\sigma^{-1} = (1,5,3,2)^{-1}\,(2,5,4)^{-1}\,(1,3)^{-1} = (2,3,5,1)\,(4,5,2)\,(3,1)\ ,$$

és

$$\tau = (3,1,4)\,(1,3,2)\,(4,3,1)\ ,$$

$$\tau^{-1} = (4,3,1)^{-1}\,(1,3,2)^{-1}\,(3,1,4)^{-1} = (1,3,4)\,(2,3,1)\,(4,1,3)\ .$$

(A fenti eredményeket a c) feladat megoldásának végén fogjuk ellenőrizni.)

Mivel a felírt ciklusok *nem diszjunktak*, $\tau\circ\sigma$ és $\sigma\circ\tau$ kiszámításához[15)] érdemes először visszaírnunk a permutációkat kétsoros alakba (most csak a mozgatott elemeket írjuk ki, a fixpontokat nem):

$$\sigma = (1,5,3,2)\circ(2,5,4)\circ(1,3) = (1,3)\,(2,5,4)\,(1,5,3,2) =$$

$$= \begin{pmatrix}1&3\\3&1\end{pmatrix}\begin{pmatrix}2&5&4\\5&4&2\end{pmatrix}\begin{pmatrix}1&5&3&2\\5&3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\2&3&5&1&4\end{pmatrix}$$

és

$$\tau = (4,3,1)\circ(1,3,2)\circ(3,1,4) = (3,1,4)\,(1,3,2)\,(4,3,1) =$$

$$= \begin{pmatrix}3&1&4\\1&4&3\end{pmatrix}\begin{pmatrix}1&3&2\\3&2&1\end{pmatrix}\begin{pmatrix}4&3&1\\3&1&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\ ,$$

tehát

$$\tau\circ\sigma = \sigma\tau = \begin{pmatrix}1&2&3&4&5\\2&3&5&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\4&1&5&3&2\end{pmatrix}$$

és

$$\sigma\circ\tau = \tau\sigma = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&3&5&1&4\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&1&2&3&4\end{pmatrix}\ .$$

σ és τ inverzeit a kétsoros alakjaikból könnyen ellenőrizhetjük:

$$\sigma^{-1} = \begin{pmatrix}1&2&3&4&5\\2&3&5&1&4\end{pmatrix}^{-1} = \begin{pmatrix}2&3&5&1&4\\1&2&3&4&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\4&1&2&5&3\end{pmatrix}\ ,$$

$$\tau^{-1} = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}^{-1} = \begin{pmatrix}3&4&1&2\\1&2&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\ ,$$

és természetesen a c) feladat megoldásának elején kapott inverzeket is át kell írnunk kétsoros alakba (HF).

[14)] **Tétel:** Tetszőleges félcsoportban ha az a és b elemeknek van inverzük, akkor az ab elemnek (szorzatnak) is van, és $(ab)^{-1} = b^{-1}a^{-1}$. $\square$

Csak kommutatív félcsoportban írhatjuk ezt egyszerűbben: $(ab)^{-1} = a^{-1}b^{-1}$.

[15)] ne feledjük: $\tau\circ\sigma = \sigma\tau$ és $\sigma\circ\tau = \tau\sigma$.

3.4.13) o) Vegyük észre, hogy $\rho\sigma$ és $\sigma\rho$ algebrai jelölések, vagyis például $1\rho\sigma = 1\,(\rho\sigma) = (1\rho)\,\sigma = 3\sigma = 3$. Tehát

$$\rho\sigma = \begin{pmatrix}1&2&3&4&5&6&7&8&9&0\\3&2&5&4&1&6&9&8&7&0\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9&0\\1&8&3&0&5&4&7&2&9&6\end{pmatrix} = \begin{pmatrix}1&2&3&4&5&6&7&8&9&0\\3&8&5&0&1&4&9&2&7&6\end{pmatrix}$$

és

$$\sigma\rho = \begin{pmatrix}1&2&3&4&5&6&7&8&9&0\\1&8&3&0&5&4&7&2&9&6\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9&0\\3&2&5&4&1&6&9&8&7&0\end{pmatrix} = \begin{pmatrix}1&2&3&4&5&6&7&8&9&0\\3&8&5&0&1&4&9&2&7&6\end{pmatrix}$$

Láthatjuk, hogy $\rho\sigma = \sigma\rho$ (vagy a másik jelöléssel: $= \sigma \circ \rho = \rho \circ \sigma$), annak ellenére, hogy sem ρ sem σ nem ciklusok. Az egyenlőség oka, vegyük észre, hogy ρ és σ diszjunktak: mozgatott elemeik $M(\rho) = \{1,3,5,7,9\}$, $M(\sigma) = \{2,8,4,0,6\}$ és $M(\rho) \cap M(\sigma) = \emptyset$.

Egyébként $\rho = \begin{pmatrix}1&2&3&4&5&6&7&8&9&0\\3&2&5&4&1&6&9&8&7&0\end{pmatrix} = (1,3,5)\,(7,9)$

és $\sigma = \begin{pmatrix}1&2&3&4&5&6&7&8&9&0\\1&8&3&0&5&4&7&2&9&6\end{pmatrix} = (2,8)\,(4,0,6)$.

Lásd még a 3.4.12) feladatot is.

a) Legyen például $\rho = (1,2,3)\,(4,5)$ és $\sigma = (4,5)\,(7,8,9)$. Ekkor $\rho\sigma = \sigma\rho = (1,2,3)\,(7,8,9)$, hiszen $(4,5)^2 = id$ és $\rho = (4,5)\,(1,2,3)$ és $\sigma = (7,8,9)\,(4,5)$.

b) Legyen például $\alpha = (1,2,3)\,(4,5,6)$ és $\beta = (6,5,4)\,(7,8,9)$. Ekkor $\alpha\beta = \beta\alpha = (1,2,3)\,(7,8,9)$ az a) feladat indoklása miatt.

Másik példa: legyen $\gamma = (1,3)\,(2,4)\,(5,6,7)$ és $\delta = (1,4)\,(2,3)\,(8,9,10)$, ekkor $\gamma\delta = \delta\gamma = (1,2)\,(3,4)\,(5,6,7)\,(8,9,10)$.

(Érdemes lerajzolni a pályákat.)

3.4.14) a) Például $\sigma = (1,2,3)$.

b) Ha $\sigma^2 = (1,3)$ akkor $\sigma^4 = id$, vagyis σ felbontásában (a,b,c,d) vagy (x,y) alakú tényezők lehetnek. Egyik esetben sem lesz $\sigma^2 = (1,3)$, vagyis a $(1,3)$ permutációnak *nincs* négyzetgyöke.

c) τ csak 9 hosszú ciklus lehet, mert: *hatványozáskor a ciklusok hossza nem növekszik*! Tehát $\tau^9 = id$ és $\tau^{10} = \tau^{9+1} = \tau$, és így

$$\tau = \tau^{10} = (\tau^2)^5 = (1,2,3,4,5,6,7,8,9)^5 = (1,6,2,7,3,8,4,9,5) .$$

3.4.15) d) Általában: Bármely *ciklus* rendje éppen a hossza, és a hatványozás azonosságai miatt több elem *szorzatának* rendje a rendek legkisebb közös *többszöröse*:

$$o(\sigma_1\sigma_2...\sigma_k) = lkkt\,(o(\sigma_1),...,o(\sigma_k)) \quad .$$

Kiemeljük, hogy a fentiek alapján érdemes a permutációt először ciklusokra bontanunk!

Tehát:

a) $o(\sigma) = lkkt(4,2) = 4$,

b) $o(\pi) = lkkt(4,3) = 12$,

c) $o(\rho) = lkkt(3,2,5) = 30$.

3.4.16) a) Az előző feladat módszerét felhasználva olyan $1 \leq i_1, ..., i_k \leq n$ számokat kell keresnünk amelyekre $i_1 + ... + i_k = n$ és $lkkt(i_1, ..., i_k)$ maximális, minden (adott) n számra. Néhány érték például:

n	$i_1, ..., i_k$	$lkkt$
1	1	1
2	2	2
3	3	3
4	4	4
5	2, 3	6
6	1, 2, 3 *vagy* 6	6
7	3, 4	12
8	3, 5	15
9	4, 5	20
10	2, 3, 5	30

n	$i_1, ..., i_k$	$lkkt$
11	5, 6 *vagy* 1, 2, 3, 5	30
12	3, 4, 5	60
13	1, 3, 4, 5	60
14	3, 4, 7	84
15	3, 5, 7	105
16	4, 5, 7	140
17	2, 3, 5, 7	210
18	5, 6, 7	210
19	3, 4, 5, 7	420
20	1, 3, 4, 5, 7	420

b) Mivel 100 = 2-től 23- ig a prímszámok összege: 2+3+5+7+11+13+ 17+19+23 = 100 , ezért S_{100} -ban $\max(o(\sigma)) \geq lkkt(2, 3, 5, 7, 11, 13, 17, 19, 23)$ = 223 092 870 .

3.4.17) Tudjuk, hogy minden transzpozíció *pontosan* két elemet cserél fel, vagyis ha $\sigma = \tau_1 \circ ... \circ \tau_k$, és τ_i az x_i elemet y_i -re képezi le, akkor szükségszerűen y_i -t x_i -re, és semmi más. így egy lehetséges megoldás σ_1 felbontására:

$$
\begin{array}{ccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
\downarrow & & & & \downarrow & & \qquad = \tau_1 \\
5 & 2 & 3 & 4 & 1 & 6 & 7 \\
 & & & \downarrow & \downarrow & & \qquad = \tau_2 \\
5 & 2 & 3 & 1 & 4 & 6 & 7 \\
 & & & \downarrow & & \downarrow & \qquad = \tau_3 \\
5 & 2 & 3 & 6 & 4 & 1 & 7 \\
 & & & & & \downarrow & \downarrow \qquad = \tau_4 \\
5 & 2 & 3 & 6 & 4 & 7 & 1 \\
 & \downarrow & \downarrow & & & & \qquad = \tau_5 \\
5 & 3 & 2 & 6 & 4 & 7 & 1
\end{array}
$$

ahonnan

$$\sigma_1 = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4 \cdot \tau_5 = \tau_5 \circ \tau_4 \circ \tau_3 \circ \tau_2 \circ \tau_1 = (2,3) \circ (1,7) \circ (1,6) \circ (1,4) \circ (1,5)$$

(a megbolygatott elemeket mindig igyekeztünk mielőbb helyükre tenni). Ne feledjük, hogy permutációk szorzásánál a sorrend lényeges (*kivéve*, ha *diszjunkt ciklusokat* szorzunk össze) !

A **permutáció előjele** pedig a felbontásban szereplő transzpozíciók számának *paritása*: $+1$ jelöli a páros, -1 a páratlan esetet. Esetünkben $sgn(\sigma_1) = (-1)^5 = -1$.

Másik megoldás: **(i)** A permutációt diszjunkt ciklusok szorzatára bontva

$$\sigma_1 = (1,5,4,6,7) \circ (2,3) \tag{3.4}$$

azonnal kapjuk, hogy $sgn(\sigma_1) = (-1)^{4+1} = -1$ hiszen tudjuk, hogy minden k -elemű ciklus előjele

$$sgn\left((i_1, ..., i_k)\right) = (-1)^{k-1} \tag{3.5}$$

és a sgn előjelfüggvény **multiplikatív**, azaz

$$sgn(\sigma \circ \rho) = sgn(\sigma) \cdot sgn(\rho) \qquad (\forall \sigma, \rho \in S_n) \ .$$

(ii) Tetszőleges $(i_1, ..., i_k) \in S_n$ ciklusra érvényes az

$$\boxed{(i_1, ..., i_k) = (i_1, i_2) \cdot (i_1, i_3) \cdot ... \cdot (i_1, i_{k-1}) \cdot (i_1, i_k)}$$

azaz

$$\boxed{(i_1,...,i_k)=(i_1,i_k)\circ(i_1,i_{k-1})\circ...\circ(i_1,i_3)\circ(i_1,i_2)}$$

összefüggés (a sorrend lényeges!), amit alkalmazva azonnal kapjuk az (3.4) és az (3.5) eredményeket. Hasonlóan[16]:

$$\sigma_{11}=(5,2,3)=(5,2)\cdot(5,3)=(5,3)\circ(5,2)\ ,$$

$$\sigma_{12}=(1,3,7,5)=(1,3)\cdot(1,7)\cdot(1,5)=(1,5)\circ(1,7)\circ(1,3)\ ,$$

$$\sigma_{13}=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&7&4&1&9&8&6&2&5\end{pmatrix}=(1,3,4)\,(2,7,6,8)\,(5,9)=$$

$$=(1,3)\cdot(1,4)\cdot(2,7)\cdot(2,6)\cdot(2,8)\cdot(5,9)=$$

$$=(1,4)\circ(1,3)\circ(2,8)\circ(2,6)\circ(2,7)\circ(5,9)\ ,$$

$$\sigma_{14}=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11\\2&4&1&5&8&3&10&9&6&7&11\end{pmatrix}=(1,2,4,5,8,9,6,3)\,(7,10)=$$

$$=(1,2)\cdot(1,4)\cdot(1,5)\cdot(1,8)\cdot(1,9)\cdot(1,6)\cdot(1,3)\cdot(7,10)=$$

$$=(1,3)\circ(1,6)\circ(1,9)\circ(1,8)\circ(1,5)\circ(1,4)\circ(1,2)\circ(7,10)\ .$$

3.4.18) a) A táblázathoz tartozó permutáció ("alsó sora") 2, 5, 1, 7, 10, 3, 8, 4, 15, 11, 6, 9, 12, 13, 14, az **inverziók**[17] száma + az üres négyzet *sora* = 1+3+0+3+5+0+2+0+6+2+0+0+0+0+0+*3* = páratlan, vagyis az a) játék *nem* rakható ki.

b) A permutáció: 12, 1, 9, 4, 2, 5, 10, 11, 8, 3, 13, 7, 15, 14, 6, az inverziók száma + az üres négyzet *sora* = 11+0+7+2+0+1+4+4+3+0 +2+1+2+1+0+*2* = páros, vagyis a b) játék *kirakható*.

3.4.19) a) 28 lépésre van szükségünk. Egy lehetséges legrövidebb megoldás:

F F B L J L B F F B L L J F F J L B B F J L L J F F B B

[16] ne feledjük: diszjunkt permutációk szorzása kommutatív

[17] Ha egy $...,i,...,j,...$ felsorolásban az i és j számok *fordított* (inverz) sorrendben vannak (vagyis $i>j$ de i előbb következik mind j), akkor *inverzióban vannak egymással*, és ez *egy* **inverzió**. □

3.4.20) I. megoldás: A

$\sigma = \begin{pmatrix} 10 & 9 & 12 & 8 & 13 & 3 & 4 & 1 & 5 & 11 & 6 & 2 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \end{pmatrix} = (1, 8, 4, 7, 13, 5, 9, 2, 12, 3, 6, 11, 10)$

permutáció négyzetgyökét kerestük: olyan $\rho \in S_n$ permutációt, amelyre $\rho^2 = \sigma$. Mivel σ egy 13 hosszú ciklus, ezért ρ is az (Mert tudjuk: ha egy permutáció több diszjunkt ciklusból áll, akkor hatványai is ekkora vagy még kisebb ciklusokból állnak.) Ekkor pedig $\rho^{13} = id$ és $\rho^2 = \sigma$ miatt

$\rho^{14} = \rho = (\rho^2)^7 = \sigma^7 = (1, 2, 8, 12, 4, 3, 7, 6, 13, 11, 5, 10, 9)$.

II. megoldás: Mivel a második keverés után a **10, 9, Q, 8, K, 3, 4, A, 5, J, 6, 2, 7** permutációt kaptuk, ezért ennek a permutációnak a *négyzetgyökét* keressük.

Ha megvizsgáljuk az eltérést az alap és a *második keverés utáni* állapot között, láthatjuk, hogy az ász átkerült a 8-as helyére, a 8-as a 4-es helyére, a 4-es a ... , és végül a 10-es az ász helyére. így minden lap megfordul előbb vagy utóbb minden másik lap helyén is, vagyis pontosan a tizenharmadik keverés után visszakapjuk a kiindulási állapotot.

Vegyünk egy lapot a pakliból, például az Ász -t, és nézzük meg hova kerül a 14. keverés után, ami megegyezik az első keverés utáni helyével:

Keverés	0	2	4	6	8	10	12	14
Pozíció	1	8	4	7	13	5	9	2

Innen már egyszerű, mert tudjuk, hogy az első keverés után a 2-es helyére került az ász. Innen következik, hogy a 2-es a 8-as helyére került. Innen következik, hogy a 8-as dáma helyére, stb.

Tehát az állapot az első keverés után[18]:

9, A, 4, Q, J, 7, 3, 2, 10, 5, K, 8, 6.

3.4.21) Addig kövessük nyomon az eseményeket, amíg Dömötör és Elek közül valamelyiknek fel kell állnia. Megmutatjuk, hogy a 78! esetnek pontosan a felében fordul elő, hogy Eleknek (számára kedvezőtlen módon) ülőhelyet kell változtatnia. Ehhez a 78! ülési sorrendet párokba állítjuk úgy, hogy minden párban pontosan az egyik sorrend legyen Elekre nézve kedvező.

A párosítás legyen a következő: egy tetszőleges sorrend párja legyen az, amelyet belőle Dömötör és Elek helycseréjével kapunk. Ez valóban párosítás,

[18] Barta László megoldása, http://www.fefo.hu/catalog/customer/jatek/oldgame141.html

hiszen minden sorrend különbözik a párjától, és a párok tagjai kölcsönösen egymásra találnak, mivel Dömötör és Elek kétszeri helycseréje az eredeti sorrendet állítja vissza. Világos, hogy egy sorrend pontosan akkor kedvező Elek számára, ha a párja kedvezőtlen. Tehát $\mathbf{1/2}$ annak a valószínűsége, hogy Elek ülve nézheti végig a Dömötör lelepleződéshez vezető eseményeket.

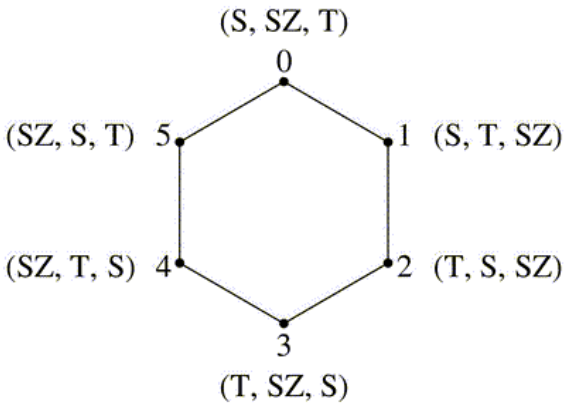
Megjegyzések: (1) A feladat szempontjából elég csak Dömötört, Eleket és a „többi utast" vizsgálni, és Dömötör és Elek helyzete szimmetrikus, felcserélhető.

(2) Könnyen megsejthető a végeredmény, ha 79 utas helyett 3-ra, majd 4-re „az ujjainkon számoljuk ki" a keresett valószínűséget. Ezután teljes indukcióval beláthatjuk, hogy a végeredmény az utasok számától függetlenül mindig $\mathbf{1/2}$.

3.4.22) I. megoldás: Ha a három jómadár[19)] sorrendje éppen "1,2,3", akkor **1** ugrása után a sorrend "2,1,3", **3** ugrása után a sorrend "1,3,2", és **2** ugrása után a sorrend vagy "2,1,3" vagy "1,3,2". Tehát a lehetséges ugrások az $\binom{1\ 2\ 3}{2\ 1\ 3} = (1,2)$ és $\binom{1\ 2\ 3}{1\ 3\ 2} = (2,3)$ permutációkat jelentik, és a feladat kérdése az, hogy 1999 db ilyen permutáció szorzata lehet-e id. Mivel ezek páratlan permutációk, ezért a válasz: *nem*, hiszen páratlan sok (bármilyen) permutáció szorzata is páratlan permutációt ad.

II. megoldás: A sáska (S), a szöcske (SZ) és a tücsök (T) összesen hatféle elrendezésben ülhetnek egymás mellett, és minden ugrásnál a középső kicserélődik. Az alábbi gráf 6 csúcsát a 6 elrendezésnek feleltettük meg, és két csúcsot akkor kötöttünk össze, ha az egyikből 1 ugrással el lehet jutni a másikhoz, és viszont.

[19)] bocs: jóbogár (pontosabban jó-rovar)



3.4.22) feladat

(A csúcsokat a 0, 1, 2, 3, 4, 5 számokkal az ábra szerint megszámoztuk.) 1999 ugrással pontosan akkor lehet eljutni a kiinduló sorrendhez, ha a gráf 0 pontjából az éleken lépegetve 1999 lépés után visszajuthatunk a 0 pontba. Minden lépésnél páros sorszámú csúcsból páratlanba vagy páratlanból párosba lépünk, így páratlan lépés után csak páratlan sorszámú pontba léphetünk, 0-ba nem. Tehát a feladat kérdésére a válasz: **nem**.

III. megoldás: Nevezzük A állapotnak az előző megoldás jelöléseit használva a következő 3 esetet: (S,SZ,T), (T,S,SZ), (SZ,T,S), B állapotnak pedig a többi 3 elrendezést: (S,T,SZ), (T,SZ,S), (SZ,S,T). Minden ugrás után az A állapotból a B-be, B-ből pedig az A-ba jutunk. így 1999 lépés után A-ból kiindulva B-be kell jutnunk, tehát nem kerülhetünk vissza sem a kiinduló, sem a másik két A-beli elrendezésbe.

Megjegyzés: Tudjuk, hogy tetszőleges $n \in \mathbb{N}$ pozitív egész számra az 1, 2, ..., n számok permutációit két csoportba, az úgynevezett *páros* és *páratlan* permutációkra lehet bontani. Egy tetszőleges $(a_1, a_2, ..., a_n)$ permutációhoz keressük meg az összes olyan $i < j$ számpárt, amelyre $a_i > a_j$. Az ilyen párok számát hívjuk a permutáció **inverziószám**ának. Ha az inverziószám páros, akkor a permutációt páros permutációnak nevezzük, ellenkező esetben pedig páratlan permutációnak.

Ha egy permutációban két tetszőleges elemet (nem feltétlenül szomszédosokat!) felcserélünk, akkor a permutáció paritása (párossága) megváltozik.

E fentiek alapján (a permutációk paritásának vizsgálatával) 3 helyett akárhány ugrándozó rovarra és 1999 helyett más számra is eldönthető a feladat.

3.4.23) Kör-telikör, vagyis *Körtelikőr* :) [20] .

[20] lásd: **Grätzer József** (1897-1945, a „rejtvénykirály", Karinthy Frigyes titkára)**:** *SICC - Szórakoztató Időtöltések, Cseles Csalafintaságok*, 1935, / Móra Kiadó, 1964, ... , https://hu.wikipedia.org/wiki/Grätzer_József
https://hu.wikipedia.org/wiki/Sicc - Szórakoztató időtöltések, cseles_csalafintaságok

4. fejezet

Gyűrűk

4.1. Alapfogalmak

4.1.1) Gyűrűk: a), b), c), d), e), nem gyűrűk: o), f), g) .

$\left(A^A, +, \circ\right)$ nem gyűrű, mert az $f \circ (g + h) = f \circ g + f \circ h$ baloldali disztributivitás nem teljesül.

$(\{i, h\}, \vee, \wedge)$ sem gyűrű, mert sem a $\vee$ sem a $\wedge$ műveletre nézve nincs inverzelem,

$(\mathcal{P}(X), \cup, \cap)$ sem gyűrű, mert sem a $\cup$ sem a $\cap$ műveletre nézve nincs inverzelem.

4.1.2) b) $(\{i, h\}, \Leftrightarrow)$ kommutatív (Abel) csoport egységeleme i hiszen
"$i \Leftrightarrow i$" $= i$ és "$h \Leftrightarrow i$" $= h$, és minden elem önmaga inverze: " $i \Leftrightarrow i$ " $= i$ és " $h \Leftrightarrow h$ " $= i$. Mivel $\vee$ kommutatív, ezért elég csak az egyik disztributivitást belátni (pl. igazságtáblával): $p \vee (q \Leftrightarrow r) = (p \vee q) \Leftrightarrow (p \vee r)$.

c) $(\mathcal{P}(X), \triangle)$ kommutatív (Abel) csoport egységeleme $\emptyset$ hiszen $A \triangle \emptyset = A$ és minden elem önmaga inverze: $A \triangle A = \emptyset$. Mivel $\cap$ kommutatív, ezért elég csak az egyik disztributivitást belátni (pl. Venn-diagramokkal): $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

d), e) Mivel $\mathbb{Z}[\sqrt{3}]$ és $\mathbb{Q}_{pn} \subset \mathbb{R}$, így a szokásos műveletek tulajdonságai biztosan teljesülnek. Csak a $+$ és $\cdot$ műveletek zártságát és egységelem létezését kell igazolnunk.

4.1.3) $(\mathbb{N}, +, \cdot)$ -ben egység 1; minden elem csak önmagával asszociált; irreducibilis = prímelemek = a szokásos prímszámok.

$(\mathbb{Z}, +, \cdot)$ -ben: egységek $+1$ és -1; asszociáltak = csak előjelben különböző egész számok (vagyis abszolút értékük megegyezik); irreducibilis = prímelemek = a szokásos pozitív *és* negatív prímszámok.

$(\mathbb{Z} \cdot 2, +, \cdot)$ (=páros számok) -ben: *semmilyen* egység nincs; tehát asszociált elemek sincsenek; irreducibilis elemek = mindazon páros számok, amelyek 4 -gyel *nem* oszthatók; prímtulajdonságú elemek = olyan páros számok, amelyek $2p$ alakúak valamilyen $p \in \mathbb{P}$ páratlan prímszámra.

$(\mathbb{R}[x], \cdot)$ -ben: egységek = konstans polinomok (=$\mathbb{R}$ elemei); asszociáltak = csak konstans-szorzótényezőben eltérő polinomok (azaz $p(x)$ és $c \cdot p(x)$ ahol $c \in \mathbb{R}$); irreducibilis = prím polinomok = a szorzattá fel nem bontható polinomok. Az Algebra Alaptétele[1)] szerint ezek pontosan az elsőfokú és a negatív diszkriminánssal rendelkező másodfokú polinomok.

c) A megoldásban felhasználhatjuk a 4.3.1. "*Euklideszi gyűrűk alapfogalmai*" fejezet 3.1.2)* feladatának, valamint a 4.3.1. "$\mathbb{Z}[\alpha]$" alfejezet eredményeit:

$N(x)$ totálisan multiplikatív, és u egység $\iff N(u) = 1$.

A fentiek alapján tehát:

$\left(\mathbb{Z}[\sqrt{2}], +, \cdot\right)$ -ben: egységek $\left(1 + \sqrt{2}\right)^n$ minden $n \in \mathbb{N}$ -re,

$(\mathbb{Z}[i], +, \cdot)$ -ben: egységek ± 1, $\pm i$,

$\left(\mathbb{Z}\left[-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right], +, \cdot\right)$ -ben: egységek ± 1, $\quad \mp\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$,

d) $\mathbb{Q}_{pn} = \left\{\frac{a}{b} \in \mathbb{Q} \mid b \textit{ páratlan}\right\}$ -ben: egységek $\frac{a}{b}$ ahol a és b *mindkettő* páratlan;

[1)] **Algebra Alaptétele** ($\mathbb{R}$ változat): *Minden* valós együtthatós *polinom* $p(x) \in \mathbb{R}[x]$ lényegében egyértelműen *(sorrendtől és asszociáltaktól eltekintve) felbontható legfeljebb másodfokú irreducibilis valós együtthatójú polinomok szorzatára.* □

Algebra Alaptétele ($\mathbb{C}$ változat): *Minden* komplex együtthatós *polinom* $p(x) \in \mathbb{C}[x]$ lényegében egyértelműen *(sorrendtől és asszociáltaktól eltekintve) felbontható elsőfokú komplex együtthatójú polinomok szorzatára.* □

$\frac{x}{y}$ és $\frac{u}{v}$ pontosan akkor asszociáltak, ha x és v 2 -nek ugyanazon hatványával oszthatók;

$\frac{a}{b}$ pontosan akkor irreducibilis ha a *nem* osztható 4 -gyel.

e) $(R[[x]], +, \cdot)$ (formális hatványsorok): egységek azon $\sum_{n=0}^{\infty} a_n x^n$ elemek, ahol $a_0 \neq 0$.

f) $(\mathbb{Z}_{p^\infty}, \oplus, \odot)$ (p -adikus egészek): egységek $\sum_{n=0}^{\infty} a_n p^n$ ahol $a_0 \neq 0$.

o) $(\mathbb{R}^{n\times n}, +, \cdot)$ -ben: egységek az invertálható mátrixok.

4.2. A $\mathbb{Z}_m$ maradékosztályok

4.2.1. Alapműveletek

4.2.1.0) a) $7 \cdot 3 = 21 = 2 \cdot 12 - 3 \equiv -3 \pmod{12}$.

b) Nem, mert pl. $6 + 4 \equiv 1 \pmod{9}$.

c) Azt kell megmutatnunk, hogy $a < b$ és $c \in Z_m$ -ből (általában) nem következik $a + c < b + c$.

4.2.1.1) a) 3 -nak nincs (multiplikatív) inverze (mod 9) mert $3 \cdot 3 \equiv 0$, azaz 3 nullosztó[2) 3)] (mod 9).

d) Nincs olyan x szám (mod 13) amelynek négyzete 7 lenne: $x^2 \equiv 7 \pmod{13}$, vagyis $\sqrt{7}$ *nem* létezik $\pmod{13}$.

4.2.1.2) a) $x \equiv (9-7)/5 \equiv 2 \cdot (5^{-1}) \equiv 2 \cdot 8 \equiv 3 \pmod{13}$.
Ellenőrzés: HF.

[2)] **Definíció:** *Az* $(S, \circ)$ *félcsoportban* $a \in S$ **nullosztó**, *ha* $a \neq u$ *ahol* $u \in S$ *az* S *félcsoport* zéruseleme, *és van olyan* $b \in S$, $b \neq u$ *elem amelyre* $a \circ b = u$. □

[3)] **Definíció:** *Az* $(S, \circ)$ *félcsoportban* $u \in S$ **zéruselem**, *ha* $u \circ a = u$ *minden* $a \in S$ *elemre.* □

b) Legelőször is kikötés: $x \not\equiv 5 \pmod{47}$.

Az egyenletet átalakítva kapjuk: $3x + 4 \equiv 35 - 7x$ azaz
$x \equiv 31/10 \equiv 31 \cdot 10^{-1} \pmod{47}$.
Következő lépésként tehát 10^{-1} -et kell meghatároznunk (mod 47) .

$y \equiv 10^{-1}$ olyan szám, amelyre $10 \cdot y \equiv 1 \pmod{47}$. **Egyik** lehetőségünk (a legegyszerűbb) tehát: végigpróbálgatjuk a $\pmod{47} = \{0, 1, ..., 46\}$ halmaz *összes* elemét: $y \equiv 33$ és így $x \equiv 31 \cdot 33 = 1023 \equiv 36 \pmod{47}$.

Másik lehetőségünk, ami kevesebb próbálgatást és számolást igényel, a következő. A feladatgyűjtemény végén levő *primitív gyök* táblázatok[4)] közül tekintsük a $\pmod{47}$ táblázatot: $g = 5$ primitív gyök. Az *indextáblázatban* látjuk, hogy $ind_5(31) = 3$ és $ind_5(10) = 19$, azaz $g^{39} \equiv 31$ és $g^{19} \equiv 10$. Tehát

$$x \equiv 33/10 \equiv g^{3-19} \equiv g^{-16} \equiv g^{46-16} \equiv g^{30} \equiv 36 \quad GF(47) \text{ -ben.}$$

Mellékesen a táblázatból azt is *kiolvashatjuk* (számolás, próbálgatás nélkül), hogy

$$10^{-1} \equiv g^{-19} \equiv g^{46-19} \equiv g^{27} \equiv 33 \pmod{47}$$

amint ezt az első megoldásban kiszámoltuk (próbálgatással).

(A primitív gyökök használatát részletesen a 4.2.1.4) feladatban mutatjuk be.)

c) Mivel $x^2 - 5x + 6 = (x - 2)(x - 3)$, ezért $x_1 \equiv 2$ és $x_2 \equiv 3$ (mod 13) . (Ne feledjük: *minden* test nullosztómentes.)

d) Szorzattá nem tudjuk bontani az $x^2 + 3x + 9$ kifejezést (diszkrimináns<0), gyököt sem tudunk vonni (a diszkrimináns indexe páratlan), tehát más módszer nem maradt: próbálgassuk végig a *véges* $GF(17) = \{0, 1, ..., 16\}$ struktúra összes elemét.

Az egyenletnek *nincs* gyöke.

e) Próbálgassuk végig $GF(17)$ elemei: az egyenlet gyöke.$x = 7$.

f) Az $5x + 3y - 13z = 9$ *lineáris Diophantikus* egyenletet kell megoldanunk (a módszert ld. a 4.3.4 fejezetben),

vagy: próbálgassuk végig $GF(13)$ elemeit ($13 \cdot 13$ eset),

[4)] hasonló a logaritmus táblázathoz

VAGY (**a legjobb megoldás**): az egyenletet oldjuk meg y -ra:

$$\begin{aligned} y &\equiv (9-5x)/3 \equiv (9-5x)\cdot 9 \equiv 81-45x \equiv \\ &\equiv 3+7x \equiv 7x+3 \pmod{13} \end{aligned}$$

(hiszen $3^{-1} \equiv 9 \pmod{13}$).

Mivel $x \in GF(13)$ tetszőleges lehet, így az egyenlet gyökei: $(0,3)$, $(1,10)$, $(2,4)$, $(3,11)$, $(4,5)$, $(5,12)$, $(6,6)$, $(7,0)$, $(8,7)$, $(9,1)$, $(10,8)$, $(11,2)$, $(12,9)$.

4.2.1.3) Számoljuk ki a függvény helyettesítési értékeit az $x = 0, 1, ..., 10$ helyeken.

4.2.1.4) a) Számítsuk ki rendre 3 hatványait $(\mathrm{mod}\, 17)$:

$3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 10$, $3^4 \equiv 13$, $3^5 \equiv 5$, $3^6 \equiv 15\ (\equiv -2)$, $3^7 \equiv 11\ (\equiv -6)$, $3^8 \equiv 16\ (\equiv -1)$, $3^9 \equiv 14\ (\equiv -3)$, $3^{10} \equiv 8\ (\equiv -9)$, $3^{11} \equiv 7\ (\equiv -10)$, $3^{12} \equiv 4\ (\equiv -13)$, $3^{13} \equiv 12\ (\equiv -5)$, $3^{14} \equiv 2\ (\equiv -15)$, $3^{15} \equiv 6\ (\equiv -11)$, $3^{16} \equiv 1\ (\equiv -16) \pmod{17}$.

Mivel a fenti listában $(\mathrm{mod}\, 17) \setminus \{0\}$ (azaz $\mathbb{Z}_{17}^* = \{1, ..., 16\}$) *összes* eleme szerepel a felsorolásban, ezért $g = 3$ valóban primitív gyök $(\mathrm{mod}\, 17)$.

b) A "kis" Fermat-tétel[5)6)] felhasználásával:

$$3^{40} \equiv 3^{2\cdot 16+8} \equiv 3^8 \pmod{17} ,$$

majd a hatványtáblázatból (ld.függelék) egyszerűen kiolvasva:

$3^8 \equiv 16 \pmod{17}$.

A $(\mathrm{mod}\, 43)$ hatványtáblázatból $3^{40} \equiv 24 \pmod{43}$.

[5)] **Fermat ("kis") tétele:** *Ha $p \in \mathbb{P}$ prímszám és $a \in \mathbb{Z}$ nem osztható p -vel, akkor* $a^{p-1} \equiv 1 \pmod{p}$. □

Fermat fenti tételének általánosítása Euler következő tétele:

Euler (számelméleti) tétele: *Ha $a, m \in \mathbb{Z}$* relatív prímek, *akkor* $a^{\varphi(m)} \equiv 1 \pmod{m}$ *ahol* $\varphi(m) :=$ *az m -nél kisebb, m -hez relatív prím pozitív számok száma* (**Euler-féle φ függvény**). □

Euler fenti tétele pedig speciális esete Lagrange (csoportelméleti) tételének.

[6)] **Pierre Fermat** (1601-1665) francia jogász és matematikus. Több, mint 400 évig megoldatlan sejtését: "*Az $x^n + y^n = z^n$ egyenletnek $n \geq 2$ esetén* csak *triviális gyökei vannak.*" (=**Nagy Fermat Sejtés =Fermat's Last Theorem =FLT**) csak 1995-ben sikerült bebizonyítani.

c) A táblázat szerint $ind_{43}^{(3)}(28) = 5$ mert $3^5 = 243 \equiv 28 \pmod{43}$.

Ennek alapján $28^8 \equiv 3^{5\cdot 8} \equiv 3^{40} \equiv 24 \pmod{43}$.

d) A táblázat szerint $g = 3$ primitív gyök $\pmod{43}$, valamint $ind_{43}^{(3)}(11) = 30$, így

$11^{40} \equiv (3^{30})^{40} \equiv 3^{1200} \equiv 3^{24} \equiv 16 \pmod{43}$

mivel a kitevőt $\pmod{42}$ kell számolni: $1200 \equiv 24 \pmod{42}$.

Ha $\pmod{47}$ kell számolnunk, akkor a $g = 5$ primitív gyököt használhatjuk, vagyis az előzőekhez hasonlóan:

$11^{40} \equiv (5^7)^{40} \equiv 5^{280} \equiv 5^{45} \equiv 19 \pmod{47}$.

e) Az Indextáblázatban (és az a) részben is) láttuk, hogy $ind_{17}^{(3)}(7) = 11$ hiszen $3^{11} \equiv 7 \pmod{17}$.

így $7^{-1} \equiv 3^{16-11} \equiv 5$ és $6/7 \equiv 6 \cdot 5 \equiv 13 \pmod{17}$.

Ellenőrzés: $13 \cdot 7 \equiv 6 \pmod{17}$.

Hasonlóan $ind_{17}^{(3)}(-1) = ind_{17}^{(3)}(16) = 8$ mivel $3^8 \equiv 16 \equiv -1 \pmod{17}$, így $\sqrt{-1} \equiv \sqrt{16} \equiv 3^{8/2} \equiv 3^4 \equiv 13 \pmod{17}$.

Ellenőrzés: $13^2 = 169 = 170 - 1 \equiv -1 \equiv 16 \pmod{17}$

vagy $13^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$

vagy $13^2 \equiv (3^4)^2 \equiv 3^8 \equiv 16 \equiv -1 \pmod{17}$

(a Hatványtáblázatból) .

f) A táblázatok szerint $g = 5$ primitív gyök $\pmod{47}$, $g^{32} \equiv 7$, amik alapján

$7^{-1} \equiv g^{-32} \equiv g^{-32+46} \equiv g^{14} \equiv 27 \pmod{47}$.

Továbbá (a táblázat szerint) $11 \equiv g^7$, így az egyenlet gyöke

$x \equiv 11/7 = 11 \cdot 7^{-1} \equiv g^{7+14} \equiv g^{21} \equiv 15 \pmod{47}$

mivel (a táblázat szerint) $g^{21} \equiv 15 \pmod{47}$.

Ellenőrzés: $7 \cdot 15 \equiv 105 \equiv 11 \pmod{47}$.

g) Először is vegyük észre, hogy

$$a^{-n} \equiv \left(a^{-1}\right)^n \pmod{m}$$

tetszőleges $a, m, n \in \mathbb{Z}$ egész számokra. Vagyis csak a^{-1} értékét kell meghatároznunk mind a három esetben!

I) Megoldás: Az $x \equiv 13^{-1} \pmod{1271}$ összefüggés ekvivalens az

$$13x - 1271y = 1$$

lineáris Diophantikus egyenlettel (ld. a 4.3.4 fejezetet).

Hasonlóan, az $x \equiv 13^{-1} \pmod{24}$ illetve az $x \equiv 3744^{-1} \pmod{9875}$ értékeket az

$13x - 24y = 1$ ill. $3744x - 9875y = 1$

lineáris Diophantikus egyenletek megoldása szolgáltatja.
(A részletes számolásokat a II) Megoldás után közöljük.)

II) Megoldás: Vegyük észre, hogy $1271 = 31 \cdot 41$ két különböző prímszám szorzata. Tehát elegendő először kiszámolnunk 13^{-1} értékét (mod 31) *és* (mod 41) , majd alkalmazzuk a Kínai Maradéktételt (ld. a 4.3.5 fejezetet).

A 24 és a 9875 modulusok nem bonthatók fel *prímek* első hatványainak szorzatára, így a fenti módszer most nem alkalmazható.

Használhatjuk még Euler (számelméleti) tételét is.

Számolások: A $3744 \cdot x - 9875y = 1$ lineáris Diophantikus egyenlet megoldása ([ ] -ben a maradékok vannak, ld. a 4.3.4 fejezet):

$$\begin{aligned}
[\,3744] &= [-9875] \cdot 0 + [3744] \\
[-9875] &= [3744] \cdot (-2) + [-2387] \\
[\,3744] &= [-2387] \cdot (-1) + [1357] \\
[-2387] &= [1357] \cdot (-1) + [-1030] \\
[\,1357] &= [-1030] \cdot (-1) + [327] \\
[-1030] &= [327] \cdot (-3) + [-49] \\
[\,327] &= [-49] \cdot (-6) + [33] \\
[-49] &= [33] \cdot (-1) + [-16] \\
[\,33] &= [-16] \cdot (-2) + [1] \\
[-16] &= [1] \cdot (-16) + [0]
\end{aligned}$$

ahonnan $lnko[3744, -9875] = 1$.

Visszafejtve:

$lnko =$

$$= 1 \cdot [33] + 2 \cdot [-16] = 1 \cdot [33] + 2 \cdot ([-49] - [-1] \cdot [33])$$
$$= 2 \cdot [-49] + 3 \cdot [33] = 2 \cdot [-49] + 3 \cdot ([327] - [-6] \cdot [-49])$$
$$= 3 \cdot [327] + 20 \cdot [-49] = 3 \cdot [327] + 20 \cdot ([-1030] - -3 \cdot [327])$$
$$= 20 \cdot [-1030] + 63 \cdot [327] = 20 \cdot [-1030] + 63 \cdot ([1357] - -1 \cdot [-1030])$$
$$= 63 \cdot [1357] + 83 \cdot [-1030] = 63 \cdot [1357] + 83 \cdot ([-2387] - -1 \cdot [1357])$$
$$= 83 \cdot [-2387] + 146 \cdot [1357] = 83 \cdot [-2387] + 146 \cdot ([3744] - -1 \cdot [-2387])$$
$$= 146 \cdot [3744] + 229 \cdot [-2387] = 146 \cdot [3744] + 229 \cdot ([-9875] - -2 \cdot [3744])$$
$$= 229 \cdot [-9875] + 604 \cdot [3744] = 229 \cdot [-9875] + 604 \cdot ([3744] - 0 \cdot [-9875])$$
$$= 604 \cdot [3744] + 229 \cdot [-9875] \ ,$$

ahonnan

$$x_0 = 604 \cdot C/d = 604 \ , \qquad y_0 = 229 \cdot C/d = 229 \ ,$$

az általános megoldás pedig:

$$x = x_0 + k \cdot b/d = 604 + k \cdot (-9875) \ , \quad y = y_0 - k \cdot a/d = 229 - k \cdot 3744 \quad (k \in \mathbb{Z}).$$

Innen $3744^{-1} \equiv 604 \pmod{9875}$.

Ellenőrzés: $3744 \cdot 604 = 2261\,376 \equiv 1 \pmod{9875}$.

4.2.1.5) Ha induláskor azonos állásban van a két megjelölt fog (mondjuk mindkettő függőlegesen lefelé[7)]), akkor *megszámolhatjuk*, hogy hányszor fordult a hajtott (általában a nagyobbik) kerék addig, amígy legközelebb mindkét kerék ugyanígy áll, vagyis mindkettő függőlegesen lefelé áll.

Tudnunk kell természetesen a két fogaskerék fogainak számát: legyenek a és b fogúak, és jelölje x ill. y hogy hányszor fordult körbe a és b, (x -et megszámoltuk, y -et nem). A láncmeghajtás miatt

$$c := ax = by \ .$$

Sőt, mivel x és y a legkisebb ilyen természetes számok, ezért

$$c = lkkt\,(a, b) \ ,$$

tehát kerékpározás közben a *legkisebb közös többszöröst* tudjuk kísérletileg meghatározni. Továbbá, a jól ismert

$$lnko\,(a, b) \cdot lkkt\,(a, b) = a \cdot b$$

[7)] sajnos a címlapon nem egy ilyen helyzet látható

összefüggésből $lnko(a,b)$ -t is már egyszerűen meg tudjuk határozni.

Megjegyzés: Hasonló, de sokkal bonyolultabb fogaskerék rendszerekkel **Derrick Norman Lehmer** (1867-1938) és **Derrick Henry Lehmer** (1905-1991) amerikai matematikusok (apa ás fia) bonyolult számelméleti számításokat oldottak meg. Fogaskerék rendszereik nem tévesztendőek össze a múlt századi fogaskerekes, csak négy alapműveletre alkalmas számológépekkel, részletesebben lásd:

https://math.uni-pannon.hu/~szalkai/Lehmer-szita.pdf ,
https://en.wikipedia.org/wiki/Derrick_Norman_Lehmer ,
https://en.wikipedia.org/wiki/Derrick_Henry_Lehmer .

4.2.2. Általános- és középiskolás feladatok

4.2.2.0) a) Emlékeztetőül pl. a 9**-es próba:** "*Egy tetszőleges* $n \in \mathbb{Z}$ *egész szám pontosan akkor osztható* 9 *-cel, ha számjegyeit összeadva a kapott összeg osztható* 9 *-cel.*"

A próba a következők miatt helyes: ha n számjegyei $a_k, ..., a_0$, akkor $10^i \equiv 1^i \equiv 1 \pmod 9$ $(i \in \mathbb{N})$ alapján az

$$n = \sum_{i=0}^{k} 10^i \cdot a_i \equiv \sum_{i=0}^{k} a_i \pmod 9$$

összefüggés igazolja a 9 -es próbát. □

Hasonlóan igazolható a többi felsorolt számpróba is.

b) Ha $n \in \mathbb{N}$ számjegyei $a_k, ..., a_0$, akkor a

$$10^i \equiv (-1)^i \equiv \begin{cases} -1 \pmod{11} & \text{ha } i \text{ páratlan} \\ 1 \pmod{11} & \text{ha } i \text{ páros} \end{cases} \qquad (i \in \mathbb{N})$$

összefüggések alapján

$$n = \sum_{i=0}^{k} 10^i \cdot a_i \equiv \sum_{i=0}^{k} (-1)^i \cdot a_i \pmod{11}$$

igazolja a 11 -es próbát. □

Mivel $2-8+3-5+7-8+9-4+2-3+7-5+3-9+1-8+0-7+1 = -22$, ezért a szám osztható 11 -gyel.

Ellenőrzés: $2\,835\,789\,423\,753\,918\,071 \;:\; 11 = 257799038523083461$.

c) Alkalmazzunk 9 -es próbát: a tényezők 9 -es maradékainak szorzata meg kell, hogy egyezzen a végeredmény 9 -es maradékával.

673 maradéka $6+7+3 \equiv 7$, 427 maradéka $4+2+7 \equiv 4$,

287371 maradéka $2+8+7+3+7+1 \equiv 1$,

így $7 \cdot 4 \equiv 1 \pmod 9$ alapján

a $673 \cdot 427 = 287\,371$ szorzás *lehet* helyes.

Hasonlóan: 425 maradéka 2, 25168 maradéka 4,

23089752420 maradéka 6 , így $2 \cdot 4 \not\equiv 6$ alapján

a $917\,425 \cdot 25\,168 = 23\,089\,752\,420$ szorzás biztosan helytelen.

Az osztásokat célszerű szorzat alakba átírni:

$907159 \stackrel{?}{=} 382 \cdot 2374 + 291$ illetve $2830917 \stackrel{?}{=} 427 \cdot 6634 + 199$.

907159 maradéka 4, 382 maradéka 4, 2374 maradéka 7, 291 maradéka 3, így $4 \equiv 4 \cdot 7 + 3$ alapján a $907159 = 382 \cdot 2374 + 291$ egyenlőség helyes *lehet.*

Hasonlóan: 2830917 maradéka 3, 427 maradéka 4, 6634 maradéka 1, 199 maradéka 1, így $4 \cdot 1 + 1 \not\equiv 3$ alapján a második osztás biztosan rossz!

A $601\,524 \cdot 548\,120 = 329797\,334880$ szorzás ellenőrzésekor a 9-ces próba nem jelez hibát, *de* a 11-es próba igen! Ennek az oka az, hogy a végeredményben a számjegyek összeg 9-cel módosult!
(Valójában: 601524*548120 = 329707334880.)
Természetesen előfordulhatnak olyan tévedések is, amit a 11-es próba nem vesz észre, csak a 9-ces próba.

A $135498 \cdot 759054 = 102850298793$ szorzás hibáját sem a 9-ces sem a 11-es próba *nem* veszi észre!
(Valójában 135498*759054 = 102 850 298 892 .)

Megjegyzés: Ha a fenti módszer egy műveletet rossznak minősít, akkor az biztosan rossz. Ha azonban a maradékok vizsgálata nem mutat eltérést, akkor még az eredeti művelet lehet hibás: a helyes végeredménytől 9 többszörösével tér el. Ennek valószínűsége 1/9, vagyis ellenőrző módszerünk csak kb.

89% -os (!) biztonsággal ellenőrzi az eredményt. Ha azonban a 11 -es próbát *is* alkalmazzuk (a bemutatotthoz hasonlóan), akkor az *ellenőrzés* tévedésének esélye már csak 1/99 , vagyis a módszer biztonsága kb. 99% !

A módszer pedig nagyon *egyszerű*, akár fejben is elvégezhető!

4.2.2.2) Ha csak az *utolsó két jegy* érdekes, az azt jelenti, hogy az eredményt $(mod\ 100)$ kell kiszámítanunk, általában pedig az *utolsó k jegy* kiszámítása $\left(mod\ 10^k\right)$ számolást kíván.

a) Vegyük észre, hogy $n \geq 10$ esetén $n!$ osztható 100 -zal, hiszen legalább két 5-tel és két 2-vel osztható szám van az $1, ..., n$ számok között.

így

$$1! + 2! + ... + 2005! \equiv 1! + 2! + 3! + 4! + 5! + 6! + 7! + 8! + 9! \equiv$$
$$\equiv 1 + 2 + 6 + 24 + 20 + 20 + 40 + 20 + 80 = 113 \equiv \mathbf{13} \quad (mod\ 100)\ .$$

b) Tudjuk, hogy tetszőleges $m \in \mathbb{Z}$ modulus esetén $x \equiv y$ -ből következik, hogy $x^2 \equiv y^2\ \ (mod\ m)$. Továbbá $m = 100$ (páros) miatt

$$(x + 50)^2 \equiv x^2 + 2 \cdot 50 \cdot x + 50^2 \equiv x^2\ (mod\ 100) \quad ,$$

így

$$1^2 + 2^2 + ... + 2005^2 \equiv (1^2 + 2^2 + ... + 50^2) \cdot 40 + (1^2 + 2^2 + 3^2 + 4^2 + 5^2) =$$
$$= \tfrac{50 \cdot 51 \cdot (2 \cdot 50 + 1)}{6} \cdot 40 + (1 + 4 + 9 + 16 + 25) = 42925 \cdot 40 + 55 \equiv \mathbf{55} \quad (mod\ 100).$$

A számolás során felhasználtuk a jól ismert

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

összefüggést is.

c) $(\text{mod}\ 10^9)$ kell számolnunk, de felhasználhatjuk a Binomiális Tételt is:

$$1001^{1965} = (1 + 1000)^{1965} = 1^{1965} + \tbinom{1965}{1} \cdot 1000 + \tbinom{1965}{2} \cdot 1000^2 + \Omega =$$
$$= 1\,929\,631\,965\,001 + \Omega = 1\,929\,631\,965\,001\ ,$$

ahol Ω egy olyan szám, amelynek (legalább) 9 utolsó számjegye 0 .

Hasonlóan (a feladatban $\eta = 1001^{1965}$):

$$1001^{\eta} = 1^{\eta} + \binom{\eta}{1} \cdot 1000 + \binom{\eta}{2} \cdot 1000^2 + \Omega = ...$$

ahol Ω -nak (legalább) 9 utolsó számjegye 0 *és* η -nak csak az utolsó 9 számjegye érdekes.

d) Legyen $A := 5 + 5^2 + ... + 5^{150}$. Mivel $186 = 2 \cdot 3 \cdot 31$, így az eredeti feladat:

$$A \equiv 0 \pmod{2 \cdot 3 \cdot 31}$$

ekvivalens az

$$\begin{cases} A \equiv 0 \pmod 2 \\ A \equiv 0 \pmod 3 \\ A \equiv 0 \pmod{31} \end{cases}$$

kongruencia rendszerrel (hiszen a 2, 3, 31 számok relatív prímek).

$5 \equiv 1 \pmod 2$ és így $5^k \equiv 1 \pmod 2$, vagyis $A \equiv 150 \equiv 0 \pmod 2$.

$5 \equiv 2 \pmod 3$ és így $5^2 \equiv 2^2 \equiv 1$, $5^3 \equiv 2 \cdot 1 \equiv 2$, $\pmod 3$,
vagyis

$$A \equiv 2 + 1 + 2 + 1 + ... + 2 + 1 \equiv (2 + 1) \cdot 75 \equiv 0 \cdot 75 \equiv 0 \pmod 3 .$$

$5 \equiv 5$, $5^2 \equiv 25$, $5^3 \equiv 5 \cdot 25 \equiv 1 \pmod{31}$, így

$$A \equiv 5 + 25 + 1 + 5 + 25 + 1 + ... + 5 + 25 + 1 \equiv (31) \cdot 50 \equiv 0 \pmod{31} .$$

4.2.2.7) Öt különböző (!) megoldást adunk.

100 **-as próba:** 14! nyilván osztható $2 \cdot 4 \cdot 5 \cdot 10 = 400$ -zal, vagyis (többek között) 100 -zal, tehát *Peti* eredménye biztosan rossz. *Panni* eredménye még lehet jó.

9 -ces, 3 **-as próba:** 14! nyilván osztható 3-mal, tehát *Panni* eredménye biztosan rossz. *Peti* eredménye még 9 -cel is osztható, tehát *ez* a módszer *Peti* eredményét nem minősíti.

11 -es **próba:** 14! nyilván osztható 11-gyel, de egyik tanuló eredménye sem osztható vele (11 -es próba!), tehát *mindkét* eredmény rossz.

7 -es, 13 **-as próba:** 14! nyilván osztható 7 -tel és 13 -mal. Bár gyors próba nincs a 7 -tel ill. 13 -mal való oszthatóságra, de talán maradékosan gyorsabban el tudjuk osztani a két "számkígyót" (7 -tel vagy 13 -mal) mint a 14 számot összeszorozni. Egyik tanuló eredménye sem osztható sem 7 -tel sem 13 -mal, tehát *mindkét* eredmény rossz.

(Egyébként: $14! = 87\,178\,291\,200$.)

4.2.2.8) A feladat szerint $10839 \equiv 11863 \pmod{m}$ vagyis $m \mid 11863 - 10839 = 1024$ ahonnan $m = 128$, 256 vagy 512.
A lehetséges *maradék* mindhárom esetben $10839 \equiv 11863 = 87 \pmod{m}$.

4.2.2.10) Az

$$1999n \equiv 2001 \pmod{10\,000}$$

kongruenciát kell megoldanunk, ami ekvivalens az

$$1999n = 10\,000m + 2001$$

vagy másképpen az

$$1999n - 10\,000m = 2001$$

úgynevezett Diophantikus egyenlettel: $n, m \in \mathbb{N}$. Ez könnyen megoldható a (4.3.4) *"Lineáris Diophantikus egyenletek"* c. fejezetben ismertetett (Euklideszi) algoritmussal:

$$\begin{aligned} n &= -4004001 + 10000k \\ m &= -800400 + 1999k \qquad k \in \mathbb{Z} \ . \end{aligned}$$

Mivel nemnegatív gyököket keresünk, ezért

$$-4\,004\,001 + 10000k > 0$$

ahonnan

$$k > 4\,004\,001$$

vagyis a legkisebb szóba jöhető érték

$$k = 401 \quad \textit{és} \quad n = 5999 \ . \quad \square$$

Összehasonlításképpen idemásoljuk a KöMaL-ban megjelent eredeti megoldást is. Legyen n egy olyan pozitív egész, amelyre az $1999n$ szám 2001-re végződik. Ekkor különbségük

$$1999n - 2001 = ...0000$$

4 nullára végződik, és így osztható -többek között- 2000-rel. Alakítsuk át a fenti különbséget a következőképpen:

$$1999n - 2001 = 2000(n-1) - (n+1) \quad .$$

Mivel a bal oldal osztható 2000-rel, a jobb oldalnak is oszthatónak kell lennie, azaz $2000 \mid n+1$. Az n szóbajöhető értékei: 1999, 3999, 5999,.... Ezeket rendre megszorozva 1999-cel $5999 \cdot 1999 = 11992001$ az első olyan, amelyik 2001 -re végződik, tehát 5999 a legkisebb n .

4.2.2.11) $\pmod{17}$ számolunk:

$$333,333,331 = (10^9-7)/3 \equiv (10^9-7)\cdot 6 \equiv \Big((10^2)^4 \cdot 10 - 7\Big)\cdot 6 \equiv$$

$$\equiv \big((-2)^4 \cdot 10 - 7\big)\cdot 6 \equiv (160-7)\cdot 6 \equiv 0 \pmod{17} .$$

4.2.2.12)* b) Ha $s=2$, akkor $s-1=1$ és a maradék 0. Tegyük fel a továbbiakban, hogy $s>2$. Jelölje S_i az $(s+1)$ -es alapú számrendszerben felírt $iii...i_{i-szer}$ számot, ekkor

$$S_i = i \cdot 111...1_{i-szer} = i \cdot \big((s+1)^{i-1} + (s+1)^{i-2} + ... + (s+1) + 1\big) \quad .$$

Az $(s+1)$ számot $(s-1)$ -gyel osztva a maradék 2, ezért S_i és

$$i \cdot \big(2^{i-1} + 2^{i-2} + ... + 2 + 1\big) = i \cdot \big(2^i - 1\big)$$

ugyanazt a maradékot adja $(s-1)$-gyel osztva. Tehát

$$F_s = 1 + 22 + 333 + 4444 + ... + \underbrace{sss...s}$$

ugyanakkora maradékot ad $(s-1)$-gyel osztva, mint

$$\begin{aligned} G &= 1\cdot(2^1-1) + 2\cdot(2^2-1) + ... + s\cdot(2^s-1) \\ &= 1\cdot 2^1 + 2\cdot 2^2 + ... + s\cdot 2^s - \frac{s(s+1)}{2} = H - \frac{s(s+1)}{2} \end{aligned}$$

hiszen $1+2+...+s = \dfrac{s(s+1)}{2}$. Legyen

$$B := H - 2 = 1\cdot 2^1 + 2\cdot 2^2 + ... + s\cdot 2^s - 2$$

ekkor

$$2B = 1 \cdot 2^2 + 2 \cdot 2^3 + ... + s \cdot 2^{s+1} - 4 \ .$$

A fenti két egyenlet különbsége

$$\begin{aligned} B &= 2B - B = -2^1 - 2^2 - 2^s + s \cdot 2^{s+1} - 2 = \\ &= -1 - 2^1 - 2^2 - 2^s + s \cdot 2^{s+1} - 1 \\ &= -\left(2^{s+1} - 1\right) + s \cdot 2^{s+1} - 1 = (s-1) \cdot 2^{s+1} \ , \end{aligned}$$

ami nyilván osztható $(s-1)$ -gyel.

Tehát a feladatban F_s maradéka megegyezik

$$\begin{aligned} B + 2 - \frac{s(s+1)}{2} &\equiv 2 - \frac{s(s+1)}{2} = 2 - \frac{s(s-1)+2s}{2} = 2 - s - \frac{s(s-1)}{2} = \\ &= 1 - (s-1) - \frac{s(s-1)}{2} \end{aligned}$$

osztási maradékával (mod $(s-1)$). Ez pedig 1, ha s páros, és

$$\begin{aligned} 1 - \frac{s(s-1)}{2} &= \frac{2}{2} - \frac{(s+1)(s-1) - (s-1)}{2} = \frac{2 + (s-1)}{2} - \frac{(s+1)(s-1)}{2} \\ &= \frac{1+s}{2} - \frac{(s+1)(s-1)}{2} \end{aligned}$$

alapján $\frac{1+s}{2}$ ha s páratlan (mert $s+1$ páros).

4.2.2.14) Vegyük észre (ellenőrizzük), hogy minden páratlan szám négyzete pontosan 1 maradékot ad 8 -cal elosztva, vagyis $8k + a \equiv 1 \pmod 8$ minden $a = \pm 1, \pm 3$ esetén. Tehát nézőktől kapott négyzetösszeg mod 8 maradéka pontosan a gondolt számok számát adja. Mivel pedig a 8 -as maradék csak az egész szám utolsó 3 jegyétől függ, kis gyakorlás után mi is előadhatjuk a bűvésztrükköt.

4.2.3. Euler és Fermat tételei, nagy kitevőjű hatványok

4.2.3.0) A tízes számrendszerben $x \in \mathbb{N}$ pontosan akkor k jegyű, ha

$$10^{k-1} \leq x < 10^k \quad .$$

Ezek alapján $k-1 \leq \lg\left(3425^{5432}\right) = 5432 \cdot \lg\left(3425\right) \approx 19200.276$, vagyis a kérdéses mennyiség 19201 jegyű 10 -es számrendszerben felírva.

Kettes számrendszerben pedig $log_2\left(3425^{5432}\right) \approx 63781.936$ alapján a hatvány 63782 számjegyből áll.

4.2.3.1) a) Tetszőleges $p \in \mathbb{P}$ prímszámra $\varphi(p) = p - 1$, továbbá a logikai szitaformula (legegyszerűbb változata) alapján

$$\varphi(p \cdot q) = pq - p - q + 1 = (p-1) \cdot (q-1)$$

ahol $p, q \in \mathbb{P}$ tetszőleges prímszámok.

b) A $[SzI]$ Feladatgyűjtemény 4. fejezetében (Logikai szitaformula) leírtak miatt

$$\varphi(n) = \prod_{p_i | n} \left(1 - \frac{1}{p_i}\right)$$

ahol az n szám prímtényezős felbontása

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} \quad .$$

c) A fentiek (azaz a logikai szitaformula) alapján

$$\begin{aligned} \varphi(1500) &= 1500 - \frac{1500}{2} - \frac{1500}{3} - \frac{1500}{5} + \frac{1500}{2 \cdot 3} + \frac{1500}{2 \cdot 5} + \frac{1500}{3 \cdot 5} - \frac{1500}{2 \cdot 3 \cdot 5} \\ &= 400 \quad . \end{aligned}$$

4.2.3.2) a) $6456^{4652} \pmod{9786}$ kiszámítása:

$k = 4652 = 1001000101100$ (bin) ,

$$\begin{aligned}
u[0] &= u = 6456 = u^{2^0} = 6456 && (\mathrm{mod}\,9786)\\
u[1] &= (u[0])^2 = u^{2^1} = 6456^2 \equiv 1362 && (\mathrm{mod}\,9786)\\
\mathbf{u[2]} &= (u[1])^2 = u^{2^2} = 1362^2 \equiv \mathbf{5490} && (\mathrm{mod}\,9786)\\
\mathbf{u[\ 3]} &= (u[2])^2 = u^{2^3} = 5490^2 \equiv \mathbf{9006} && (\mathrm{mod}\,9786)\\
u[4] &= (u[3])^2 = u^{2^4} = 9006^2 \equiv 1668 && (\mathrm{mod}\,9786)\\
\mathbf{u[\ 5]} &= (u[4])^2 = u^{2^5} = 1668^2 \equiv \mathbf{3000} && (\mathrm{mod}\,9786)\\
u[6] &= (u[5])^2 = u^{2^6} = 3000^2 \equiv 6666 && (\mathrm{mod}\,9786)\\
u[7] &= (u[6])^2 = u^{2^7} = 6666^2 \equiv 7116 && (\mathrm{mod}\,9786)\\
u[8] &= (u[7])^2 = u^{2^8} = 7116^2 \equiv 4692 && (\mathrm{mod}\,9786)\\
\mathbf{u[\ 9]} &= (u[8])^2 = u^{2^9} = 4692^2 \equiv \mathbf{6150} && (\mathrm{mod}\,9786)\\
u[10] &= (u[9])^2 = u^{2^{10}} = 6150^2 \equiv 9396 && (\mathrm{mod}\,9786)\\
u[11] &= (u[10])^2 = u^{2^{11}} = 9396^2 \equiv 5310 && (\mathrm{mod}\,9786)\\
\mathbf{u[12]} &= (u[11])^2 = u^{2^{12}} = 5310^2 \equiv \mathbf{2634} && (\mathrm{mod}\,9786)
\end{aligned}$$

így

$$u^k \equiv 5490 \cdot 9006 \cdot 3000 \cdot 6150 \cdot 2634 \equiv 4068 \cdot 3000 \cdot 6150 \cdot 2634 \equiv$$

$$\equiv 858 \cdot 6150 \cdot 2634 \equiv 2046 \cdot 2634 \equiv 6864 \quad (\mathrm{mod}\,9786)\ ,$$

vagyis $6456^{4652} \equiv 6864 \pmod{9786}$.

b) $4326^{1818} \pmod{1003}$ kiszámítása:

$k = 11100011010$ (bin) ,

$$\begin{aligned}
u[0] &= u \equiv 314 = u^{2^0} \pmod{1003} \\
u[1] &= (\mathrm{u}[0])^2 = u^{2^1} \equiv 302 \pmod{1003} \\
u[2] &= (\mathrm{u}[1])^2 = u^{2^2} \equiv 934 \pmod{1003} \\
u[3] &= (\mathrm{u}[2])^2 = u^{2^3} \equiv 749 \pmod{1003} \\
u[4] &= (\mathrm{u}[3])^2 = u^{2^4} \equiv 324 \pmod{1003} \\
u[5] &= (\mathrm{u}[4])^2 = u^{2^5} \equiv 664 \pmod{1003} \\
u[6] &= (\mathrm{u}[5])^2 = u^{2^6} \equiv 579 \pmod{1003} \\
u[7] &= (\mathrm{u}[6])^2 = u^{2^7} \equiv 239 \pmod{1003} \\
u[8] &= (\mathrm{u}[7])^2 = u^{2^8} \equiv 953 \pmod{1003} \\
u[9] &= (\mathrm{u}[8])^2 = u^{2^9} \equiv 494 \pmod{1003} \\
u[10] &= (\mathrm{u}[9])^2 = u^{2^{10}} \equiv 307 \pmod{1003}
\end{aligned}$$

Tehát

$$4326^{1818} \equiv 314^{1818} \equiv 302 \cdot 749 \cdot 324 \cdot 953 \cdot 494 \cdot 307 \equiv 64 \pmod{1003} .$$

c) $2222^{5555} \pmod{137}$ kiszámítása:

Mivel 137 prímszám és sokkal kisebb a kitevőnél, ezért célszerű először a "kis" Fermat tételt használni, amivel a kitevőt csökkenthetjük:

$$2222^{5555} \equiv 2222^{136 \cdot 40 + 115} \equiv 2222^{115} \pmod{137}$$

ami alapján (a rövidebb) számolás:

$k = 1110011$ (bin) ,

$$\begin{aligned}
u[0] &\equiv u^{2^0} \equiv 30 \pmod{137} \\
u[1] &\equiv u^{2^1} \equiv 78 \pmod{137} \\
u[2] &\equiv u^{2^2} \equiv 56 \pmod{137} \\
u[3] &\equiv u^{2^3} \equiv 122 \pmod{137} \\
u[4] &\equiv u^{2^4} \equiv 88 \pmod{137} \\
u[5] &\equiv u^{2^5} \equiv 72 \pmod{137} \\
u[6] &\equiv u^{2^6} \equiv 115 \pmod{137}
\end{aligned}$$

$u^k \equiv 30 \cdot 78 \cdot 88 \cdot 72 \cdot 115 \equiv 11 \cdot 88 \cdot 72 \cdot 115 \equiv 9 \cdot 72 \cdot 115 \equiv 100 \cdot 115 \equiv 129$.

Vagyis $2222^{5555} \equiv 30^{115} \equiv 129 \pmod{137}$.

Megjegyzés: a kitevőt nem prím modulus esetén is csökkenthetjük, ha a hatvány alapja relatív prím a modulushoz, Euler (számelméleti) tétele alapján.

4.2.4. RSA - titkosírás

4.2.4.0) a) $440747 = 613 \cdot 719$,

b) $2347589 = 1483 \cdot 1583$,

c) $97189241 = 7151 \cdot 13591$,

d) $17967876255379 = 81371 \cdot 220814249$,

e) $444113096135661846937 = 3719977867 \cdot 119385951211$,

f) $2^{67} - 1 = 193707721 \cdot 761838257287$

4.2.4.1) a) "Wir treffen uns am Samstag" üzenet kódolva: =

12 04 17 00 15 17 25 41 41 25 09 00 21 09 24 00 01 07 00

24 01 07 24 15 01 28.

b) $24^f \equiv 24^{17} \equiv 29 =$Ü $(\mathrm{mod}\, 55)$, ... s.í.t., az üzenet: *ÜGYES.*

c) $10^f \equiv 10^7 \equiv 10 =$H $(\mathrm{mod}\, 77)$, ... s.í.t., az üzenet: *HELYES.*

4.2.4.2) a) $n = pq = 269 \cdot 241 = 64829$, $s = \varphi(n) = 268 \cdot 240 = 64320$,

b) az $ef - sy = 1$, azaz $53201 \cdot f - 64320 \cdot y = 1$ Diophantikus egyenletet kell megoldanunk: $f = 28721$,

c) $y \equiv x^e \pmod{n}$ azaz $y \equiv 48055^{53201} \equiv 61606 \pmod{64829}$,

d) $x \equiv y^f \pmod{n}$ azaz $x \equiv 61606^{28721} \equiv 48055 \pmod{64829}$,

e) $8^{53201} \equiv 13745$, $512^{53201} \equiv 57388$ és $1215^{53201} \equiv 18638 \pmod{64829}$, vagyis a "HELLO" üzenet kódolva = 0008 0512 1215,

f) $36376^{28721} \equiv 16$, $28210^{28721} \equiv 918$, $53334^{28721} \equiv 1519 \pmod{64829}$, vagyis a kódolt üzenet: 0016 0918 1519 = "PIROS"

4.2.4.3) a) $n = pq = 29539$, $s = \varphi(n) = 29160$,

b) $13201 \cdot f - 29160 \cdot y = 1$ alapján $f = 26041$,

c) $y \equiv 11418^{13201} \equiv 24836 \pmod{29539}$,

d) $x \equiv 24836^{26041} \equiv 11418 \pmod{29539}$,

e) $8^{13201} \equiv 9709$, $512^{13201} \equiv 512$ és $1215^{13201} \equiv 13473 \pmod{29539}$, vagyis a "HELLO" üzenet kódja: 970951213473 ,

f) $424^{26041} \equiv 112$, $20621^{26041} \equiv 1301$, vagyis a kódolt üzenet: 01121301 = "$ALMA$" .

4.2.4.5) a) $00000001^{209} \equiv 00000001$, $16160100^{209} \equiv 00022271 \pmod{n}$, $18211813^{209} \equiv 47610329 \pmod{n}$, tehát a kódolt üzenet = 00000001 00022271 47610329 (eml: $n = 49,891,381$).

b) "OLVASD EL" = 15 12 22 01 19 04 00 05 12 amit 8 hosszú részekre tördelve $k_1 = 1512220$, $k_2 = 11904000$ és $k_3 = 512$. Ekkor

$k_1^e = 1512220^{209} \equiv 11812012 \pmod{49,891,381}$,

$k_2^e = 11904000^{209} \equiv 4882790 \pmod{49,891,381}$,

$k_3^e = 512^{209} \equiv 42839442 \pmod{49,891,381}$,

vagyis a kódolt üzenet : 11812012 4882790 42839442 .

c) $z^e \equiv 49691150^{209} \equiv 19211115 \pmod{n}$ és 19 21 11 15 ="PRIM" értelmes üzenet.

d) $n = 49891381 = 6091 \cdot 8191 = p \cdot q$,

$s = (p-1) \cdot (q-1) = 49877100$,

$f = 4056989 = 11110111100111100111101^{(BIN}$;

így $(y_1)^f \equiv 37791786^{4056989} \equiv 22\ 30\ 17\ 14$ ="SZOL" $\pmod{n}$,

$(y_2)^f \equiv 01150082^{4056989} \equiv 11\ 05\ 01\ 21$ ="IDAR" $\pmod{n}$,

$(y_3)^f \equiv 32137718^{4056989} \equiv 11\ 23\ 02\ 22$ ="ITÁS" $\pmod{n}$, azaz a feltört üzenet: "SZOLIDARITÁS" .

4.2.4.6) Ha

n = 444 113 096 135 661 846 937 = 3 719 977 867 * 119 385 951 211

és $f = 2039$,

akkor e= 217 809 267 294 044 099 és $x = 32$ kódja

$y \equiv x^e \equiv 316\ 326\ 629\ 379\ 980\ 725\ 998 \pmod{n}$.

4.2.4.7) Ha $n \in \mathbb{N}$, akkor az egy részként kódolható betűsorozatok hossza k -jegyű szám, azaz k/2 betűt tartalmazhat ha az n szám k-jegyű, feltéve hogy n legalább 35-tel kezdődik. Vagyis n<3535 esetén csak betűnként tudunk kódolni, ami könnyen feltörhető. Ne feledkezzünk még meg a kódolás utáni (dekódolás előtti) szóközökről sem!

4.2.4.8)* A történet az [M] cikk szerint a következő: Rivest, Shamir és Adleman a *Scientific American* 1977. augusztusi számában tűzte ki ezt a feladatot (az első megfejtőnek 100$ jutalmat ajánlottak fel. 1994 áprilisában gazdája akadt a 100$-nak.)

n -et a következőképpen sikerült faktorizálni:

n = 3490 5295108476 5094914784 9619903898 1334177646 3849338784˜
˜3990820577 *
∗ 32769 1329932667 0954996198 8190834461 4131776429 6799294253˜
˜9798288533.

A "titkos" kitevő:

f = 106 69861436857 8024442868 7713289201 54780709906 63393786280 1226224496 63106312591 17744708733 4016859746 23065539685 4451327710 9053606095 .

A hatványozás után az eredeti, rejtjelezett üzenet:

P = 20 08 05 00 13 01 07 09 03 00 23 15 18 04 19 00 01 18 05 00 19 17 21 05 01 13 09 19 08 00 15 19 19 09 06 18 01 07 05
= " THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE"
= " A VARÁZSSZÓ A KÉNYESGYOMRÚ HALÁSZSAS" .

A faktorizáció (1994-ben!) azáltal vált lehetségessé, hogy írtak egy programot, amely a számításokat képes volt sok számítógépre szétosztani s a részeredményeket a központba elküldeni, s több mint 600-an, amikor éppen nem volt szükség számítógépükre, ezt a programot futtatták. A munka így 8 hónapig tartott. A befutott részeredmények egy 569466 x 524338 mátrixot

alkottak, amelyet Gauss-féle eliminációval 188614 x 188160-ra csökkentettek. Ennek alapján a faktorizáció 16K MasPar P-1-es gépen 45 óráig tartott. Ez az első eset, hogy sikerült RSA kódban írt szöveget feltörni; mint láthatjuk, elég szép munka volt.

4.3. Euklideszi gyűrűk

4.3.1. Alapfogalmak

4.3.1.1) a) $(\mathbb{N},+,\cdot)$ és $(\mathbb{Z},+,\cdot)$ mindegyike Euklideszi gyűrű: $\varphi(n)=|n|$ a szokásos abszolútérték, és a maradékos osztás is a szokásos.

$(\mathbb{Z}\cdot 2,+,\cdot)$ nem Euklideszi gyűrű: pl. 20 sem osztható el 6 -tal maradékosan a *páros* számok körében úgy, hogy a maradék kisebb legyen mint az osztó (most éppen 6).

Más indoklás: tanultuk, hogy minden Euklideszi gyűrűben teljesül az egyértelmű prímfelbontási tulajdonság, márpedig a páros számok gyűrűjében pl. 60 többféleképpen is felbontható *irreducibilis* (tovább már nem bontható) elemek szorzatára: $60=2\cdot 30=10\cdot 6=\ldots$.

b) Egy $R[x]$ polinomgyűrű *pontosan akkor* Euklideszi, ha R test. Vagyis $(\mathbb{Z}_p[x],+,\cdot)$, $(\mathbb{Q}[x],+,\cdot)$, $(\mathbb{R}[x],+,\cdot)$, $(\mathbb{C}[x],+,\cdot)$, $(\mathcal{Q}[x],+,\cdot)$, $(\Gamma[x],+,\cdot)$ mindegyike Euklideszi gyűrű. Ekkor $\varphi(p)=$ **a** p **polinom fokszáma+1** ha $p\neq 0$. (A "+1" növelésre azért van szükség, mert $\varphi(c)>0$ kell minden $c\neq 0$ konstans [azaz 0 -fokú] polinomra.)

$(\mathbb{N}[x],+,\cdot)$, $(\mathbb{Z}[x],+,\cdot)$, $(\mathbb{Z}_m[x],+,\cdot)$ nem Euklidesziek: például az $5x^2+4x-2$ polinom sem osztható a $3x-2$ polinommal úgy, hogy a maradék elsőfokú legyen.

c) $(\mathbb{Z}[\alpha],+,\cdot)$ Euklideszi gyűrű, ha $\alpha=i$, $\sqrt{2}$, $\sqrt[3]{1}=\frac{-1}{2}+\frac{\sqrt{3}}{2}i$, nem Euklideszi gyűrű, ha $\alpha=\sqrt{3}i$, $\sqrt{5}i$, $\sqrt{6}i$, $\sqrt{19}i$, $\sqrt{43}i$, $\sqrt{67}i$, $\sqrt{163}i$ vagy $1+\frac{\sqrt{19}i}{2}$.

A $\mathbf{Z}[\alpha]$ struktúrák

Most külön alfejezetben *általánosan* is megvizsgáljuk a **norma** és a **maradékos osztás** problémáját **a**

$$\mathbb{Z}[\alpha] = \{a + b \cdot \alpha : a, b \in \mathbb{Z}\}$$

gyűrűkben α *másodfokú algebrai egész* esetén, azaz ha α gyöke egy

$$\alpha^2 + p\alpha + q = 0 \tag{4.1}$$

egyenletnek.

Mivel szeretnénk, hogy a maradékos osztás elvégezhető legyen $\mathbb{Z}[\alpha]$ halmazunkban, ezért tegyük fel még, hogy $p, q \in \mathbb{Z}$ olyan egész számok, amelyekre

$$1 + |p| + |q| < 4 \quad . \tag{4.2}$$

($N(u)$ legfontosabb tulajdonságait megtaláljuk a 3.1.2) feladatban)

Speciális esetek:

ha $p = 0$, $q = 0$ akkor $\alpha = 0$, $\mathbb{Z}[\alpha] = \mathbb{Z}$=egész számok, $N(a) = a^2$,

ha $p = 0$, $q = 1$ akkor $\alpha = i$, $\mathbb{Z}[i]$="Gauss-egészek", $N(a + bi) = a^2 + b^2$,

ha $p = 1$, $q = 1$ akkor $\alpha = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\mathbb{Z}[\alpha]$="Euler-egészek",

$N(a + b\alpha) = a^2 + b^2 - ab$,

ha $p = 0$, $q = -2$ akkor $\alpha = \sqrt{2}$, $\mathbb{Z}[\alpha]$="H-egészek", $N(a + b\alpha) = a^2 - 2 * b^2$.

Jelölje D a (4.1) egyenlet diszkriminánsát, azaz

$$D := \left(\frac{p}{2}\right)^2 - q \ , \quad \textit{és így} \quad \alpha = \left(\frac{p}{2}\right) + \sqrt{D} \quad . \tag{4.3}$$

Mivel $\mathbb{Z}[\alpha] \subset \mathbb{C}$, ezért a $\mathbb{Z}[\alpha]$ halmaz elemei között az alapműveleteket a szokásos módon végezzük[8]. Továbbá, $\mathbb{Z}[\alpha]$ részhalmaza a

$$\mathbb{Q}[\alpha] := \{a + b \cdot \alpha : a, b \in \mathbb{Q}\}$$

[8] Meg kell még gondolnunk azt is, hogy $\mathbb{Z}[\alpha]$ *zárt* a műveletekre (ld.a 1.3. "*Függvények, műveletek*" c. fejezet 3.5. feladatát). Ez csak a szorzás esetében nem nyilvánvaló:
ha $a\alpha + b$ és $c\alpha + d \in \mathbb{Z}[\alpha]$, *akkor*
$(a\alpha + b)\cdot(c\alpha + d) = ac\alpha^2 + (ad+bc)\alpha + bd = ac(-p\cdot\alpha - q) + (ad+bc)\alpha + bd = u\alpha + v \in \mathbb{Z}[\alpha]$.
Itt használtuk fel, hogy α kielégíti a (4.1) összefüggést.

és a

$$\mathbb{Q}[\sqrt{D}] := \{a + b \cdot \sqrt{D} : a, b \in \mathbb{Q}\}$$

halmazoknak is, ezért az osztást is el tudjuk végezni $\mathbb{Q}[\sqrt{D}]$ és $\mathbb{Q}[\alpha]$ -ban:

Ha $a + b \cdot \alpha,\, c + d \cdot \alpha \in \mathbb{Z}[\alpha]$, *akkor*

$$\begin{aligned} a + b \cdot \alpha &= a + b \cdot \left(\frac{p}{2} + \sqrt{D}\right) = x + y \cdot \sqrt{D} \\ c + d \cdot \alpha &= c + d \cdot \left(\frac{p}{2} + \sqrt{D}\right) = u + v \cdot \sqrt{D} \end{aligned}$$

és

$$\begin{aligned} \frac{a + b \cdot \alpha}{c + d \cdot \alpha} &= \frac{x + y \cdot \sqrt{D}}{u + v \cdot \sqrt{D}} = \frac{\left(x + y \cdot \sqrt{D}\right) \cdot \left(u - v \cdot \sqrt{D}\right)}{\left(u + v \cdot \sqrt{D}\right) \cdot \left(u - v \cdot \sqrt{D}\right)} \\ &= \frac{(xu - yvD) + (yu - xv) \cdot \sqrt{D}}{u^2 - v^2 \cdot D} \quad , \end{aligned}$$

majd bevezetjük a

$$w := u^2 - v^2 \cdot D$$

jelölést, és felhasználjuk az (4.3) összefüggést, akkor kapjuk, hogy

$$\begin{aligned} &= \frac{(xu - yvD) + (yu - xv) \cdot (\alpha - \frac{p}{2})}{w} \\ &= \frac{xu - yvD - (yu - xv) \cdot \frac{p}{2}}{w} + \frac{yu - xv}{w} \cdot \alpha \\ &= \frac{m}{w} + \frac{n}{w} \cdot \alpha \quad \in \quad \mathbb{Q}[\alpha] \end{aligned} \tag{4.4}$$

ahol $m, n, w \in \mathbb{Z}$.

Jelölje továbbá

$$N(a + b\alpha) := |a^2 + qb^2 - pab|$$

az $a + b\alpha \in \mathbb{Z}[\alpha]$ szám **normáját**[9)].

[9)] Könnyen belátható, hogy N mindig multiplikatív függvény $\mathbb{Z}[\alpha]$ -n, azaz $N(\kappa \cdot \lambda) = N(\kappa) \cdot N(\lambda)$ tetszőleges $\kappa, \lambda \in \mathbb{Z}[\alpha]$ számokra. (Lásd még a 3.1.2) feladatot is.)

Célunk a *maradékos osztás* elvégzése a $\mathbb{Z}[\alpha]$ gyűrűben, azaz:
adott $a+b\alpha,\ c+d\alpha \in \mathbb{Z}[\alpha]$, $c+d\alpha \neq 0$ számok esetén keresendők olyan $e+f\alpha,\ g+h\alpha \in \mathbb{Z}[\alpha]$ számok, amelyekre

$$\begin{aligned} a+b\alpha &= (c+d\alpha)\cdot(e+f\alpha)+(g+h\alpha) \\ \textit{és} \quad N(g+h\alpha) &< N(c+d\alpha) \quad . \end{aligned} \tag{4.5}$$

Ennek **receptje**: végezzük el az

$$\frac{a+b\cdot\alpha}{c+d\cdot\alpha} = \frac{m}{w}+\frac{n}{w}\cdot\alpha$$

osztást a (4.4) képlet szerint, és kerekítsük az $\frac{m}{w}, \frac{n}{w}$ racionális számokat a *legközelebbi* (akár nagyobb akár kisebb) $e, f \in \mathbb{Z}$ egész számokra. (Vagyis a *hányadost* már megtaláltuk.)

A (4.2) feltétel miatt a

$$\begin{aligned} (g+h\alpha) &:= (a+b\alpha)-(c+d\alpha)\cdot(e+f\alpha) \\ &= (a-ce+dfq)+(b-cf-ed+dfp)\cdot\alpha \end{aligned}$$

számra teljesülni fog a (4.5) feltétel. A fenti képlet pedig a maradékot szolgáltatja. □ ■

4.3.2. Prímfelbontás

4.3.2.1) $60 = 6\cdot 10 = 2\cdot 30$ - ez két különböző felbontás irreducibilis elemekre.

4.3.3. Euklidesz algoritmusa

4.3.3.1) a) $lnko(7732, 149)$ meghatározása (a maradékokat () -ben

írtuk fel):

$$\begin{aligned}(7732) &= (149)\cdot 51 + (133)\\ (149) &= (133)\cdot 1 + (16)\\ (133) &= (16)\cdot 8 + (5)\\ (16) &= (5)\cdot 3 + (1)\\ (5) &= (1)\cdot 5 + (0)\end{aligned}$$

így $lnko(7732, 149) = 1$.

b) $lnko(94542, 24981)$ meghatározása:

$$\begin{aligned}(94542) &= (24981)\cdot 3 + (19599)\\ (24981) &= (19599)\cdot 1 + (5382)\\ (19599) &= (5382)\cdot 3 + (3453)\\ (5382) &= (3453)\cdot 1 + (1929)\\ (3453) &= (1929)\cdot 1 + (1524)\\ (1929) &= (1524)\cdot 1 + (405)\\ (1524) &= (405)\cdot 3 + (309)\\ (405) &= (309)\cdot 1 + (96)\\ (309) &= (96)\cdot 3 + (21)\\ (96) &= (21)\cdot 4 + (12)\\ (21) &= (12)\cdot 1 + (9)\\ (12) &= (9)\cdot 1 + (3)\\ (9) &= (3)\cdot 3 + (0)\end{aligned}$$

így $lnko(94542, 24981) = 3$.

4.3.3.2) A

$$lkkt(a, b) = \frac{a \cdot b}{lnko(a, b)}$$

összefüggés alapján $lkkt(56354, 2956) = \dfrac{56354 \cdot 2956}{2} = 83291212$.

4.3.3.3) Használjuk a

$$lnko(a, b, c) = (lnko(a, b), c)$$

összefüggést.

Mivel $lnko(65924, 33284) = 4$,

így $lnko(65924, 33284, 53142) = lnko(4, 53142) = 2$.

4.3.3.4) Használjuk az

$$lkkt(a, b) = \frac{a \cdot b}{lnko(a, b)}$$

és az

$$\begin{aligned} lnko(a, b, c) &= lnko(\ lnko(a, b)\ ,\ c) \\ lnko(a, b, c, d) &= lnko\,(\ lnko(lnko(a, b), c)\ ,\ d\ ) \\ lkkt(a, b, c) &= lkkt(\ lkkt(a, b)\ ,\ c) \\ lkkt(a, b, c, d) &= lkkt\,(\ lkkt(lkkt(a, b), c)\ ,\ d\ ) \end{aligned}$$

azonosságokat (ez utóbbiak azt mondják, hogy: az $lnko$ és $lkkt$ műveletek *asszociatívak*).

Általában pedig:

$$lnko(a_1, ..., a_k) = lnko\,(lnko(a_1, ..., a_{k-1}), a_k) \quad \square$$

a) Az Euklideszi algoritmust kétszer futtatva kapjuk, hogy $lnko(a, b) = d$ és $lnko(c, d) = x$, ami adja a végeredményt: $lnko(a, b, c) = x$.

Esetünkben $lnko(29601, 26565) = 759$ és $lnko(16302, 759) = 33$, így $\mathbf{lnko(29601, 26565, 16302) = 33}$.

Továbbá $lkkt(29601, 26565) = 29601 \cdot 26565/759 = 1\,036\,035$

és $lkkt(16302, 1036035) = 16302 \cdot 1036035$ / $lnko(16302, 1036035) =$

$= 16302 \cdot 1036035/429 = 39\,369\,330$,

vagyis $\mathbf{lkkt(29601, 26565, 16302) = 39\,369\,330}$.

Hasonlóan

$lnko(5292, 7623, 6435, 5005) =$

$= lnko(\ lnko\,(\ lnko(5292, 7623), 6435\ )\ ,\ 5005\ ) =$

$= lnko(\ lnko\,(\mathbf{63}, 6435)\ ,\ 5005\ ) =$

$= lnko(\ 9\ ,\ 5005\ ) = 1\ ,$

és

$lkkt(5292, 7623, 6435, 5005) =$

$= lkkt(\ lkkt\,(\ lkkt(5292, 7623), 6435\ )\ ,\ 5005\ ) =$

$= lkkt(\ lkkt\,(\ (5292 \cdot 7623/63), 6435\ )\ ,\ 5005\ ) =$

$= lkkt(\ lkkt\,(640332, 6435)\ ,\ 5005\ ) =$

$= lkkt(\ (640332 \cdot 6435/lnko(640332, 6435))\ ,\ 5005\ ) =$

$= lkkt(\ (640332 \cdot 6435/99)\ ,\ 5005\ ) =$

$= lkkt(\ 41621580,\ 5005\ ) =$

$= 41621580 \cdot 5005\ /\ lnko(41621580, 5005) =$

$= 41621580 \cdot 5005\ /\ 5005 =$

$= 41621580\ .$

b) Mivel $lnko(14700, 21021, 9867) = 3$, ezért a három szám *nem* relatív prím.

c) Pl. 6, 10 és 15 .

4.3.3.5) Kézenfekvő, hogy $T = lkkt(t_1, t_2)$ idő múlva mindketten egész köröket futottak, vagyis ekkor a *startnál* találkoznak. Ugyanezt másképpen is megfogalmazhatjuk: a startnál *csak akkor* találkozhatnak, ha mindketten egész köröket futottak, vagyis csak $T = lkkt(t_1, t_2)$ idő múlva.

DE:

a) $lkkt(6, 10) = 30$ percenként a startnál találkoznak.
DE pl. 15 perc múlva egyikük $2\frac{1}{2}$ kört, másikuk $1\frac{1}{2}$ kört futott, vagyis a pálya felénél (a starttal szemközt) is találkoznak! Lásd még a általános megoldást a (d) pontban!

b) $lkkt(20, 35) = 140$ percenként a startnál találkoznak.
DE pl. $\frac{140}{3} = 46\frac{2}{3}$ perc múlva egyikük $\frac{140}{3} : 20 = \frac{7}{3} = 2\frac{1}{3}$ kört, másikuk $\frac{140}{3} : 35 = \frac{4}{3} = 1\frac{1}{3}$ kört futott, vagyis a pálya *harmadánál* is találkoznak! Lásd még a általános megoldást a (d) pontban!

c) $lkkt(5,15) = 15$ percenként a startnál találkoznak.
DE pl. $7\frac{1}{2}$ perc múlva egyikük $1\frac{1}{2}$ kört, másikuk $\frac{1}{2}$ kört futott, vagyis a pálya felénél (a starttal szemközt) is találkoznak! Lásd még a általános megoldást a d) pontban!

d) i) *Mikor* találkoznak?
Legyen a pálya hossza K, a versenyzők sebessége $v_1 = K/t_1$ és $v_2 = K/t_2$. Tegyük fel, hogy $t_1 < t_2$ azaz $v_1 > v_2$. Nyilván akkor találkoznak (t idő múlva), ha az általuk megtett utak *különbsége* éppen a pálya hosszának *egész* számú többszöröse, azaz

$$v_1 \cdot t = v_2 \cdot t + x \cdot K \quad (x \in \mathbb{N})$$

aminek megoldása (kis rendezés után)

$$t = x \cdot \frac{t_2 t_1}{t_2 - t_1} \quad (x \in \mathbb{N}) \quad . \tag{4.6}$$

Abban az esetben, *ha* t_1 és t_2 *egész számok*, akkor felhasználhatjuk a

$$T = lkkt(t_1, t_2) = d \cdot t_1^{'} \cdot t_2^{'} \tag{4.7}$$

összefüggést, ahol

$$\begin{aligned} t_1 \;\; = \;\; & d \cdot t_1^{'} \, , \quad t_2 = d \cdot t_2^{'} \, , \quad d = lnko(t_1, t_2) \, , \\ & t_1^{'} \textit{és } t_2^{'} \textit{ relatív prímek} \, , \end{aligned} \tag{4.8}$$

aminek alapján a (4.6) eredmény így is írható:

$$t = x \cdot \frac{T}{t_2^{'} - t_1^{'}} \quad (x \in \mathbb{N}) \quad . \tag{4.9}$$

Ez magyarázatot ad az (a),...,(c) esetekben "véletlenül" felfedezett tényekre: a versenyzők a pálya más részénél, azaz T törtrésze idő múlva is találkozhatnak.

d) ii) *Hol* (a pálya mely részénél) találkoznak?
Jelölje α azt a törtszámot, hogy t idő múlva a pálya hosszának *hányad részénél* találkoznak:

$$0 \leq \alpha < 1$$

és a versenyzők által megtett utak

$v_1 t = y_1 K + \alpha K$ illetve $v_2 t = y_2 K + \alpha K$ $(y_1, y_2 \in \mathbb{N})$.

Egyszerűen

$$\alpha = \left\{ \frac{t}{t_1} \right\}$$

(ami persze ugyanaz, mint $\{t/t_2\}$), ahol $\{\mathbf{r}\}$ jelöli az $r \in \mathbb{R}$ valós szám tört részét[10)].

A (4.6) eredményt felhasználva kapjuk hogy

$$\alpha = \left\{ x \cdot \frac{t_2}{t_2 - t_1} \right\} \quad (x \in \mathbb{N}) \tag{4.10}$$

(ami sajnos legtöbbször *nem* egyezik meg[11)] $x \cdot \left\{ \frac{t_2}{t_2 - t_1} \right\}$ -el),

vagy (amennyiben lehetséges): $lnko(t_1, t_2)$ -vel való egyszerűsítés után

$$\alpha = \left\{ x \cdot \frac{t_2'}{t_2' - t_1'} \right\} \quad (x \in \mathbb{N}) \quad . \tag{4.11}$$

Ha λ -val jelöljük, hogy a második futó hányszor lassabb az elsőnél, azaz

$$t_2 = \lambda \cdot t_1 \qquad (\lambda \in \mathbb{R} \ , \quad \lambda \geq 1) \ ,$$

akkor (4.10) a következőképpen is írható:

$$\alpha = \left\{ x \cdot \frac{\lambda}{\lambda - 1} \right\} \quad (x \in \mathbb{N}) \quad . \tag{4.12}$$

d) iii) Milyen *feltételek* esetén találkozhatnak *csak* a a startjelnél? A megoldás mindenképpen

$$\alpha = 0 \quad .$$

[10)] **Definíció:** *Tetszőleges* $r \in \mathbb{R}$ *valós számra* $\{r\} := r - [r]$ *jelöli az* r *szám* **tört rész**ét, *és* $\{\}$ *a* **törtrész függvény**. □

Pozitív r szám esetén $\{r\}$ a tizedesjegy *utáni* részét jelöli, míg negatív r esetén $\{r\} = 1-$ a fenti mennyiség. Nyilvánvalóan $0 \leq \{r\} < 1$ minden $r \in \mathbb{R}$ esetén.

[11)] **Állítás:** *Ha* $u > 0$, $x \in \mathbb{N}$ *és* $x \cdot \{u\} < 1$, *akkor* $\{x \cdot u\} = x \cdot \{u\}$.
Bizonyítás: Mivel $u > 0$, ezért $u = [u] + \{u\}$, és így
$\{x \cdot u\} = \{x[u] + x\{u\}\} = \{x\{u\}\} = x\{u\}$ mivel $x \in \mathbb{N}$. □
$x \cdot \{u\} \geq 1$ esetén az állítás nyilvánvalóan *nem* teljesül.

Amennyiben t_1 és t_2 *egész számok*, akkor az (4.11) képletből érdemes kiindulni: $\alpha = 0$ *akkor és csak akkor* teljesül, ha

$$t_2^{'} - t_1^{'} = 1 \quad .$$

Ha t_1 és t_2 *nem* egész számok, akkor az (4.12) képletből kapjuk, hogy a feltétel

$$v = \frac{\lambda}{\lambda - 1} \in \mathbb{N}$$

ahonnan

$$\lambda = \frac{v}{v-1} = 1 + \frac{1}{v-1} \qquad (v \in \mathbb{N}) \ ,$$

vagy szavakban: λ *csak* $1 + \frac{1}{v-1}$ alakú tört lehet.

Javasoljuk az Olvasónak, hogy a fenti képleteket legalább az a), b), c) esetekre próbálja ki!

4.3.3.6) a) Az előző feladat d) részének jelöléseit használva

$$v_1 \cdot t + v_2 \cdot t = x \cdot K \quad (x \in \mathbb{N})$$

ahonnan

$$t = x \cdot \frac{t_2 t_1}{t_2 + t_1} \quad (x \in \mathbb{N}) \quad .$$

Vegyük észre, hogy a pálya bármely részén találkozhat, és utána a feladat ismét ugyanaz: a startjel helyett a találkozási pontot kell tekintenünk.

b) Az ingamozgás képletei szerint: t idő múlva a hinták helyzetei

$\sin(t \cdot \frac{2\pi}{t_1})$ illetve $\sin(t \cdot \frac{2\pi}{t_2})$, azaz a találkozás feltétele

$$\sin(t \cdot \frac{2\pi}{t_1}) = \sin(t \cdot \frac{2\pi}{t_2})$$

aminek megoldásai:

egyirányú mozgásnál

$$t \cdot \frac{2\pi}{t_1} = t \cdot \frac{2\pi}{t_2} + k \cdot 2\pi \quad (k \in \mathbb{Z})$$

azaz

$$t = k \cdot \frac{t_1 t_2}{t_2 - t_1} \quad (k \in \mathbb{Z}) \tag{4.13}$$

amely megegyezik a (4.6) eredménnyel,

míg ellentétes irányú mozgásnál

$$t \cdot \frac{2\pi}{t_1} = t \cdot \frac{2\pi}{t_2} + m \cdot 2\pi \quad (m \in \mathbb{Z})$$

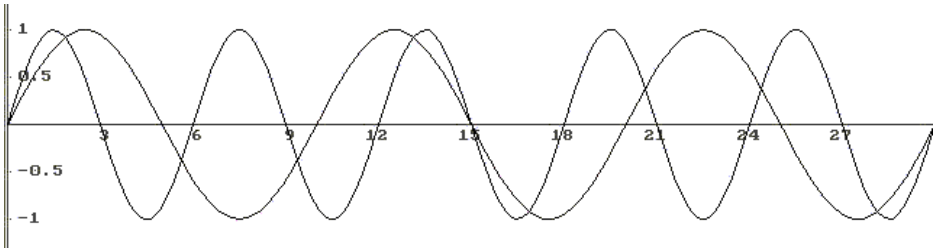
azaz

$$t = \frac{2m+1}{2} \cdot \frac{t_1 t_2}{t_2 + t_1} \quad (m \in \mathbb{Z}) \,. \tag{4.14}$$

Abban az esetben, *ha* t_1 és t_2 *egész számok*, akkor felhasználhatjuk a (4.7) és (4.8) összefüggéseket, amik alapján

$$(2m+1) \cdot \frac{T}{2\left(t_2' + t_1'\right)} \quad (m \in \mathbb{Z}) \,.$$

A (4.13) és (4.14) eredményeket jól láthatjuk az alábbi ábrán ($t_1 = 6$ és $t_2 = 10$):



4.3.3.6) feladat

A metszéspontok: $t = k \cdot 15$ és $t = (2m+1) \cdot \frac{30}{2 \cdot 8}$ $(k, m \in \mathbb{Z})$.

4.3.3.7) Amíg az egyik futó 22 métert fut, addig a gyorsabbik 32 métert tesz meg, vagyis sebességük aránya 11:16. Amíg tehát az első futó 11 kört fut, addig a második 16-ot. így egy lekörözés után a második futónak 16 kört kell futnia, míg újra a pályának ugyanazon a helyén éri utol és körözi le társát. Közben azonban ő 5-tel több kört tett meg, így közben már négyszer lekörözte társát, a pálya 4 különböző pontján. Vagyis az első lekörözés helyével együtt 5 olyan pontja van a pályának, ahol a gyorsabbik futó lekörözheti társát.

4.3.3.8) A kitűzött (és hasonló) problémák kapcsolatát a tényleges valóságos jelenségekkel részletesen elemzi Sárközy András [$SA'78$] könyve.

4.3.3.9) a)

$$\frac{n+11}{n-9} = \frac{n-9+20}{n-9} = 1 + \frac{20}{n-9} \quad ,$$

vagyis a tört értéke akkor egész, ha $\frac{20}{n-9}$ is egész, vagyis a nevező osztója a számlálónak. Vagyis

$n-9 = \pm 1,\ \pm 2,\ \pm 4,\ \pm 5,\ \pm 10$ vagy ± 20

lehet csak, ahonnan n lehetséges értékei

$n = 10,\ 8,\ 11,\ 7,\ 13,\ 5,\ 14,\ 4,\ 19,\ -1,\ 29,\ -11$.

b) $\frac{(3n+5)}{(n+3)} = 3 - \frac{4}{n+3}$.

c) $\frac{\left(n^2+1\right)}{(n+1)} = \frac{n(n+1)-(n+1)+2}{n+1} = n - 1 + \frac{2}{n+1}$.

4.3.3.10) Legelső gondolatunk az lehet, hogy egy tört akkor (és csak akkor) egyszerűsíthető, ha

$$\textit{lnko(számláló,nevező)} > 1 .$$

Azonban $\mathbb{Z}[x]$ hiába polinomgyűrű, de ebben a struktúrában **nincs** Euklideszi algoritmus (mert $\mathbb{Z}$ -ben nem lehet osztani).

Azonban **tudjuk**, hogy *tetszőleges* gyűrűben $d|x$ *és* $d|y$ -ból következik, hogy $d|x \pm y$, sőt általában

$$d \mid mx + ny$$

tetszőleges x, y gyűrűbeli elemekre és $m, n \in \mathbb{Z}$ egész együtthatókra. □

a) $\frac{n+13}{n-9} = \frac{n-9+22}{n-9}$, vagyis egyszerűsíteni pontosan akkor lehet, ha $lnko(22, n-9) > 1$. Ez akkor teljesül, ha $n-9$ osztható 2-vel vagy 11-gyel (de $n-9 \neq 0$); vagyis $n = 2k+9 = 2\ell+1$ vagy $n = 11t+9$ alakú valamilyen $\ell, t \in \mathbb{Z}$, $k, t \neq 0,\ \ell \neq 4$ egész számokra.

b) Mivel

$$3 \cdot (14n+3) - 2 \cdot (21n+4) = 1 \quad ,$$

ezért

$$lnko\left((14n+3), (21n+4)\right) \mid 1 \quad ,$$

vagyis a tört *nem* egyszerűsíthető[12)].

[12)] KöMaL C.461.gyakorlat, 1997/nov.,481.old.

c) Póbáljuk meg az Euklideszi algoritmust alkalmazni:

$$\begin{aligned}(8n+7) &= 1\cdot(5n+6)+(3n+1)\\ (5n+6) &= 1\cdot(3n+1)+(2n+5)\\ (3n+1) &= 1\cdot(2n+5)+(n-4)\\ (2n+5) &= 2\cdot(n-4)+13\end{aligned}$$

ezért

$$lnko\left((5n+6),(8n+7)\right) = 13 \quad .$$

Mivel 13 prímszám, ezért az $\frac{5n+6}{8n+7}$ törtet csak olyan $n\in\mathbb{Z}$ egész szám esetén lehet egyszerűsíteni, amelyre

$$13 \mid 5n+6 \quad \text{és} \quad 13 \mid 8n+7$$

azaz

$$\begin{cases} 5n+6\equiv 0 \pmod{13} \\ 8n+7\equiv 0 \pmod{13} \end{cases} ,$$

melynek megoldása

$$\begin{cases} n\equiv -6/5\equiv 7\cdot 8\equiv 4 \pmod{13} \\ n\equiv -7/8\equiv 6\cdot 5\equiv 4 \pmod{13} \end{cases}$$

vagyis a megoldás:

$$n=13k+4 \quad (k\in\mathbb{Z}) \quad .$$

Ellenőrzés: $5n+6=5\,(13k+4)+6=13(5k+2)$
és $8n+7=8\,(13k+4)+7=13(8k+3)$, vagyis a tört az ilyen $n\in\mathbb{Z}$ egész számokra valóban egyszerűsíthető 13 -mal.

Az alábbi feladatok megoldása előtt érdemes átolvasni a 4.3.1 "*Z[α] struktúrák*" c. alfejezetet a 4.3.1.1) c) feladat megoldásánál.

4.3.3.11) b) $(p=0,\, q=1,\, \alpha=i)$ $\frac{2+7i}{-1+3i}=\frac{19}{10}-\frac{13}{10}i$,
ezért a hányados $2-i$, a maradék

$$(2+7i)-(-1+3i)*(2-i)=1 \quad ,$$

tehát a maradékos osztás

$$(2+7i)=(-1+3i)*(2-i)+1 \quad ,$$

és valóban $N(1) = 1 < N(-1+3i) = 10$.

4.3.3.12) a) $(p = 0,\, q = 1,\, \alpha = i)$

Az Euklideszi algoritmust használva

$N(6+6i) = 72 > N(5+3i) = 34$, ezért

$(6+6i) = (5+3i) * 1 + (1+3i)$, $N(1+3i) = 10$

$(5+3i) = (1+3i) * (1-i) + (1+i)$, $N(1+i) = 2$

$(1+3i) = (1+i) * (2+i) + 0$, $N(0) = 0$,

tehát $lnko(6+6i,\, 5+3i) = (1+i)$.

b) $(p = 0,\, q = 2,\, \alpha = i\sqrt{2})$ $lnko = 1 + i\sqrt{2}$,

c) $(p = 1,\, q = 1,\, \alpha = -\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ $lnko = 1$,

d) $(p = 0,\, q = -2,\, \alpha = \sqrt{2})$ $lnko = 2 - \sqrt{2}$.

e) $lnko(13+8i,\, 5+3i) = 1$

f) $lnko(3+22i,\, 39-20i) = 1-4i$.

4.3.4. Lineáris Diophantikus egyenletek

4.3.4.1) a) $6120x + 3141y = 4$ *egyenlet megoldása:*

Először az Euklideszi algoritmussal meghatározzuk az együtthatók lnko -ját (a maradékokat < > -be zártuk):

<6120> = <3141> * 1 + <2979>
<3141> = <2979> * 1 + < 162>
<2979> = < 162> * 18 + < 63>
< 162> = < 63> * 2 + < 36>
< 63> = < 36> * 1 + < 27>
< 36> = < 27> * 1 + < 9>
< 27> = < 9> * 3 + < 0>

Mivel $lnko(6120, 3141) = 9$ nem osztója a konstans tagnak: $9 \nmid 4$, ezért az egyenletnek nincs gyöke ("nem oldható meg") .

b) $5682x + 4836y = 30$ *egyenlet megoldása:*

Az együtthatók lnko -ja (a maradékokat [ ] -be zártuk):

$$\begin{aligned}
[5682] &= [4836] \cdot 1 + [846] \\
[4836] &= [846] \cdot 5 + [606] \\
[846] &= [606] \cdot 1 + [240] \\
[606] &= [240] \cdot 2 + [126] \\
[240] &= [126] \cdot 1 + [114] \\
[126] &= [114] \cdot 1 + [12] \\
[114] &= [12] \cdot 9 + [6] \\
[12] &= [6] \cdot 2 + [0]
\end{aligned}$$

tehát $lnko(5682, 4836) = 6$,

majd visszafejtve:

$$\begin{aligned}
6 = & \ 1 \cdot [114] - 9 \cdot [12] = \\
= & \ 1 \cdot [114] - 9 \cdot ([126] - 1 \cdot [114]) = -9 \cdot [126] + 10 \cdot [114] = \\
= & -9 \cdot [126] + 10 \cdot ([240] - 1 \cdot [126]) = 10 \cdot [240] - 19 \cdot [126] = \\
= & \ 10 \cdot [240] - 19 \cdot ([606] - 2 \cdot [240]) = -19 \cdot [606] + 48 \cdot [240] = \\
= & -19 \cdot [606] + 48 \cdot ([846] - 1 \cdot [606]) = 48 \cdot [846] - 67 \cdot [606] = \\
= & \ 48 \cdot [846] - 67 \cdot ([4836] - 5 \cdot [846]) = -67 \cdot [4836] + 383 \cdot [846] = \\
= & -67 \cdot [4836] + 383 \cdot ([5682] - 1 \cdot [4836]) = 383 \cdot [5682] - 450 \cdot [4836] \ ,
\end{aligned}$$

ahonnan a gyökök:

$$x_0 = 383 \cdot C/d = 1915, \quad y_0 = -450 \cdot C/d = -2250$$

és az egyenlet általános megoldása:

$$x = x_0 + k \cdot b/d = 1915 + k \cdot 806, \quad y = y_0 - k \cdot a/d = -2250 - k \cdot 947 \quad (k \in \mathbb{Z})$$

c) Az $10518x + 5682y = 6$ egyenlet megoldása

$$\begin{aligned}
[10518] &= [5682] \cdot 1 + [4836] \\
[5682] &= [4836] \cdot 1 + [846] \\
[4836] &= [846] \cdot 5 + [606] \\
[846] &= [606] \cdot 1 + [240] \\
[606] &= [240] \cdot 2 + [126] \\
[240] &= [126] \cdot 1 + [114] \\
[126] &= [114] \cdot 1 + [12] \\
[114] &= [12] \cdot 9 + [6]
\end{aligned}$$

$$[12] = \quad [6] \cdot 2 + \quad [0]$$

majd

$$\begin{aligned}
&lnko(10518, 5682) = 6 = 1 \cdot [114] - 9 \cdot [12] = \\
&\quad = 1 \cdot [114] - 9 \cdot ([126] - 1 \cdot [114]) = -9 \cdot [126] + 10 \cdot [114] = \\
&\quad = -9 \cdot [126] + 10 \cdot ([240] - 1 \cdot [126]) = 10 \cdot [240] - 19 \cdot [126] = \\
&\quad = 10 \cdot [240] - 19 \cdot ([606] - 2 \cdot [240]) = -19 \cdot [606] + 48 \cdot [240] = \\
&\quad = -19 \cdot [606] + 48 \cdot ([846] - 1 \cdot [606]) = 48 \cdot [846] - 67 \cdot [606] = \\
&\quad = 48 \cdot [846] - 67 \cdot ([4836] - 5 \cdot [846]) = -67 \cdot [4836] + 383 \cdot [846] = \\
&\quad = -67 \cdot [4836] + 383 \cdot ([5682] - 1 \cdot [4836]) = 383 \cdot [5682] - 450 \cdot [4836] = \\
&\quad = 383 \cdot [5682] - 450 \cdot ([10518] - 1 \cdot [5682]) = -450 \cdot [10518] + 833 \cdot [5682]
\end{aligned}$$

ahonnan

$$x_0 = -450 \cdot C/d \ , \qquad y_0 = 833 \cdot C/d = 833 \ .$$

Az általános megoldás:

$$x = x_0 + k \cdot b/d = -450 + k \cdot 947 \ , \qquad y = y_0 - k \cdot a/d = 833 - k \cdot 1753$$

$(k \in \mathbb{Z})$

d) $4512x + 1111y = 3248$ egyenlet megoldása:

$$\begin{aligned}
[4512] &= [1111] \cdot 4 + [68] \\
[1111] &= [68] \cdot 16 + [23] \\
[68] &= [23] \cdot 2 + [22] \\
[23] &= [22] \cdot 1 + [1] \\
[22] &= [1] \cdot 22 + [0]
\end{aligned}$$

vagyis $lnko(4512, 1111) = 1$.

Visszafejtve

$$\begin{aligned}
&lnko(4512, 1111) = 1 = \\
&\quad = [23] - 1 \cdot [22] = \\
&\quad = 1 \cdot [23] - 1 \cdot ([68] - 2 \cdot [23]) = -1 \cdot [68] + 3 \cdot [23] = \\
&\quad = -1 \cdot [68] + 3 \cdot ([1111] - 16 \cdot [68]) = 3 \cdot [1111] + (-49) \cdot [68] = \\
&\quad = 3 \cdot [1111] + (-49) \cdot ([4512] - 4 \cdot [1111]) = -49 \cdot [4512] + 199 \cdot [1111]
\end{aligned}$$

ahonnan

$$x_0 = -49 \cdot C/d = -159152 \ , \qquad y_0 = 199 \cdot C/d = 646352 \ .$$

Az általános megoldás:

$x = x_0 + k \cdot b/d = -159152 + k \cdot 1111$,

$y = y_0 - k \cdot a/d = 646352 - k \cdot 4512 \qquad (k \in \mathbb{Z})$

4.3.4.2) A $24x+33y = 25200$ Diophantikus egyenlet általános megoldása:

$$x = -33600 + k \cdot 11 \ , \quad y = 25200 + k \cdot 8 \quad (k \in \mathbb{Z}) \ ,$$

ennek nemnegatív gyökei kellenek:

$0 \leq -33600 + k * 11$ és $0 \leq 25200 - k * 8 \quad (k \in \mathbb{Z})$,

azaz $\frac{33600}{11} \approx 3054.54 \leq k \leq \frac{25200}{8} = 3150 \quad (k \in \mathbb{Z})$,

vagyis a válasz: 96 lehetőségünk van.

Megjegyzés: Természetesen a szokásos általános iskolai "favágós" megoldás is van: x -et növeljük 0 -tól addig, míg y egész nem lesz, majd ebből a kezdő megoldásból más megoldásokat gyártunk (hogyan?)

4.3.4.3) a) A $4x + 2,5y = 42$, vagyis egész számokra beszorozva (bővítve) a

$$8x + 5y = 84$$

lineáris Diophanikus egyenlet (nemnegatív) gyökeit keressük.

A megoldások: $(3; 12)$ és $(8; 4)$.

b) Az $x + 0,7y = 4,6$, azaz a $10x + 7y = 46$ egyenletnek nincs *nemnegatív* gyöke.

Ha azonban megelégszünk 1dl veszteséggel, akkor az $x + 0,7y = 4,5$, azaz a $10x + 7y = 45$ egyenlet nemnegatív gyökeit kell megkeresnünk: $x = 1$, $y = 5$.

c) Az $85x + 60y = 700$ lineáris Diophanikus egyenlet (nemnegatív) gyökei: $x = 4$, $y = 6$.

4.3.4.4) A $4x - 6y \equiv 3$ illetve a $238x - 28y \equiv 436$ Diophantikus egyenleteket kell megoldanunk.

4.3.4.5) a) Átalakítás után a $114x - 1683y = 3$ lineáris Diophantikus egyenletet kapjuk, aminek megoldása:

$[114] \ = [-1683] \cdot 0 + [114]$

$$
\begin{aligned}
[-1683] &= [114]\cdot(-14)+[-87]\\
[114] &= [-87]\cdot(-1)+[27]\\
[-87] &= [27]\cdot(-3)+[-6]\\
[27] &= [-6]\cdot(-4)+[3]\\
[-6] &= [3]\cdot(-2)+[0]\ ,
\end{aligned}
$$

így

$$
\begin{aligned}
&lnko(114,-1683)=3=\\
&=1\cdot[27]+4\cdot[-6]\\
&=1\cdot[27]+4\cdot([-87]-(-3)\cdot[27])=4\cdot[-87]+13\cdot[27]\\
&=4\cdot[-87]+13\cdot([114]-(-1)\cdot[-87])=13\cdot[114]+17\cdot[-87]\\
&=13\cdot[114]+17\cdot([-1683]-(-14)\cdot[114])=17\cdot[-1683]+251\cdot[114]\\
&=17\cdot[-1683]+251\cdot([114]-0\cdot[-1683])=251\cdot[114]+17\cdot[-1683]\ ,
\end{aligned}
$$

$$x_0=251\cdot C/d=251\ ,\quad y_0=17\cdot C/d=17\ ,$$

Az általános megoldás:

$$x=x_0+k\cdot b/d=251+k\cdot(-561)\ ,\qquad y=y_0-k\cdot a/d=17-k\cdot 38$$
$(k\in\mathbb{Z})$.

A fentiek alapján a kongruencia megoldása: $x\equiv 251 \pmod{1683}$.

b) Átalakítás után a $18x-175y=1$ lineáris Diophantikus egyenletet kapjuk, aminek megoldása:

$$
\begin{aligned}
[18] &= [-175]\cdot 0+[18]\\
[-175] &= [18]\cdot(-9)+[-13]\\
[18] &= [-13]\cdot(-1)+[5]\\
[-13] &= [5]\cdot(-2)+[-3]\\
[5] &= [-3]\cdot(-1)+[2]\\
[-3] &= [2]\cdot(-1)+[-1]\\
[2] &= [-1]\cdot(-2)+[0]\ ,
\end{aligned}
$$

így $lnko(18,-175)=-1=$

$$
\begin{aligned}
&=1\cdot[-3]-(-1)\cdot[2]\\
&=1\cdot[-3]+1\cdot([5]-(-1)\cdot[-3])=1\cdot[5]+2\cdot[-3]\\
&=1\cdot[5]+2\cdot([-13]-(-2)\cdot[5])=2\cdot[-13]+5\cdot[5]\\
&=2\cdot[-13]+5\cdot([18]-(-1)\cdot[-13])=5\cdot[18]+7\cdot[-13]\\
&=5\cdot[18]+7\cdot([-175]-(-9)\cdot[18])=7\cdot[-175]+68\cdot[18]\\
&=7\cdot[-175]+68\cdot([18]-0\cdot[-175])=68\cdot[18]+7\cdot[-175]
\end{aligned}
$$

ahonnan

$x_0 = 68 \cdot C/d = -68$, $y_0 = 7 \cdot C/d = -7$.

Az általános megoldás:

$x = x_0 + k \cdot b/d = -68 + k \cdot 175$, $y = y0 - k \cdot a/d = -7 - k \cdot (-18)$ $(k \in \mathbb{Z})$.

A fentiek alapján a 18 multiplikatív inverze:

$$18^{-1} \equiv -68 \equiv 107 \pmod{175} \quad .$$

Ellenőrzés: $18 \cdot 107 = 1926 \equiv 1 \pmod{175}$.

4.3.4.6) Ha m jelöli a keresett számot, akkor

$$\begin{cases} 25707 \equiv 32 \pmod{m} \\ 37568 \equiv 43 \pmod{m} \end{cases}$$

ahonnan

$$\begin{cases} 25707 = k \cdot m + 32 \\ 37568 = \ell \cdot m + 43 \end{cases}$$

vagyis

$$m \mid lnko(25707 - 32\ ,\ 37568 - 43) = lnko(25675, 37525) = 1975 \quad .$$

Mivel m négyjegyű, ezért csak $m = 1975$ lehet a megoldás.

4.3.4.7) **(0)** Előrebocsátjuk, hogy a megoldhatóság *szükséges és elégséges* feltétele:

$$lnko(a, b, c) \mid m \quad .$$

(1) Az Euklideszi algoritmussal megkeressük $d := lnko(a, b)$ -t.

(2) az $ax + by = td$ $(t \in \mathbb{Z})$ egyenletek általános megoldása

$x = t \cdot x_o + \frac{lkkt(a,b)}{a} \cdot k$, $y = t \cdot y_o + \frac{lkkt(a,b)}{b} \cdot k$ $(k \in \mathbb{Z})$.

(3) Számítsuk ki $\delta := lnko(d, c)$ értékét (az Euklideszi algoritmussal).

(4) Oldjuk meg az $dt + cz = m$ egyenletet, melynek általános megoldása

$t = \frac{m}{\delta} \cdot t_o + \frac{lkkt(d,c)}{d} \cdot \ell \ , \quad z = \frac{m}{\delta} \cdot z_o - \frac{lkkt(d,c)}{c} \cdot \ell \qquad (\ell \in \mathbb{Z}) \ .$

Tehát az $ax + by + cz = m$ lineáris Diophantikus egyenletek általános megoldása:

$$\left\{ \begin{array}{ll} x = t \cdot x_o + \frac{lkkt(a,b)}{a} \cdot k & \\ y = t \cdot y_o + \frac{lkkt(a,b)}{b} \cdot k \qquad ahol & t = \frac{m}{\delta} \cdot t_o + \frac{lkkt(d,c)}{d} \cdot \ell \\ z = \frac{m}{\delta} \cdot z_o - \frac{lkkt(d,c)}{c} \cdot \ell & k, \ell \in \mathbb{Z} \end{array} \right. .$$

Megjegyzés: $\delta = lnko(a,b,c)$, továbbá a megoldhatóság *szükséges és elégséges* feltétele:

$$\delta \mid m \quad .$$

4.3.4.8) a) Az $12x + 30y + 15z = 18$ egyenlet megoldása:

(0) mivel $lnko(12, 30, 15) = 3 \mid 18$, ezért van gyöke az egyenletnek,

(1) $d = lnko(12, 30) = 6$,

(2) a $12x + 30y = t \cdot 6$ egyenletek általános megoldása:

$x = t \cdot (-2) + 5k \ , \quad y = t \cdot 1 - 2k \ ,$

(3) $\delta = lnko(d, c) = lnko(6, 15) = 3$,

(4) a $6 \cdot t + 15 \cdot z = 18$ egyenletek általános megoldása:

$t = 6 \cdot (-2) + 5\ell \ , \qquad z = 6 \cdot 1 - 2\ell \ ,$

így az általános megoldás:

$$\left\{ \begin{array}{ll} x = t \cdot (-2) + 5 \cdot k & \\ y = t \cdot 1 - 2 \cdot k \qquad ahol & t = -12 + 5 \cdot \ell \\ z = 6 \cdot 1 - 2\ell & k, \ell \in \mathbb{Z} \end{array} \right.$$

azaz

$$\left\{ \begin{array}{ll} x = (-12 + 5\ell) \cdot (-2) + 5k & \\ y = (-12 + 5\ell) - 2k \qquad ahol & k, \ell \in \mathbb{Z} \\ z = 6 - 2\ell & \end{array} \right. .$$

Ellenőrzés: $12x + 30y + 15z =$

$= 12 \cdot ((-12 + 5\ell) \cdot (-2) + 5k) + 30 \cdot ((-12 + 5\ell) - 2k) + 15 \cdot (6 - 2\ell) = 18.$

Érdekességképpen közlünk egy "elemi iskolás" megoldást is.

Mivel teljesül a $3 = lnko(12, 30, 15) \mid 18$ (szükséges) feltétel, ezért az egyenletnek léteznek egész gyökei.

Egyszerűsítés után a

$$4x + 10y + 5z = 6 \tag{4.15}$$

egyenletet kapjuk.

Először megoldjuk a *kétismeretlenes*

$$4x + 10y = 6 - 5z \tag{4.16}$$

egyenletet ($z \in \mathbb{Z}$ paraméter): $lnko(4, 10) = 2$ és $lkkt(4, 10) = 20$ alapján a megoldás

$$x = \left(-2 - \frac{20}{4}k\right) \cdot \left(\frac{6 - 5z}{2}\right) \ , \quad y = \left(1 + \frac{20}{10}k\right) \cdot \left(\frac{6 - 5z}{2}\right) \tag{4.17}$$

feltéve, hogy $6 - 5z$ osztható 2 -vel. Ez utóbbi feltétel

$$6 - 5z = 2\ell \ , \quad \text{vagyis} \quad 6 = 5z + 2\ell$$

alakban írható, amely egyenlet megoldása:

$$z = 6 + t * 2 \ , \quad \ell = -12 + t * 5 \quad (t \in \mathbb{Z}) \ ,$$

ami alapján a (4.15) egyenlet általános megoldása

$$\begin{aligned} x_0 &= \left(-2 - \frac{20}{4}k\right) \cdot \ell = \left(-2 - \frac{20}{4}k\right) \cdot (-12 + t * 5) \ , \\ y_0 &= \left(1 + \frac{20}{10}k\right) \cdot \ell = \left(1 + \frac{20}{10}k\right) \cdot (-12 + t * 5) \ , \\ z_0 &= 6 + t * 2 \ , \qquad k, t \in \mathbb{Z} \ . \end{aligned}$$

Az eredeti egyenlet megoldása tehát, $lnko(12, 30, 15) = 3$ alapján

$$\begin{aligned} x &= 3 \cdot \left(-2 - \frac{20}{4}k\right) \cdot (-12 + t * 5) \ , \\ y &= 3 \cdot \left(1 + \frac{20}{10}k\right) \cdot (-12 + t * 5) \ , \\ z &= 3 \cdot (6 + t * 2) \ , \qquad k, t \in \mathbb{Z} \ . \end{aligned}$$

d) Az a) egyenlet pozitív gyökeinek megtalálásához olyan $k, \ell \in \mathbb{Z}$ *egész* számokat kell keresnünk, amelyekre

$$\begin{cases} 0 & \leq & (-12+5\ell)\cdot(-2)+5k \\ 0 & \leq & (-12+5\ell)-2k \\ 0 & \leq & 6-2\ell \end{cases} .$$

4.3.4.9) Mivel 3 , 4 és 7 relatív prímek[13)], ezért először megoldjuk a

$$3x+4y+7z=1$$

egyenletet, majd a kapott gyökök mindegyikét n -el szorozzuk.

4.3.4.10) Azt keressük, hogy milyen n esetén vannak ill. nincsenek a $6x+9y+20z=n$ Diophantikus egyenleteknek *nemnegatív* gyökei. A problémát a fenti általános módszerekkel is megoldhatjuk (HF), alább azonban a KöMaL -ban megjelent megoldást közöljük.

Most csak olyan egész számokról beszélünk, amelyek előállíthatók 6, 9 és 20 többszöröseinek összegeként.

A 6 és 9 többszöröseinek összegei a $6a+9b=3(2a+3b)$ alakú számok, ezek között minden $3k$ $(k \geq 2)$ alakú szám előfordul, hiszen $2a+3b$ alakban az 1-nél nagyobb $3r$, $3r+1$, $3r+2$ alakú számok egyaránt felírhatók. Ezért a $20+3k$ alakú számok $k \geq 2$ esetén előállíthatók a kívánt módon, és ugyanez a $40+3k$ alakú számokra is igaz. A 46-tól kezdve így minden szám előfordul, mert vagy többszöröse 3-nak, vagy ha $20+3k$ alakú, akkor 3-mal osztva 2-t, míg ha $40+3k$ alakú, akkor 3-mal osztva 1-et ad maradékul.

Kérdés, hogy 26 és 46 között sikerül-e minden számot előállítani? Azt állítjuk, hogy nem, a 43 kimarad, s ez egyben a legnagyobb olyan szám, amelyiket nem írhatunk fel 6, 9 és 20 többszöröseinek összegeként.

A 45 a 9 többszöröse, a $20+3k$ alakú számok $(k \geq 2)$: 26, 29, 32, 35, 38, 41, 44, 47, ... , míg a $40+3k$ alakúak $(k \geq 2)$ 46-tal kezdődnek. A többi (hiányzó) szám vagy többszöröse 3-nak, vagy kisebb 43-nál.

A 43 valóban nem bontható fel a kívánt módon, mert ha 1 db 20-as szerepel benne, akkor 43=20+23, de 23 nem szerepel a 20+3k alakúak között

[13)] Mivel lineáris Diophantikus egyenletről van szó, az együtthatóknak *nem* szükséges *páronként* relatív prímeknek lenniük.

$k \geq 2$ miatt. Ha viszont 43-ban 2 db 20-as szerepel, akkor 43=20+20+3, de 3 darabos csomag nincs.
Tehát a legnagyobb olyan darabszám, amit nem tudunk megrendelni, a 43.

4.3.5. Kínai maradéktétel

4.3.5.1) a) Mivel a $7, 9, 11$ modulusok páronként relatív prímek, ezért $M = lkkt(7, 9, 11) = 7 \cdot 9 \cdot 11 = 693$.

Elsőként az

$$y_i \cdot \frac{M}{m_i} \equiv 1 \pmod{m_i}$$

alakú

$$\begin{aligned} y_1 \cdot 99 &\equiv 1 \quad \text{azaz} \quad y_1 \cdot 1 \equiv 1 \pmod 7 \\ y_2 \cdot 77 &\equiv 1 \quad \text{azaz} \quad y_2 \cdot 5 \equiv 1 \pmod 9 \\ y_3 \cdot 63 &\equiv 1 \quad \text{azaz} \quad y_3 \cdot 8 \equiv 1 \pmod{11} \end{aligned}$$

kongruenciákat kell (egyesével) megoldanunk, amelyek (egyik) megoldása $y_1 = 1, \quad y_2 = 2$ és $y_3 = 7$.

Ezután az eredeti kongruenciarendszer megoldása

$$x \equiv \sum_{i=1}^{3} a_i y_i \frac{M}{m_i} \equiv 2 \cdot 1 \cdot 99 + 3 \cdot 2 \cdot 77 + 3 \cdot 7 \cdot 63 \equiv 597 \pmod{693} \quad .$$

b) A modulusok ismét páronként relatív prímek, ezért

$M = lkkt(7, 12, 25, 11) = 7 \cdot 12 \cdot 25 \cdot 11 = 23\ 100$.

Az

$$y_i \cdot \frac{M}{m_i} \equiv 1 \pmod{m_i}$$

alakú kongruenciák

$$\begin{aligned} y_1 \cdot 3300 &\equiv 1 \pmod 7 \\ y_2 \cdot 1925 &\equiv 1 \pmod{12} \\ y_3 \cdot 924 &\equiv 1 \pmod{25} \\ y_4 \cdot 2100 &\equiv 1 \pmod{11} \end{aligned}$$

megoldásai: $y_1 = -2 \equiv 5$, $y_2 = 5$, $y_3 = -1 \equiv 24$, $y_4 = -1 \equiv 10$.

A kongruenciarendszer megoldása

$$\begin{aligned} x &\equiv \sum_{i=1}^{4} a_i y_i \frac{M}{m_i} \equiv 5 \cdot 5 \cdot 3300 + 2 \cdot 5 \cdot 1925 + 3 \cdot 24 \cdot 924 + 0 = \\ &\equiv 168\,278 \equiv 6578 \pmod{23\,100} . \end{aligned}$$

4.3.5.2) A kongruenciák **nem** $x \equiv a_i$ alakúak, így az általános módszer előtt át kell alakítanunk őket:

Mivel $3^{-1} \equiv 2 \pmod 5$, ezért a $3x \equiv 4 \pmod 5$ kongruencia ekvivalens az $x \equiv 4 \cdot 2 \equiv 3 \pmod 5$ kongruenciával.

Hasonlóan $2^{-1} \equiv 2 \pmod 3$ miatt a $2x \equiv 1 \pmod 3$ kongruencia ekvivalens az $x \equiv 1 \cdot 2 \equiv 2 \pmod 3$ kongruenciával,

$3^{-1} \equiv 5 \pmod 7$ miatt $3x \equiv 2 \pmod 7$ **helyett**
$x \equiv 2 \cdot 5 \equiv 3 \pmod 7$ -et írunk,

$2^{-1} \equiv 5 \pmod 9$ miatt $2x \equiv 3 \pmod 9$ **helyett**
$x \equiv 3 \cdot 2 \equiv 6 \pmod 9$ -et írunk,

$5^{-1} \equiv -2 \pmod{11}$ miatt $5x \equiv 4 \pmod{11}$ **helyett**
$x \equiv 4 \cdot (-2) \equiv 3 \pmod{11}$ -et írunk,

$2^{-1} \equiv 3 \pmod 5$ miatt $2x \equiv 3 \pmod 5$ **helyett**
$x \equiv 3 \cdot 3 \equiv 4 \pmod 5$ -et írunk.

4.3.5.3) Az eredeti kongruenciarendszer :

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 4 \pmod 5 \end{cases}$$

de itt a modulusok nem relatív prímek. Azonban az első kongruencia következik a harmadikból, így elegendő csak az utolsó hármat tekintenünk:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 4 \pmod 5 \end{cases}$$

Ennek megoldása: $M = 60,\quad A_1 = 20,\ A_2 = 15,\ A_3 = 12$ és $y_1 = -1,\ y_2 = -1,\ y_3 = -2,$ ami alapján $x = -1 \equiv 59 \pmod{60}$ vagyis $x = 59 + 60k\ (k \in \mathbb{Z})$.

A kongruenciarendszert kielégítő legkisebb *természetes* szám $x = 59$.

II. megoldás (rövidebb): Mivel a kongruenciarendszer *speciális* alakú:

$$x \equiv m_i - 1 \pmod{m_i} \qquad /m_1 = 2,\ m_2 = 3,\ m_3 = 4,\ m_4 = 5/ \quad ,$$

ezért a megoldás

$$x \equiv M - 1 \pmod{M} \qquad ahol \quad M = lkkt(m_1, ..., m_4) = 60 .$$

4.3.5.4) Emlékeztetünk arra, hogy több hasonló méretű szorzás elvégzéséhez az *előkészítő* számolásokat csak egyszer kell elvégeznünk, és utána a szorzások helyett csak összeadásokat kell végeznünk.

Továbbá érdemes mindenütt igyekezzünk legkisebb abszolút értékekkel (azaz negatív maradékokkal is) számolni.

(0) Előkészítés: Könnyen ellenőrizhető, hogy a megadott modulusok *páronként* relatív prímek. Ekkor

$$M = 253 \cdot 200 \cdot 261 \cdot 247 = 3\,262\,030\,200 ,$$

$(\sqrt{M} \approx 57114.186$, ez a szorzótényezők kb. max. mérete),

az $\boxed{y_i \cdot \frac{M}{m_i} \equiv 1 \pmod{m_i}}$ kongruenciák megoldásai:

$$y_1 = -18 , \quad y_1\tfrac{M}{m_1} = (-18) \cdot (3\,262\,030\,200/253) = -232\,081\,200 ,$$
$$y_2 = -49 , \quad y_2\tfrac{M}{m_2} = (-49) \cdot (3\,262\,030\,200/200) = -799\,197\,399 ,$$
$$y_3 = 17 , \quad y_3\tfrac{M}{m_3} = 17 \cdot (3\,262\,030\,200/261) = 212\,469\,400 ,$$
$$y_4 = 62 , \quad y_4\tfrac{M}{m_4} = 62 \cdot (3\,262\,030\,200/247) = 818\,809\,200 .$$

(1) A tényleges szorzások:

a) input: $X = 56079 , \quad Z = 58144 .$

(i) a párhuzamos számolások:

$$\begin{cases} x_1 :\equiv X \equiv 166 \pmod{m_1} \\ x_2 :\equiv X \equiv 79 \pmod{m_2} \\ x_3 :\equiv X \equiv -44 \pmod{m_3} \\ x_4 :\equiv X \equiv 10 \pmod{m_4} \end{cases} , \qquad \begin{cases} z_1 :\equiv Z \equiv -46 \pmod{m_1} \\ z_2 :\equiv Z \equiv -56 \pmod{m_2} \\ z_3 :\equiv Z \equiv -59 \pmod{m_3} \\ z_4 :\equiv Z \equiv 99 \pmod{m_4} \end{cases}$$

majd

$$\begin{cases} x_1 \cdot z_1 \equiv -46 \pmod{m_1} \\ x_2 \cdot z_1 \equiv -24 \pmod{m_2} \\ x_3 \cdot z_1 \equiv 36 \pmod{m_3} \\ x_4 \cdot z_1 \equiv 2 \pmod{m_4} \end{cases}$$

(ii) az összesítés:

$$\begin{aligned} X \cdot Z &= \sum_{i=1}^{t} y_i \frac{M}{m_i} \cdot x_i \cdot z_i = \\ &= (-232\,081\,200) \cdot (-46) + (-799\,197\,399) \cdot (-24) + 212\,469\,400 \cdot 36 \\ &\quad +818\,809\,200 \cdot 2 \\ &= 39\,142\,989\,576 \equiv 3\ 260\ 657\ 376 \pmod{M} \end{aligned}$$

Az eredmény jó, mert valóban $\mathbf{X \cdot Z = 3\ 260\ 657\ 376}$.

b) input: $X_2 = 49\ 745$, $Z_2 = 55846$.

(i) a párhuzamos számolások (töltse ki az üres helyeket!):

$$\begin{cases} x_1 \equiv X \equiv \pmod{\ } \\ x_2 \equiv X \equiv \pmod{\ } \\ x_3 \equiv X \equiv \pmod{\ } \\ x_4 \equiv X \equiv \pmod{\ } \end{cases} , \quad \begin{cases} z_1 \equiv Z \equiv \pmod{\ } \\ z_2 \equiv Z \equiv \pmod{\ } \\ z_3 \equiv Z \equiv \pmod{\ } \\ z_4 \equiv Z \equiv \pmod{\ } \end{cases}$$

majd

$$\begin{cases} x_1 \cdot z_1 \equiv \pmod{\ } \\ x_2 \cdot z_1 \equiv \pmod{\ } \\ x_3 \cdot z_1 \equiv \pmod{\ } \\ x_4 \cdot z_1 \equiv \pmod{\ } \end{cases}$$

(ii) az összesítés:

$$\begin{aligned} X \cdot Z &= \sum_{i=1}^{t} y_i \frac{M}{m_i} \cdot x_i \cdot z_i = \\ &= (-232\,081\,200) \cdot (\quad) + (-799\,197\,399) \cdot (\quad) \\ &\quad +212\,469\,400 \cdot (\quad) + 818\,809\,200 \cdot (\quad) \\ &\equiv \pmod{\quad} \end{aligned}$$

Ellenőrzés: $\mathbf{X \cdot Z =}$ ☐ OK ☐ nem OK .

4.3.5.5) b) A

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \tag{4.18}$$

kongruenciarendszer *általános* megoldása, *ha* a modulusok nem feltétlenül relatív prímek:

A kongruenciák definíciója miatt

$$x = m_1 \cdot \ell_1 + a_1 = m_2 \cdot \ell_2 + a_2 \quad ,$$

ezért az

$$m_1 \cdot \ell_1 - m_2 \cdot \ell_2 = a_2 - a_1 \tag{4.19}$$

lineáris Diophantikus egyenletet kell megoldanunk, és a (4.18) kongruenciarendszer *megoldhatóságának* szükséges és elégséges feltétele:

$$lnko(m_1, m_2) \mid a_2 - a_1 \quad .$$

Legyen $d := lnko(m_1, m_2)$, ekkor az (4.19) egyenlet általános megoldása

$$\ell_1 = \ell_1^{(0)} + \frac{lkkt(m_1, m_2)}{m_1} \cdot t \ , \quad \ell_2 = \ell_2^{(0)} + \frac{lkkt(m_1, m_2)}{m_2} \cdot t \quad (t \in \mathbb{Z}) \ ,$$

ahonnan (4.18) megoldása például:

$$x = m_1 \cdot \ell_1^{(0)} + lkkt(m_1, m_2) \cdot t + a_1 \qquad (t \in \mathbb{Z}) \ . \tag{4.20}$$

(vagy ami ugyanaz: $x = m_2 \cdot \ell_2^{(0)} + lkkt(m_1, m_2) \cdot t + a_2 \quad (t \in \mathbb{Z})$.)

Láthatjuk, hogy a megoldás $\pmod{M}$ egyértelmű, ahol

$$M := lkkt(m_1, m_2) \quad .$$

a) a (4.19) egyenlet most $6\ell_1 - 10\ell_2 = 7 - 3 = 4$,

aminek megoldása $\ell_1 = -1 + 5 \cdot t$, $\ell_2 = 1 + 3 \cdot t \quad (t \in \mathbb{Z})$.

Innen $x = -6 + 30t + 3 = 27 + 30t \quad (t \in \mathbb{Z})$, vagy másképpen

$x \equiv 27 \pmod{30}$.

4.3.5.6) b) A

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \end{cases} \tag{4.21}$$

kongruenciarendszer *általános* megoldása, *ha* a modulusok nem feltétlenül relatív prímek a következő:

A kongruenciák definíciója alapján a *kongruenciarendszer* ekvivalens az alábbi (lineáris Diophantikus) *egyenletrendszerrel*:

$$\begin{cases} x = m_1 \cdot \ell_1 + a_1 & (1) \\ x = m_2 \cdot \ell_2 + a_2 & (2) \\ x = m_3 \cdot \ell_3 + a_3 & (3) \end{cases}$$

valamilyen (megkeresendő) ℓ_1 , ℓ_2 , ℓ_3 , $x \in \mathbb{Z}$ egész számokra.

Az egyenleteket egymásból páronként kivonva kapjuk, hogy a megoldhatóság (egyik) *szükséges* feltétele:

$$lnko(m_i, m_j) \mid a_i - a_j \qquad (1 \leq i \neq j \leq 3) \; . \tag{4.22}$$

(Ez nyilván tetszőleges számú kongruenciát tartalmazó rendszerre egy szükséges feltétel.)

Az előző feladat (4.20) végeredménye alapján az (1) és (2) egyenletek megoldása

$$x = m_1 \cdot \ell_1^{(0)} + L_{1,2.} \cdot t + a_1 \qquad (t \in \mathbb{Z}) \; . \quad (4)$$

ahol

$$L_{1,2.} := lkkt(m_1, m_2)$$

és $\ell_1^{(0)}$ egyik gyöke az (1) és (2) egyenleteket tömörítő

$$m_1 \cdot \ell_1 - m_2 \cdot \ell_2 = a_2 - a_1 \tag{4.23}$$

egyenletnek (ld. (4.19) az előző feladatban).

Vagyis a (3) és (4) egyenletekből álló rendszert kell már csak megoldanunk (az ismeretlenek most: $x, \ell_3, t \in \mathbb{Z}$) :

$$\begin{cases} x = m_3 \cdot \ell_3 + a_3 & (3) \\ x = L_{1,2.} \cdot t + \left(m_1 \cdot \ell_1^{(0)} + a_1 \right) & (4) \end{cases}$$

A fenti egyenletrendszer megoldhatóságának *szükséges* feltétele (mint eddig):

$$lnko(m_3, L_{1,2.}) \mid a_3 - \left(m_1 \cdot \ell_1^{(0)} + a_1 \right) \quad , \tag{4.24}$$

és a megoldás (ismét a (4.20) végeredmény alapján):

$$x = m_3 \cdot \ell_3^{(L)} + lkkt\,(L_{1,2}, m_3) \cdot s + a_3 \qquad (s \in \mathbb{Z}) \tag{4.25}$$

ahol $\ell_3^{(L)}$ egyik megoldása az

$$m_3 \cdot \ell_3 - L_{1,2.} \cdot t = a_3 - \left(m_1 \cdot \ell_1^{(0)} + a_1 \right) \tag{4.26}$$

Diophantikus egyenletnek.

Érdemes még azt is észrevennünk, hogy

$$lkkt\,(L_{1,2}, m_3) = lkkt(m_1, m_2, m_3) \quad .$$

ÖSSZEGEZVE: A (4.21) kongruenciarendszer megoldhatóságának szükséges és elégséges feltétele (4.22) és (4.24), gyökeit (4.25) adja meg, amelyhez előbb meg kell oldanunk a (4.23) és (4.26) egyenleteket.

a) i) Az $\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 1 \pmod{10} \\ x \equiv 11 \pmod{15} \end{cases}$ egyenlet megoldása:

Először a (4.23) egyenletet kell megoldanunk:

$$6 \cdot \ell_1 - 10 \cdot \ell_2 = -4 \ , \qquad \begin{cases} \ell_1 = -4 - 5u \\ \ell_2 = -2 - 3u \end{cases} \quad (u \in \mathbb{Z}) \quad .$$

Ezután kapjuk a (4.26) egyenletet, megoldása:

$$15 \cdot \ell_3 - 30 \cdot t = 11 - (6 \cdot (-4) + 5) = 30 \ , \quad \begin{cases} \ell_3 = 2 - 2v \\ t \ = -v \end{cases} \quad (v \in \mathbb{Z}) \quad .$$

Tehát az i) kongruenciarendszer megoldása:

$$x = 15 \cdot 2 + 30s + 11 = 41 + 30s \qquad (s \in \mathbb{Z})$$

vagyis

$$x \equiv 11 \pmod{30} .$$

4.4. Polinomok

4.4.1) a)

$$(x^4 + x^2) : (x - 2) = x^3 + 2x^2 + 5x + 10$$
$$2x^3 + x^2$$
$$5x^2$$
$$10x$$
$$20$$

azaz $(x^4 + x^2) = (x - 2) \cdot (x^3 + 2x^2 + 5x + 10) + (20)$.

A felbontás a $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{C}[x]$ struktúrák mindegyikében igaz.

b) $(x^3 + 3x + 5) : (2x^2 - 7x + 9) = \frac{1}{2}x + \frac{7}{4}$, a maradék $\frac{43}{4}x - \frac{43}{4}$.

A maradékos osztás a $\mathbb{Z}[x]$ gyűrűben nem végezhető el, a többi polinomgyűrűben igen.

c) $(4x^5 + 5x - 2) : (2x^3 + 3) = 2x^2$
$-6x^2 + 5x - 2$

azaz $4x^5 + 5x - 2 = (2x^3 + 3) \cdot 2x^2 + (-6x^2 + 5x - 2)$, a felbontás mind a négy polinomgyűrűben igaz.

4.4.2) Legelőször is gyűjtsünk össze pár **általános ötlet**et polinomok felbontásával kapcsolatban.

i) Érdemes a felbontandó polinomnak egy gyökét keresni (vagy kitalálni), mert ezután Bézout tétele[14] és a maradékos osztás segítségével faktorizálni tudjuk a polinomot. □

ii) Az Algebra Alaptétele[15] szerint a valós (-együtthatójú) *irreducibilis* polinomok legfeljebb másodfokúak, míg a komplex (-együtthatójú) irreducibilis polinomok *csak* elsőfokúak lehetnek. □

iii) A fenti Tétel egyik következménye, hogy *páratlan fokú* valós polinomnak *mindig* van valós gyöke. □

(Gyökképlet ugyan nincs 4-nél magasabbfokú egyenletekre, de közelítő módszerek igen.)

iv) Ne feledjük azt sem, hogy: *egész* együtthatós polinom *egész* gyökei csak a konstans tag (azaz a_0) pozitív és negatív *osztói* lehetnek[16] ! □

v) *Másodfokú* valós polinom $ax^2 + bx + c \in \mathbb{R}[x]$ akkor és csak akkor reducibilis, ha diszkriminánsa nemnegatív: $D \geq 0$, és ekkor a felbontás

$$ax^2 + bx + c = a\,(x - x_1)\,(x - x_2)$$

a jólismert "gyöktényezős alak", ahol a a főegyüttható és x_1 , x_2 a polinom gyökei. Mégegyszer: $D < 0$ esetén a polinom irreducibilis $\mathbb{R}[x]$ -ben.

vi) Egyenlő együtthatók (vagy **együtthatók összehasonlítása**) módszere: ha a $p(x) = \sum_{i=0}^{n} a_i x^i$ polinomot

$$\sum_{i=0}^{n} a_i x^i = \left(\sum_{j=0}^{m} b_j x^j\right) \cdot \left(\sum_{k=0}^{\ell} c_k x^k\right)$$

alakban kívánjuk felbontani, akkor az a_i együtthatók alapján felírjuk az alábbi $n + 1$ (nemlineáris) egyenletet

$$a_i = \sum_{j=0}^{i} b_j c_{i-j} \qquad (0 \leq i \leq n)$$

---

[14] a maradék nélküli polinomosztás elvégezhetőségét Étienne Bézout (1730-1783) francia matematikus következő eredménye biztosítja:

Bézout Tétele: *Ha* $p(x) \in \Gamma[x]$ *egy tetszőleges* Γ *test feletti polinom, és* $\gamma \in \Gamma$ *gyöke a* $p(x)$ *polinomnak (azaz* $p(\gamma) = 0$*), akkor* $p(x)$ *osztható az* $(x-\gamma)$ **gyöktényezővel,** *azaz* $p(x) = (x - \gamma) \cdot q(x)$ *teljesül valamilyen* $q(x) \in \Gamma[x]$ *polinomra.* □

E tételnek speciális esete (ha $p(x)$ másodfokú) a középiskolában tanult "a másodfokú egyenlet gyöktényezős alakja ..." állítás.

[15] Az Algebra Alaptételét lásd a 4. *Gyűrűk* c. fejezet elején.

[16] persze egy egész együtthatós polinomnak nem biztos, hogy van *egész* gyöke!

a b_j és c_k ismeretlenekre, és *megpróbáljuk* megoldani. (Amire persze általános módszer nincs.)

Hasznunkra lehet még a következő összefüggés is:

vii) Tétel: *Ha* $p(x) \in \mathbb{R}[x]$ *tetszőleges* valós *együtthatós polinom, és* $\gamma \in \mathbb{C}$ *gyöke, akkor* $\bar{\gamma}$ *(komplex konjugált) is gyöke a* $p(x)$ *polinomnak.* $\square$

A **4.4.2) feladat megoldása:**

o) $x^2 - 1 = (x-1)(x+2)$ reducibilis a $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ struktúrák mindegyikében,

$x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$ felbontható (*reducibilis*) $\mathbb{R}[x]$ és $\mathbb{C}[x]$ -ben, de $\mathbb{Z}[x]$ és $\mathbb{Q}[x]$ -ben nem,

$x^2 + 1 = (x - i)(x + i)$ csak $\mathbb{C}[x]$ -ben reducibilis,

$x^3 - 1$ és $x^3 + 1$ páratlan fokúak, tehát *van* valós gyökük. Egész együtt hatósak, tehát a konstans együttható $a_0 = 1$ (ill. $a_0 = -1$) osztóit kell kipróbálnunk (bár így csak *egész* gyököket kereshetünk): mindkét esetben $x = +1$ és $x = -1$ jöhet szóba, és utána polinomosztás (Bézout tétele).

Vagy: a jólismert azonosságok alapján:

$$x^3 - 1 = (x-1)(x^2 + x + 1) \quad \text{és} \quad x^3 + 1 = (x+1)(x^2 - x + 1) \quad .$$

Mivel a fenti másodfokú polinomoknak nincs valós gyökük, ezért a fenti felbontások $\mathbb{C}[x]$ kivételével véglegesek (azaz a tényezők irreducibilisek).

$\mathbb{C}[x]$ -ben azonban gyökeiket könnyen megkereshetjük, így

$$x^3 - 1 = (x-1)(x-\rho)(x-\bar{\rho})$$

és

$$x^3 + 1 = (x+1)(x-\sigma)(x-\bar{\sigma})$$

ahol

$$\rho = -\frac{1}{2} + \frac{1}{2}i\sqrt{3} \quad \text{és} \quad \sigma = \frac{1}{2} - \frac{1}{2}i\sqrt{3}$$

és $\bar{\rho}$ ill. $\bar{\sigma}$ a komplex konjugáltat jelenti.

A jólismert azonosságok alapján

$$x^4 - 1 = (x-1)(x+1)(x^2+1) \ .$$

A fenti számolások alapján ez $\mathbb{C}[x]$ kivételével irreducibilis tényezőkre való felbontás, míg $\mathbb{C}[x]$ -ben (szintén a fentiek szerint)

$$x^4 - 1 = (x-1)(x+1)(x-i)(x+i) \ .$$

x^4+1 reducibilis az *Algebra Alaptétele* szerint mind $\mathbb{R}[x]$ mind $\mathbb{C}[x]$ -ben. Mivel gyöke nincs, ezért próbálkozzunk

$$x^4 + 1 = \left(x^2 + ax + b\right)\left(x^2 + cx + d\right)$$

alakú felbontással, ahonnan az együtthatók összehasonlítása alapján az

$$\begin{aligned} x^4 &: \quad 1 = 1 \ , \\ x^3 &: \quad 0 = c + a \ , \\ x^2 &: \quad 0 = d + ac + b \ , \\ x &: \quad 0 = ad + bc \ , \\ 1 &: \quad 1 = bd \end{aligned}$$

egyenletrendszert kapjuk. Ennek megoldása az

$$x^4 + 1 = \left(x^2 - x\sqrt{2} + 1\right)\left(x^2 + x\sqrt{2} + 1\right) \tag{4.27}$$

felbontást adja, amely tényezők $\mathbb{R}[x]$ -ben irreducibilisek.

A fenti számolás azt is mutatja, hogy az x^4+1 polinom a $\mathbb{Z}[x]$ és $\mathbb{Q}[x]$ struktúrákban *irreducibilis*.

A (4.27) egyenlet alapján könnyen megtaláljuk a $\mathbb{C}[x]$ -beli felbontást is (HF).

Másik megoldás: Megkereshetjük az

$$x^4 + 1 = 0$$

egyenlet *összes komplex gyökét*: -1 -ből kell negyedik gyököt vonnunk*:*

$$x_k = \cos\left(\frac{180^o}{4} + (k-1)\cdot\frac{360^o}{4}\right) + i\sin\left(\frac{180^o}{4} + (k-1)\cdot\frac{360^o}{4}\right)$$
$$(k = 1, 2, 3, 4)$$

ahonnan azonnal megkapjuk a $\mathbb{C}[x]$ -beli felbontást:

$$x^4 + 1 = (x - x_1)(x - x_2)(x - x_3)(x - x_4) \ .$$

Használjuk most a vii) tételt: mivel a a négy gyök párosával egymás konjugáltja:

$$x_3 = \bar{x}_2 \quad \text{és} \quad x_4 = \bar{x}_1 \ ,$$

ezért az

$$(x - x_2)(x - x_3) = x^2 + x\sqrt{2} + 1$$

és az

$$(x - x_1)(x - x_4) = x^2 - x\sqrt{2} + 1$$

valós együtthatójú polinomok irreducibilis tényezői az x^4+1 polinomnak $\mathbb{R}[x]$ -ben.

4.4.2) a) $x^2 - 3x + 1$ gyökei $x_{1,2} = \frac{3}{2} \pm \frac{1}{2}\sqrt{5}$, vagyis felbonthatatlan (irreducibilis) $\mathbb{Z}[x]$ és $\mathbb{Q}[x]$ -ben, míg $\mathbb{R}[x]$ és $\mathbb{C}[x]$ -ben felbontható (reducibilis):

$$x^2 - 3x + 1 = \left(x - \left(\tfrac{3}{2} + \tfrac{1}{2}\sqrt{5}\right)\right) \cdot \left(x - \left(\tfrac{3}{2} - \tfrac{1}{2}\sqrt{5}\right)\right) \ .$$

Az $x^2 + 5x + 7$ polinom diszkriminánsa negatív, tehát $\mathbb{R}[x]$ -ben is irreducibilis, míg $\mathbb{C}[x]$ -ben természetesen felbontható:

$$x^2 + 5x + 7 = \left(x - \left(-\tfrac{5}{2} + \tfrac{1}{2}i\sqrt{3}\right)\right) \cdot \left(x - \left(-\tfrac{5}{2} - \tfrac{1}{2}i\sqrt{3}\right)\right) \ .$$

4.4.2) b) **A** $2x^3 - 5x^2 + 3x - 2$ polinom felbontása:

Mivel harmadfokú, ezért $\mathbb{R}[x]$ -ben biztosan van gyöke.
A polinom egész együtthatós, ezért nézzük meg először: van-e *egész* gyöke! A konstans tag $a_0 = 2$, aminek osztóit (+1, -1, +2 és -2) kipróbálva kapjuk az $x = 2$ gyököt. Ezután Bézout tétele alapján az $(x - 2)$ gyöktényezővel osztjuk a $p(x)$ polinomot:

$$\begin{array}{l} (2x^3 - 5x^2 + 3x - 2) : (x - 2) = 2x^2 - x + 1 \\ \quad -x^2 + 3x - 2 \\ \qquad\quad x - 2 \\ \qquad\quad\ \ 0 \end{array}$$

(Nem meglepő az $r(x) = 0$ maradék, hiszen Bézout tétele éppen ezt mondja ki!)

Ekkor tehát

$$\left(2x^3 - 5x^2 + 3x - 2\right) = (x-2) \cdot \left(2x^2 - x + 1\right) \quad . \tag{4.28}$$

Mivel most a másodfokú $2x^2 - x + 1$ polinomot kell szorzattá bontanunk, használhatjuk a gyökképletet és a polinom gyöktényezős alakját[17]:

$$x_{1,2} = \frac{1 \pm \sqrt{1 - 4 \cdot 2}}{4} = \frac{1}{4} \pm \frac{\sqrt{7}}{4} i \quad \notin \mathbb{R} \quad .$$

Ez azt jelenti, hogy az $2x^2 - x + 1$ polinom irreducibilis.

Tehát (4.28) mutatja a végleges felbontást $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ és $\mathbb{R}[x]$ -ben, míg $\mathbb{C}[x]$ -ben

$$\left(2x^3 - 5x^2 + 3x - 2\right) = (x-2) \cdot \left(x - (\frac{1}{4} + \frac{\sqrt{7}}{4} i)\right) \cdot \left(x - (\frac{1}{4} - \frac{\sqrt{7}}{4} i)\right) \quad .$$

A $2x^3 - x^2 - 1$ polinomot hasonlóan bonthatjuk fel $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ és $\mathbb{R}[x]$ -ben:

$$2x^3 - x^2 - 1 = (x-1) \cdot \left(2x^2 + x + 1\right) \ ,$$

illetve $\mathbb{C}[x]$ -ben:

$$2x^3 - x^2 - 1 = (x-1) \cdot \left(x - \left(-\frac{1}{4} + \frac{1}{4} i\sqrt{7}\right)\right) \cdot \left(x - \left(-\frac{1}{4} - \frac{1}{4} i\sqrt{7}\right)\right) \quad .$$

4.4.2) c) Az $x^4 + 2x^3 + 2x^2 + 2x - 1 = 0$ negyedfokú egyenlet gyökei[18]

[17] **Állítás:** *Ha a $p(x) \in \Gamma[x]$ polinom n-fokú, és van n db (nem feltétlenül különböző) gyöke: $x_1, ..., x_n \in \Gamma$, akkor*

$$p(x) = a_n \cdot (x - x_1) \cdot ... \cdot (x - x_n) \tag{4.29}$$

ahol $a_n \in \Gamma$ a $p(x)$ polinom **főegyütthatója** *(legmagasabb fokú tag együtthatója) .* □

A (4.29) szorzatot hívjuk $p(x)$ **gyöktényezős alak**jának.

(Az Állítás Bézout tételének egyszerű következménye.)

[18] A harmad- és negyedfokú egyenletek (egzakt [pontos]) megoldóképletei megtalálhatók bármely matematikai lexikonban, mérnöki kézikönyvben "*Cardano formula*" címszó alatt (bár a képletet Tartaglia fedezte fel). Továbbá, legtöbb szimbolikus matematikai program (pl. Derive, Maple, Mathematica,...) is ismeri.

$$x_1 = \sqrt{\sqrt{\alpha} + \beta} - \sqrt{\gamma} - \frac{1}{2} \tag{4.30}$$

ahol

$$\alpha = \sqrt[3]{\frac{371}{93312} - \frac{11\cdot\sqrt{69}}{31104}} + \sqrt[3]{\frac{371}{93312} + \frac{11\cdot\sqrt{69}}{31104}} - \sqrt[3]{\frac{\sqrt{69}}{3888} - \frac{11}{11664}} + \sqrt[3]{\frac{\sqrt{69}}{3888} + \frac{11}{11664}} +$$
$$+ \sqrt[3]{\frac{371}{3456} - \frac{11\cdot\sqrt{69}}{1152}} + \sqrt[3]{\frac{371}{3456} + \frac{11\cdot\sqrt{69}}{1152}} + \frac{7}{12} \ ,$$

$$\beta = \frac{\sqrt[3]{\frac{3\cdot\sqrt{69}}{2} - \frac{11}{2}} - \sqrt[3]{\frac{3\cdot\sqrt{69}}{2} + \frac{11}{2}} - 1}{6} \ ,$$

$$\gamma = -\sqrt[3]{\frac{\sqrt{69}}{144} - \frac{11}{432}} + \sqrt[3]{\frac{\sqrt{69}}{144} + \frac{11}{432}} - \frac{1}{12}$$

a többi gyököt nem részletezzük, közelítőleg

$x_1 \approx 0.339\,246$,
$x_2 \approx -1.712\,984$,
$x_{3,4} \approx -0.313\,130 \pm 1.273\,873 \cdot i$

tehát $p(x)$ felbontása $\mathbb{C}[x]$ -ben:

$$p(x) = (x - x_1) \cdot (x - x_2) \cdot (x - x_3) \cdot (x - x_4)$$

alapján

$$p(x) \approx (x - 0.339)\,(x + 1.713)\,(x + 0.313 - 1.274i)\,(x + 0.313 + 1.274i)$$

Észrevehetjük, hogy mivel $p(x) \in \mathbb{R}[x]$ valós együtthatós polinom, ezért minden komplex gyök konjugáltja is gyöke a polinomnak: $x_4 = \overline{x_3}$. így az

$$(x - x_3)(x - x_4) \approx x^2 + 0.626261 \cdot x + 1.720804$$

másodfokú polinom irreducibilis tényezője $p(x)$ -nek.

így $p(x)$ felbontása $\mathbb{R}[x]$ -ben:

$$p(x) \approx (x - 0.3392) \cdot (x + 1.7130) \cdot \left(x^2 + 0.6263 \cdot x + 1.7208\right) \quad . \tag{4.31}$$

Polinomunk $\mathbb{Z}[x]$ és $\mathbb{Q}[x]$ -beli felbontása attól függnek, hogy a fenti (4.31) kifejezésben mik az együtthatók *pontos* értékei[19]: mindegyikük egész ill. racionális, vagy van közöttük (akár csak egy is) irracionális. Mivel ezt a

[19] esetleg szóbajöhet még az $(x - 0.3392) \cdot (x + 1.7130)$ szorzótényező is,

gyökök (4.30) alatti és hasonló pontos értékei döntik el - a számításokat most nem részletezzük.

Másik megoldás: *A fentiek alapján* az $x^4 + 2x^3 + 2x^2 + 2x - 1$ polinom $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ ill. $\mathbb{R}[x]$ -beli felbontásai

$$x^4 + 2x^3 + 2x^2 + 2x - 1 = (x - A)(x - B)(x^2 + Cx + D) \tag{4.32}$$

VAGY

$$x^4 + 2x^3 + 2x^2 + 2x - 1 = (x^2 + Ax + B)(x^2 + Cx + D) \tag{4.33}$$

alakú lehet valamely

$$A, B, C, D \in \Gamma$$

számokra (itt Γ a $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ halmazok valamelyikét jelöli, a feladattól függően).

Az együtthatók összehasonlításai alapján (4.32)-ből az

$$\begin{cases} 2 = C - A - B \\ 2 = -BC + AB + D - AC \\ 2 = -AD - BD + ABC \\ -1 = ABD \end{cases}$$

míg (4.33)-ből az

$$\begin{cases} 2 = C + A \\ 2 = D + AC + B \\ 2 = AD + BC \\ -1 = BD \end{cases}$$

nemlineáris egyenletrendszert kapjuk. Ennek megoldására automatikus módszerünk nincs: vagy meg tudjuk oldani, vagy nem.

4.4.2) d) $p(x) = x^5 - 2x^4 + 13x^3 - 18x^2 + 22x - 12$

A gyökképletek elméletéből [20)] tudjuk, hogy ötödfokú egyenletekre *nem lehet* gyökképlet (algoritmus). A konstans tag (= 12) egész osztói között

[20)] másodfokú (algebrai) egyenletekre a tanult gyökképlet (már 4000 évvel ezelőtt Mezopotámiában is ismerték), harmad- és negyedfokú egyenletekre *Girolamo Cardano* (1501-1576), *Nicolo Tartaglia* (1500-1557) és *Ludovico Ferrari* (1522-1565) olasz tudósok képletei adnak megoldást. Ötöd- és magasabbfokú egyenletekre *Niels Henrik Abel* (1802-1829) norvég és *Paolo Ruffini* (1765-1822) olasz matematikusok bizonyították, hogy *nincs* általános gyökképlet, az eredeti bizonyítás hibáját *Bolyai János* (1802-1860) is kijavította (**Abel-Ruffini-Bolyai János Tétel**).

sem találunk gyököt. Azonban könnyen találunk különböző előjelű értéket adó pontokat $\mathbb{R}$ -ben[21]: $p(0) < 0$ és $p(1) > 0$, így a $[0,1]$ intervallumban gyorsan kiszámolhatjuk a p polinom *egyik* gyökének[22] *közelítő* értékét. Legegyszerűbb az *intervallumfelezéses* módszer[23][24], a gyök közelítő értéke:

$$x_1 \approx 0.784\,674 \ ,$$

így polinomosztással:

$$\begin{aligned}
&(x^5 - 2x^4 + 13x^3 - 18x^2 + 22x - 12) : (x - 0.785) \approx \\
&\qquad\qquad \approx x^4 - 1.215x^3 + 12.046x^2 - 8.548x + 15.293 \\
&-1.215x^4 + 13x^3 - 18x^2 + 22x - 12 \\
&\quad 12.046x^3 - 18x^2 + 22x - 12 \\
&\qquad -8.548x^2 + 22x - 12 \\
&\qquad\quad 15.293x - 12
\end{aligned}$$

vagyis már csak a 4-edfokú

$$q(x) = x^4 - 1.215x^3 + 12.046x^2 - 8.548x + 15.293$$

polinomot kell faktorizálnunk, mint az előző feladatban.

Ez utóbbi polinom gyökei

---

[21] Páratlan fokú polinomoknál ez mindig sikerül (miért?) .

[22] **Darboux tétele:** *Ha $f(x)$ folytonos az $[a,b]$ intervallumon és f különböző előjelű értékeket vesz fel az $[a,b]$ intervallum végpontjaiban* (*azaz $f(a)\cdot f(b) < 0$*), *akkor a f -nek* van *gyöke az $[a,b]$ intervallumban.* □ (Gaston Darboux francia matematikus, 1842-1917)

[23] Egyenletek gyökeinek **közelítő módszereit** (*intervallumfelezés, húrmódszer [regula falsi], stb.*) bármely matematikai lexikonban, mérnöki kézikönyvben megtalálhatjuk, esetleg **Urbán J.:** *Határértékszámítás* (Bolyai-könyvek sorozat, Műszaki Kiadó) c. könyvének 300.oldalán; illetve a legtöbb szimbolikus matematikai program (pl. Derive, Maple, Mathematica) is ismeri és kiszámítja a módszert.

[24] Az $f(x) = 0$ **(*)** alakú egyenletek (ahol f folytonos) egy gyökének *közelítő* meg keresésére a legegyszerűbb (de mégis exponenciálisan gyors) megoldása az *intervallum felezés*: Tegyük fel, hogy $f(a)$ és $f(b)$ különböző előjelűek, ekkor (*)-nak *van* gyöke az $[a,b]$ intervallumban. Legyen $x_0 := a$, $x_1 := b$ és $x_2 := (x_0 + x_1)/2$ az $[x_0, x_1]$ intervallum felezőpontja. $f(x_2)$ előjelének vizsgálatával kiválaszthatjuk kiválaszthatjuk az $[x_0, x_2]$ és $[x_2, x_1]$ intervallumok közül azt, amelyben a keresett gyök van. Ezt a lépést ismételgetjük: $x_{n+1} := (x_{n-1} + x_n)/2$ és $f(x_{n+1})$ előjelének vizsgálata.

n lépés után, ha (*) gyökét x_{n+1} -el közelítjük, a hiba kisebb mint $|a-b|/2^n$, azaz kb. minden $3-4$ lépés után kapunk egy újabb tizedesjegyet.

$$x_{1,2} \approx 0.221\,192 \pm 3.\,186\,974 \cdot i \ ,$$
$$x_{3,4} \approx 0.386\,307 \pm 1.161\,567 \cdot i \ ,$$

ami alapján $\mathbb{C}[x]$ -ben:

$$\begin{aligned} p(x) \ \approx \ & (x - 0.785) \cdot (x - (0.221\,1 + 3.\,186\,9i)) \cdot (x - (0.221\,1 - 3.\,186\,9i)) \cdot \\ & \cdot (x - (0.3863 + 1.1615i)) \cdot (x - (0.3863 - 1.1615i)) \end{aligned}$$

míg $\mathbb{R}[x]$ -ben (a konjugált-gyökpárokat összeszorozva)

$$p(x) \approx (x - 0.785) \cdot \left(x^2 - 0.4422x + 10.2052\right) \cdot \left(x^2 - 0.772\,6x + 1.4983\right) \quad .$$

4.4.3) A felbontandó szám $10^{15}+1$, ezért próbálkozzunk az $x^{15}+1$ polinom felbontásával (és majd utána helyettesítsük az $x = 10$ értéket):

$$\begin{aligned} x^{15} + 1 \ &= \ \left(x^5\right)^3 + 1 = \left(x^5 + 1\right)\left((x^5)^2 - x^5 + 1\right) = \\ &= \ (x + 1)\left(x^4 - x^3 + x^2 - x + 1\right)\left(x^{10} - x^5 + 1\right) \\ &= \ (x + 1)\left(x^4 - x^3 + x^2 - x + 1\right) \cdot \\ &\quad \cdot \left(x^2 - x + 1\right)\left(x^8 + x^7 - x^5 - x^4 - x^3 + x + 1\right) \end{aligned}$$

Az első két lépés a középiskolában tanult egyik azonosság:

$$a^{2k+1} + 1 = (a + 1)\left(a^{2k} - a^{2k-1} + a^{2k-2} - +... + 1\right) \quad ,$$

majd az

$$x^{10} - x^5 + 1 = 0 \tag{4.34}$$

egyenlet komplex gyökeit kiszámolva észrevehetjük, hogy minden $\gamma \in \mathbb{C}$ gyök $\overline{\gamma}$ konjugáltja is gyöke az egyenletnek. Ekkor az

$$(x - \gamma) \cdot (x - \overline{\gamma})$$

alakú szorzatok megadják az (4.34) polinom *valós együtthatójú* felbontását. Ezek közül párat összeszorozgatva (próbálkozva) kaphatjuk meg a

$$x^{10} - x^5 + 1 = \left(x^2 - x + 1\right)\left(x^8 + x^7 - x^5 - x^4 - x^3 + x + 1\right)$$

felbontást[25)].

x helyére 10 -et írva kapjuk az adott szám egy kezdeti felbontását:

$$\begin{aligned} 10^{15}+1 &= 11\cdot(10^4-10^3+10^2-10+1)\cdot(10^2-10+1)\cdot \\ &\quad \cdot(10^8-10^7+10^5-10^4-10^3+10+1) \\ &= 11\cdot 9091\cdot 91\cdot 90089011 \end{aligned}$$

Mivel a tényezők nem mind prímszámok,ezért tovább kell őket faktorizálni. Ez (ha nincs jobb módszerünk) már történhet a szokásos "*osztogatásos*" algoritmussal[26)], de vegyük észre: a fenti polinomos módszerrel 16 jegyű szám helyett már csak egy 8 jegyű számot kell felbontanunk. Ha figyelembe vesszük, hogy az "osztogatós" módszer exponenciálisan lassú, akkor kb. 10^{16} lépés helyett már csak 10^8 lépésre van szükségünk !!!

A végeredmény: 9091 prímszám, $91 = 7\cdot 13$ és 90089011 prímszám, vagyis

$$10^{15}+1 = 11\cdot 9091\cdot 91\cdot 90089011 \quad .$$

4.4.4) a) I. Megoldás: A polinomot tulajdonképpen "$(x-2)$ *alapú számrendszerben*" kell felírnunk, így maradékos osztogatással[27)] is megkaphatjuk az együtthatókat:

$$\begin{aligned} p_0(x) = x^3-2x^2+2x-1 &= (x-2)\cdot(x^2+2)+3\ , \\ (x^2+2) &= (x-2)\cdot(x+2)+6\ , \\ x+2 &= (x-2)\cdot 1+4\ , \end{aligned}$$

Tehát a megoldás:

$$\begin{aligned} p(x) &= (x-2)\cdot[(x-2)\cdot((x-2)\cdot 1+4)+6]+3 = \\ &= (x-2)^3+4\cdot(x-2)^2+6\cdot(x-2)+3\ . \end{aligned}$$

II. Megoldás: Taylor polinomot kell keresnünk $a=2$ pont körül, így:

$p(x) = x^3-2x^2+2x-1\ , \quad p(2)=3\ ,$

[25)] Az utolsó átalakítást a körosztási polinomok elméletének ismeretélben rövidebben is elvégezhetjük.

[26)] vagy használhatjuk a könyv végén levő prímtáblázatot is,

[27)] ez lényegében a Horner elrendezés

$p'(x) = 3x^2 - 4x + 2$, $\qquad p'(2) = 6$,

$p"(x) = 6x - 4$, $\qquad p"(2) = 8$,

$p^{(3)}(x) = 6$, $\qquad p^{(3)}(2) = 6$,

Tehát a megoldás ismét (a jól ismert Taylor formula szerint):

$p(x) = 3 + \frac{6}{1}(x-2) + \frac{8}{2}(x-2)^2 + \frac{6}{6}(x-2)^3$.

III. Megoldás: Használjunk elemi bázistranszformációt:

a $p(x) = x^3 - 2x^2 + 2x - 1$ polinom koordinátáit kell kiszámolnunk az

$$\left\{1, (x-2), (x-2)^2, (x-2)^3\right\}$$

bázisra vonatkozóan. Az induló táblázat:

	1	$x-2$	$(x-2)^2$	$(x-2)^3$	$p(x)$
x^3	0			1	1
x^2	0		1	-6	-2
x	0	1	-4	12	2
1	1	-2	4	8	-1

.

b) $x^4 + x^2 = 20 + 36\,(x-2) + 25\,(x-2)^2 + 8\,(x-2)^3 + (x-2)^4$.

4.4.5) Vegyük észre, hogy $x^2 + 2x + 1 = (x+1)^2$,
így a binomiális tétel szerint

$$\begin{aligned} x^{2001} &= ((x+1)-1)^{2001} = \\ &= \sum_{k=2}^{2001} \binom{2001}{k} (x+1)^k (-1)^{2001-k} + \binom{2001}{1}(x+1) + (-1)^{2001} \equiv \\ &\equiv 2001\,(x+1) + (-1) = 2001x + 2000 \qquad (\mathrm{mod}\ (x+1)^2)\ . \end{aligned}$$

4.4.6) a) I. Megoldás: Az Euklideszi algoritmus alapján:

$$\begin{aligned} \left(x^3 + 2x^2 - 2x + 1\right) &= \left(x^2 - x - 2\right) \cdot (x+3) + (3x+7) \\ \left(x^2 - x - 2\right) &= (3x+7) \cdot \left(\tfrac{1}{3}x - \tfrac{10}{9}\right) + \tfrac{52}{9} \\ (3x+7) &= \tfrac{52}{9} \cdot \left(\tfrac{27}{52}x + \tfrac{63}{52}\right) + 0 \end{aligned}$$

amiből

$$lnko\,(p(x), q(x)) = \tfrac{52}{9} \sim 1 \ .$$

Mivel az eredmény asszociált 1-hez, ezért a két polinom *relatív prím* egymáshoz (mind a négy polinomgyűrűben).

II. Megoldás: A két polinom gyökeit (közelítő értékeiket) megkeresve a polinomokat tényezőkre bonthatjuk:

$$x^3+2x^2-2x+1 = (x + 2.8312)\,(x - 0.4156 - 0.4248i)\,(x - 0.4156 + 0.4248i)$$

és

$$x^2 - x - 2 = (x + 1)(x - 2)$$

ahonnan szintén látszik, hogy a két polinom mind a négy polinomgyűrűben *relatív prím* egymáshoz.

b) $f(x) = x^4 + 3x^3 - x^2 - 4x - 3$ és $g(x) = 3x^3 + 10x^2 + 2x - 3$ legnagyobb közös osztója az Euklideszi algoritmussal:

Az első osztás:

$$\begin{array}{l}(x^4 + 3x^3 - x^2 - 4x - 3) : (3x^3 + 10x^2 + 2x - 3) = \left(\tfrac{x}{3} - \tfrac{1}{9}\right) \\ \quad -x^3/3 - 5/3 \cdot x^2 - 3x - 3 \\ \qquad\qquad -5/9 \cdot x^2 - 25/9 \cdot x - 30/9\end{array}$$

azaz

$$\boxed{(x^4+3x^3-x^2-4x-3)=(3x^3+10x^2+2x-3)\left(\tfrac{x}{3}-\tfrac{1}{9}\right)+\left(\tfrac{-5}{9}x^2-\tfrac{25}{9}x-\tfrac{30}{9}\right),}$$

a második osztás

$$\begin{array}{l}(3x^3 + 10x^2 + 2x - 3) : (-5/9 \cdot x^2 - 25/9 \cdot x - 30/9) = -27/5 \cdot x + 9 \\ \quad -5x^2 - 16x - 3 \\ \qquad\quad 9x + 27\end{array}$$

azaz

$$\boxed{(3x^3 + 10x^2 + 2x - 3) = \left(\tfrac{-5}{9}x^2 - \tfrac{25}{9}x - \tfrac{30}{9}\right)\left(\tfrac{-27}{5}x + 9\right) + (9x + 27)\ ,}$$

a harmadik osztás:

$$\tfrac{-5}{9}(x^2 + 5x + 6) = (9(x + 3)) \cdot \left(\tfrac{-5}{81}(x + 2)\right) + 0 \quad .$$

Tehát

$$lnko(f(x), g(x)) = c \cdot (x + 3) \qquad (c \in \mathbb{R}) \quad .$$

4.4.7) Alkalmazzuk az Euklideszi algoritmust
(a maradék polinomokat [ ] jelöli):

$$\begin{aligned}
\left[x^3-x^2+3x-10\right] &= \left[x^3+6x^2-9x-14\right]\cdot 1+\left[-7x^2+12x+4\right] \ , \\
\left[x^3+6x^2-9x-14\right] &= \left[-7x^2+12x+4\right]\cdot\left(\frac{-x}{7}-\frac{54}{49}\right)+\left[\frac{235}{49}(x-2)\right] \ , \\
\left[-7x^2+12x+4\right] &= \left[\frac{235}{49}(x-2)\right]\cdot\left(\frac{-49}{235}\,(7x+2)\right)+0
\end{aligned}$$

vagyis

$$lnko\,(f(x),g(x)) = c\,(x-2) \qquad (c\in\mathbb{R}) \quad .$$

Visszafejtve kapjuk:

$$\begin{aligned}
&lnko\,(f(x),g(x)) = (x-2) = \\
&= \tfrac{49}{235}\left(\left[x^3+6x^2-9x-14\right]-\left[-7x^2+12x+4\right]\left(\tfrac{-x}{7}-\tfrac{54}{49}\right)\right) = \\
&= \tfrac{49}{235}\left[x^3+6x^2-9x-14\right]-\tfrac{49}{235}\left(\tfrac{-x}{7}-\tfrac{54}{49}\right)\left[-7x^2+12x+4\right] = \\
&= \tfrac{49}{235}\left[x^3+6x^2-9x-14\right]- \\
&\quad -\tfrac{49}{235}\left(\tfrac{-x}{7}-\tfrac{54}{49}\right)\left(\left[x^3-x^2+3x-10\right]-\left[x^3+6x^2-9x-14\right]\right) = \\
&= \left(\tfrac{49}{235}+\tfrac{49}{235}\left(\tfrac{-x}{7}-\tfrac{54}{49}\right)\right)\left[x^3+6x^2-9x-14\right]- \\
&\quad -\tfrac{49}{235}\left(\tfrac{-x}{7}-\tfrac{54}{49}\right)\left[x^3-x^2+3x-10\right]
\end{aligned}$$

vagyis

$$u(x) \;=\; -\frac{49}{235}\left(\frac{-x}{7}-\frac{54}{49}\right) \;=\; \frac{7}{235}x+\frac{54}{235}$$

és

$$v(x) \;=\; \left(\frac{49}{235}+\frac{49}{235}\left(\frac{-x}{7}-\frac{54}{49}\right)\right) \;=\; \frac{-7}{235}x-\frac{5}{235} \quad .$$

4.4.8) Az alábbi összefüggések alapján többféle megoldási módszer közül választhatunk:

i) Definíció: *A $\gamma\in\Gamma$ szám k* **-szoros gyöke** *a $p(x)\in\Gamma[x]$ polinomnak, ha $p(x)$ osztható az $(x-\gamma)^k$ polinommal, de nem osztható $(x-\gamma)^{k+1}$-el.* □

ii) Tétel: *A $\gamma\in\Gamma$ szám pontosan akkor k -szoros gyöke a $p(x)\in\Gamma[x]$ polinomnak, ha $p^{(i)}(\gamma)=0$ (deriváltak) minden $i=0,1,...,k-1$ esetén de $p^{(k)}(\gamma)\neq 0$.* □

a) Mivel $f(x_0) = 0$ és $f'(x_0) \neq 0$, ezért x_0 csak 1 -szeres gyöke $f(x)$ -nek.

Másik megoldás: az $f(x)$ polinomot megpróbáljuk többször elosztani az $x - x_o$ polinommal:
első osztás:

$$(x^3 + 3x^2 + 2x - 6) : (x - 1) = x^2 + 4x + 6 \ ,$$
$$4x^2 + 2x - 6$$
$$6x - 6$$
$$0$$

második osztás:

$$(x^2 + 4x + 6) : (x - 1) = x + 5 \ .$$
$$5x + 6$$
$$11$$

Mivel a legutolsó maradék $\neq 0$, ezért $f(x)$ nem osztható $(x-1)^2$ -el, csak $(x - 1)$ -el, vagyis az $x = 1$ szám egyszeres gyöke az $f(x)$ polinomnak.

b) $f(-2) = f'(-2) = 0$ és $f''(-2) \neq 0$, ezért $x_1 = -2$ pontosan 2 -szeres gyöke $g(x)$ -nek.

4.4.9) a) Az $a(x)$ polinomnak könnyen láthatóan van gyöke: $x = 1$. Az előző feladathoz hasonlóan: $a'(1) = 0$ miatt ellenőrizhetjük, hogy $x = 1$ (legalább) *kétszeres* gyöke $a(x)$ -nek, vagyis $a(x)$ osztható $(x-1)^2$ -el. Tehát az $a(x)$ polinom *nem* négyzetmentes.

b) $b(x)$ -nek nincs gyöke, így a következő eredményt kell használnunk:

Tétel: *Egy tetszőleges* $p(x) \in \Gamma[x]$ *polinom pontosan akkor négyzetmentes, ha*

$$lnko(\ p(x)\ ,\ p\prime(x)\ ) = 1 \ . \quad \square$$

Tehát (az Euklideszi algoritmust használva):

$$b(x) = x^4 + x^3 + 4x^2 + x + 3 \ ,$$

$$b'(x) = 4x^3 + 3x^2 + 8x + 1 \ ,$$

az első osztás: ([ ]-ben a maradékokat jelöltük):

$$(x^4 + x^3 + 4x^2 + x + 3) : (4x^3 + 3x^2 + 8x + 1) = 0.25x + 0.0625 \ ,$$
$$0.25x^3 + 2x^2 + 0.75x + 3$$

$$[1.813x^2 + 0.250x + 2.938]$$

a második osztás:

$$(4x^3 + 3x^2 + 8x + 1) : (1.813x^2 + 0.250x + 2.938) = 2.206x + 1.350 \ ,$$
$$2.448x^2 + 1.518x + 1.000$$
$$[1.180x - 2.968]$$

a harmadik osztás:

$$(1.813x^2 + 0.250x + 2.938) : (1.180x - 2.968) = 1.536x + 4.076 \ .$$
$$4.810x + 2.938$$
$$[15.037]$$

Mivel a maradék nem 0 , így a b és b' polinomok relatív prímek. Ez pedig azt jelenti, hogy a $b(x)$ polinom *négyzetmentes.*

c) $lnko\,(c(x), c\prime(x)) = (x^2 + 3)$, vagyis $(x^2 + 3)^2 \mid c(x)$, vagyis a $c(x)$ polinom *nem* négyzetmentes.

(Egyébként $a(x) = (x - 1)^2(x + 1)$, $b(x) = (x^2 + 1)(x^2 + x + 3)$, $c(x) = (x^2 + 3)^2(x^2 + 2x + 5)$.)

4.4.10) Egy polinom gyökei egyszeresek pontosan akkor, ha négyzetmentes, azaz $lnko(p, p') \approx 1$. A $p(x) = ax^2 + bx + c$ polinomot deriváltjával maradékosan elosztva kapjuk

$$\left(ax^2 + bx + c\right) = (2ax + b) = \left(\frac{1}{2}x + \frac{b}{4a}\right) \cdot \left(c - \frac{b^2}{4a}\right)$$

ahonnan

$$lnko(p, p') = c - \frac{b^2}{4a}$$

hiszen p' elsőfokú. Vagyis a gyökök egyszerességének kritériuma a jólismert

$$\frac{-1}{4a} D \ = \ \frac{-1}{4a} \left(b^2 - 4ac\right) \ \neq \ 0$$

feltétel.

4.4.11) Érdemes először megnézni, hogy a polinomnak van-e gyöke a kérdéses halmazban, valamint a Feladatgyűjtemény végén levő irreducibilis polinomok táblázatát is használhatjuk.

o) $o_1(x) = x^2 + 1 \equiv (x + 1)^2 \pmod 2$,

$o_2(x) = x^2 + x + 1$ végigpróbálgatás után: irreducibilis $\mathbb{Z}_2[x]$ -ben,

a) $a(x) = x^7 - 1 \equiv (x+1)(x^3 + x^2 + 1)(x^3 + x + 1) \pmod 2$,

b) $b(x) = x^5 - x + 1$ irreducibilis (mod 5), mert nincs gyöke $\mathbb{Z}_5$ -ben, továbbá a másodfokú (irreducibilis) polinomokat mind végigpróbálgatva kap juk, hogy $b(x)$ -nek másodfokú osztója sincs.

c) $c(x) = x^7 - 1 \equiv (x-1)^7 \pmod 7$, hiszen: *tetszőleges* $p \in \mathbb{P}$ *prímszámra és* $a, b \in \mathbb{Z}_p$ *számokra igaz, hogy*

$$(a+b)^p \equiv \sum_{k=0}^{p} a^k b^{p-k} \binom{p}{k} \equiv a^p + b^p \pmod p$$

mert

$$\binom{p}{k} \equiv p\frac{(p-1)...(p-k+1)}{k!} \equiv 0 \pmod p \qquad ha \quad 0 \lneqq k \lneqq p \quad .$$

d) $d(x) = 2x^6 + 3x^5 + 5x^3 + 2x^2 + 4 \equiv (x+1)^2(x+3)(2x^3 - 1) \pmod 7$.

4.4.12) Az $x = 0$ választással kapjuk, hogy

$$7 \mid P(0) = a_0 \quad .$$

Továbbá

$$P(x) - P(-x) = 2x \cdot \left(a_5x^4 + a_3x^2 + a_1\right) \tag{4.35}$$

miatt, az $x = 1$, $x = 2$ és $x = 4$ választással kapjuk, hogy

$$7 \mid (a_5 + a_3 + a_1) \tag{4.36}$$
$$7 \mid (16a_5 + 4a_3 + a_1) \tag{4.37}$$
$$7 \mid (256a_5 + 16a_3 + a_1) \tag{4.38}$$

(felhasználtuk azt a közismert Állítást, mely szerint: *"Ha egy szorzat osztható egy olyan* $c \in \mathbb{Z}$ *számmal, amely a szorzat egyik tényezőjéhez relatív prím, akkor a szorzat másik tényezője osztható* c *-vel".*)

A fenti mennyiségeket összeadva kapjuk

$$7 \mid (273a_5 + 21a_3 + 3a_1) = 3 \cdot (7(13a_5 + a_3) + a_1)$$

ahonnan, az előbb említett állítás szerint

$$7 \mid 7(13a_5 + a_3) + a_1$$

vagyis

$$7 \mid a_1 \quad .$$

Mindezek alapján (4.36) és (4.37) a következőképpen alakul:

$$7 \mid a_5 + a_3 \quad \text{és} \quad 7 \mid 16a_5 + 4a_3 \quad .$$

Ismét e két mennyiséget összeadva és állításunkat használva kapjuk, hogy

$$7 \mid a_3 \quad \text{és} \quad 7 \mid a_5 \quad .$$

Mivel

$$P(x) + P(-x) - 2P(0) = 2x^2 \cdot \left(a_6x^4 + a_4x^2 + a_2\right) \quad ,$$

ezért a (4.35) -ben szereplő kifejezéshez hasonlóan vizsgálhatjuk a fenti kifejezés 7 -tel való oszthatóságát, és kapjuk, hogy

$$7|a_2 \ , \quad 7|a_4 \quad \text{és} \quad 7|a_6 \quad . \qquad \square$$

MEGJEGYZÉSEK: (i) Az

$$a_6 = ... = a_3 = a_0 = 0 \ , \quad a_2 = a_1 = \frac{7}{2}$$

együtthatókkal megadott $P(x) := \frac{7}{2}(x^2 - x)$ polinom szintén minden egész $x \in \mathbb{Z}$ számra 7 -tel osztható *egész* számot ad, de együtthatói mégsem oszthatók 7 -tel (hiszen nem is egész számok).

(ii) Hetedfokú polinomra a feladat eredeti állítása már nem igaz, amint az $x^7 - x$ polinom mutatja. $\square$

5. fejezet

Testek

5.1.3) Felhívjuk a figyelmet, hogy az alábbiakban $=$ jelöli a szokásos egyenlőség jelet, $\equiv_m$ a *modulo* m relációt (mint mindig), és $\equiv_{f(x)}$ a *modulo* $f(x)$ ("polinomosztás" $\mathbb{Z}$ -ben) maradékot.

$$
\begin{aligned}
p(x)\cdot q(x) &= (3x^4+2x^3-4x+1)\cdot(-4x^4+x^2-3x+2)\\
&= -12x^8-8x^7+3x^6+9x^5-4x^4+13x^2-11x+2\\
&\equiv_5 -2x^8-3x^7+3x^6-1x^5+1x^4+3x^2-1x+2\\
&= (x^5-2x^4+3x^3-5x^2+x)\cdot f(x)+(15x^4-18x^3+24x^2-5x+2)\\
&\equiv_{f(x)} 15x^4-18x^3+24x^2-5x+2\\
&\equiv_5 \quad -18x^3+24x^2-5x+2\\
&= \ (-9)\cdot f(x)+(33x^2-14x+38)\\
&\equiv_{f(x)} \quad 33x^2-14x+38\\
&\equiv_5 \quad 3x^2+x+3\ .
\end{aligned}
$$

5.1.4) $GF(4) = Z_2[x]/_{(x^2+x+1)} = (\{0,1,x,x+1\},+,\cdot)$, ahol

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

mert pl.

$$x\cdot x = x^2 \equiv x^2-(x^2+x+1) \equiv x+1 \qquad (\text{mod } x^2+x+1,\ \text{mod } 2)$$

és

$$(x+1)^2 \equiv x^2+1 \equiv x^2+1-(x^2+x+1) \equiv x \qquad (\mathrm{mod}\ x^2+x+1,\ \mathrm{mod}\, 2).$$

6. fejezet

Hálók, Boole-algebrák

6.1. Hálók

6.1.2) $\Re \in Sub(\Re)$ maximális és legnagyobb eleme is $Sub(\Re)$ -nek. Legkisebb ill. minimális eleme nem minden struktúrának van: például a $\mathfrak{Z} = (\mathbb{Z}, +)$ struktúrának minden $k \in \mathbb{Z}$ szám által generált

$$(k) = \{kx : x \in \mathbb{Z}\}$$

részhalmaza zárt az + műveletre, azaz (*ciklikus*[1)]) rész-struktúrája, melynek *bármely* $y \in \mathbb{Z}$ esetén (yk) rész-struktúrája:

$$(yk) \leq (k) \leq \mathfrak{Z} \quad (y \in \mathbb{Z}) \ .$$

[1)] **Definíció:** Az $\mathfrak{A} = \{A, ...\}$ struktúra *egyetlen* elemmel generálható $[a] \leq \mathfrak{A}$ rész-struktúráit ($a \in A$ tetszőleges) **ciklikus** rész-struktúrának nevezzük. □

6.2. Boole-algebrák

Emlékeztetőül a BA axiómák:

kommutativitás	$A \cup B = B \cup A$	(BA1)
	$A \cap B = B \cap A$	(BA2)
asszociativitás	$A \cup (B \cup C) = (A \cup B) \cup C$	(BA3)
	$A \cap (B \cap C) = (A \cap B) \cap C$	(BA4)
disztributivitás	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	(BA5)
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	(BA6)
elnyelési tulajdonságok	$A \cup (A \cap B) = A$	(BA7)
	$A \cap (A \cup B) = A$	(BA8)
$\emptyset$ és I tulajdonságai	$A \cup \overline{A} = I$	(BA9)
	$A \cap \overline{A} = \emptyset$	(BA10)
	$A \cup \emptyset = A$	(BA11)
	$A \cap \emptyset = \emptyset$	(BA12)
	$A \cup I = I$	(BA13)
	$A \cap I = A$	(BA14)

Nem árt felidéznünk azt sem, hogy a Boole Algebrák szerkezetének részletesebb vizsgálata (pl. [$Sz'01$]) alapján megállapítható (pl.[J], 8.§):

Tétel: *Minden* véges *Boole-Algebra elemszáma* 2^k *valamilyen* $k \in \mathbb{N}$ *számra.* □

6.2.1) Csak néhány példát sorolunk fel:

$\mathcal{R}$ -ben: (BA5): $A + (B \cdot C) = (A + B) \cdot (A + C)$ nem igaz,

(BA7), (BA8): $A + (A \cdot B) = A$, $A \cdot (A + B) = A$ nem igazak,

$\mathcal{T}$ -ben (BA4): $min(a, min(b, c)) = min(min(a, b), c)$ igaz,

(BA5): $max(a, min(b, c)) = min\,(max(a, b), max(a, c))$ igaz,

(BA6): $min(a, max(b, c)) = max\,(min(a, b), min(a, c))$ igaz,

(BA9), (BA10): $min(a, 1-a) = 0$, $max(a, 1-a) = 1$ nem igazak,

De Morgan:

$$\begin{aligned} 1 - max(a, b) &= min(1 - a, 1 - b)\ , \\ 1 - min(a, b) &= max(1 - a, 1 - b) \quad \text{igazak.} \end{aligned}$$

6.2.2) Csak néhány példát sorolunk fel:

$\mathcal{P}_\Omega$ -ben (BA5): $A + (B \cdot C) = (A + B) \cdot (A + C)$,

(BA6): $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$ (események összege és szorzata).

Felhívjuk a figyelmet, hogy a *valós számok* ($\mathbb{R}$) szokásos összeadása és szorzása *nem* teljesíti a (BA1)-(BA14) axiómákat, azaz *nem* Boole algebra !

$\mathcal{N}_N$ -ben (BA4): $lnko(a, lnko(b, c)) = lnko(lnko(a, b), c)$,

(BA5): $lkkt(a, lnko(b, c)) = lnko\,(lkkt(a, b), lkkt(a, c))$

(BA6): $lnko(a, lkkt(b, c)) = lkkt\,(lnko(a, b), lnko(a, c))$

(BA9), (BA10): $lnko\left(a, \frac{N}{a}\right) = 1$, $lkkt\left(a, \frac{N}{a}\right) = N$
(mert N négyzetmentes),

De Morgan:

$$\frac{N}{lnko(a,b)} = lkkt\left(\frac{N}{a}, \frac{N}{b}\right) \ , \quad \frac{N}{lkkt(a,b)} = lnko\left(\frac{N}{a}, \frac{N}{b}\right) \ ,$$

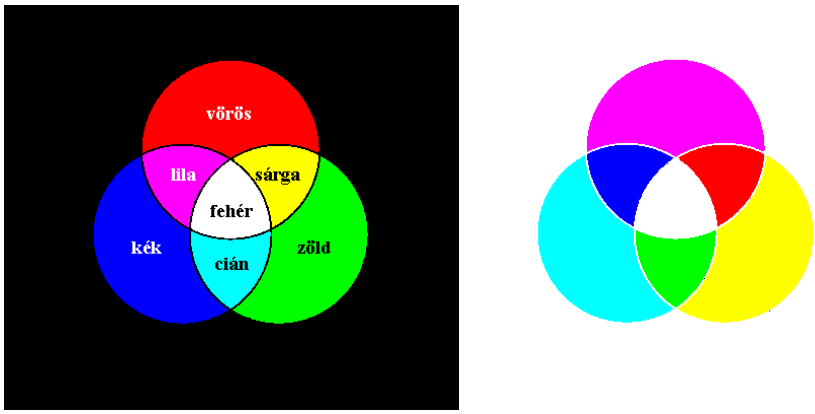
$\mathcal{C}$ -ben: $\mathcal{C} = (C, \cup, \cap, ^- , Fehér, Fekete)$ ahol

$C = \{Fekete,\ Sárga,\ Cián,\ Magenta,\ Kék,\ Zöld,\ Vörös,\ Fehér\}$

és például $Vörös \cup Zöld = Sárga$, $Cián \cap Sárga = Zöld$, $\overline{Vörös} = Zöld$,

De Morgan:

$$\overline{Kék \cup Zöld} = Vörös, \quad \overline{Magenta \cap Cián} = Sárga \quad .$$



Additív és szubtraktív[2)] *színkeverés*

[2)] **addíció** = összeadás, **szubtrakció** = kivonás

III. rész

Függelék

.1. Gót ABC

Aa	𝔄a	𝔄 𝔞
Bb	𝔅b	𝔅 𝔟
Cc	ℭc	ℭ 𝔠
Dd	𝔇d	𝔇 𝔡
Ee	𝔈e	𝔈 𝔢
Ff	𝔉f	𝔉 𝔣
Gg	𝔊g	𝔊 𝔤
Hh	ℌh	ℌ 𝔥
Ii	ℑi	ℑ 𝔦
Jj	𝔍j	𝔍 𝔧
Kk	𝔎k	𝔎 𝔨
Ll	𝔏l	𝔏 𝔩
Mm	𝔐m	𝔐 𝔪
Nn	𝔑n	𝔑 𝔫
Oo	𝔒o	𝔒 𝔬
Pp	𝔓p	𝔓 𝔭
Qq	𝔔q	𝔔 𝔮
Rr	ℜr	ℜ 𝔯
Ss	𝔖s	𝔖 𝔰
Tt	𝔗t	𝔗 𝔱
Uu	𝔘u	𝔘 𝔲
Vv	𝔙v	𝔙 𝔳
Ww	𝔚w	𝔚 𝔴
Xx	𝔛x	𝔛 𝔵
Yy	𝔜y	𝔜 𝔶
Zz	ℨz	ℨ 𝔷

Modified Vowels (Umlaute)

Ää	Ä ä	Ä ä
Öö	Ö ö	Ö ö
Üü	Ü ü	Ü ü

Compound Consonants

ch	ch	ch
sch	ſch	ſch
ck	ck	ck
ss	ſſ	ſſ
ß (SZ, SS)	ß (ſz ſſ)	ß
st	ſt	ſt
tz	tz	tz
ph	ph	ph

.2. Egész számok felbontása 30.000 -ig

Csak a 2, 3, 5 és 11-el *nem* osztható számokat soroltuk fel.

Emlékeztetőül a **11-es próba:** *Egy tetszőleges $n \in \mathbb{Z}$ egész szám pontosan akkor osztható* 11 *-gyel, ha számjegyeit* váltakozó előjellel *összeadva a kapott összeg osztható* 11 *-gyel.* □

7, 13, 17,
19, 23, 29,
31, 37, 41,
43, 47
49 = 7*7
53
59
61
67
71
73
79
83
89
91 = 7*13
97
101
103
107
109
113
119 = 7*17
127
131
133 = 7*19
137
139
149
151
157
161 = 7*23
163
167
169 = 13*13
173
179
181
191
193
197
199
203 = 7*29
211
217 = 7*31
221 = 13*17
223
227
229
233
239
241
247 = 13*19
251
257
259 = 7*37
263
269
271
277
281
283
287 = 7*41
289 = 17*17
293
299 = 13*23
301 = 7*43
307
311
313
317
323 = 17*19
329 = 7*47
331
337
343 = 7*7*7
347
349
353
359
361 = 19*19
367
371 = 7*53
373
377 = 13*29
379
383
389
391 = 17*23
397
401
403 = 13*31
409
413 = 7*59
419
421
427 = 7*61
431
433
437 = 19*23
439
443
449
457
461
463
467
469 = 7*67
479
481 = 13*37
487
491
493 = 17*29
497 = 7*71
499
503
509
511 = 7*73
521
523
527 = 17*31
529 = 23*23
533 = 13*41
541
547
551 = 19*29
553 = 7*79
557
559 = 13*43
563
569
571
577
581 = 7*83
587
589 = 19*31
593
599
601
607
611 = 13*47
613
617
619
623 = 7*89
629 = 17*37
631
637 = 7*7*13
641
643
647
653
659
661
667 = 23*29
673
677
679 = 7*97
683
689 = 13*53
691
697 = 17*41
701
703 = 19*37
707 = 7*101
709
713 = 23*31
719
721 = 7*103
727
731 = 17*43
733
739
743
749 = 7*107
751
757
761
763 = 7*109
767 = 13*59
769
773
779 = 19*41
787
791 = 7*113
793 = 13*61
797
799 = 17*47
809
811
817 = 19*43
821
823
827
829
833 = 7*7*17
839
841 = 29*29
851 = 23*37
853
857
859
863
871 = 13*67
877
881
883
887
889 = 7*127
893 = 19*47
899 = 29*31
901 = 17*53
907
911
917 = 7*131
919
923 = 13*71
929
931 = 7*7*19
937
941
943 = 23*41
947
949 = 13*73
953
959 = 7*137
961 = 31*31
967
971
973 = 7*139
977
983
989 = 23*43
991
997
1003 = 17*59
1007 = 19*53
1009
1013
1019
1021
1027 = 13*79
1031
1033
1037 = 17*61
1039
1043 = 7*149
1049
1051
1057 = 7*151
1061
1063
1069
1073 = 29*37
1079 = 13*83
1081 = 23*47
1087
1091
1093
1097
1099 = 7*157
1103
1109
1117
1121 = 19*59
1123
1127 = 7*7*23
1129
1139 = 17*67
1141 = 7*163
1147 = 31*37
1151
1153
1157 = 13*89
1159 = 19*61
1163
1169 = 7*167

1171
1181
1183 = 7*13*13
1187
1189 = 29*41
1193
1201
1207 = 17*71
1211 = 7*173
1213
1217
1219 = 23*53
1223
1229
1231
1237
1241 = 17*73
1247 = 29*43
1249
1253 = 7*179
1259
1261 = 13*97
1267 = 7*181
1271 = 31*41
1273 = 19*67
1277
1279
1283
1289
1291
1297
1301
1303
1307
1313 = 13*101
1319
1321
1327
1333 = 31*43
1337 = 7*191
1339 = 13*103
1343 = 17*79
1349 = 19*71
1351 = 7*193
1357 = 23*59
1361
1363 = 29*47
1367
1369 = 37*37
1373
1379 = 7*197
1381
1387 = 19*73
1391 = 13*107
1393 = 7*199
1399
1403 = 23*61
1409
1411 = 17*83
1417 = 13*109
1421 = 7*7*29
1423
1427
1429
1433
1439
1447
1451
1453
1457 = 31*47
1459
1469 = 13*113
1471
1477 = 7*211
1481
1483
1487
1489
1493
1499
1501 = 19*79
1511
1513 = 17*89
1517 = 37*41
1519 = 7*7*31
1523
1531
1537 = 29*53
1541 = 23*67
1543
1547 = 7*13*17
1549
1553
1559
1561 = 7*223
1567
1571
1577 = 19*83
1579
1583
1589 = 7*227
1591 = 37*43
1597
1601
1603 = 7*229
1607
1609
1613
1619
1621
1627
1631 = 7*233
1633 = 23*71
1637
1643 = 31*53
1649 = 17*97
1651 = 13*127
1657
1663
1667
1669
1673 = 7*239
1679 = 23*73
1681 = 41*41
1687 = 7*241
1691 = 19*89
1693
1697
1699
1703 = 13*131
1709
1711 = 29*59
1717 = 17*101
1721
1723
1729 = 7*13*19
1733
1739 = 37*47
1741
1747
1751 = 17*103
1753
1757 = 7*251
1759
1763 = 41*43
1769 = 29*61
1777
1781 = 13*137
1783
1787
1789
1799 = 7*257
1801
1807 = 13*139
1811
1813 = 7*7*37*
1817 = 23*79
1819 = 17*107
1823
1829 = 31*59
1831
1841 = 7*263
1843 = 19*97
1847
1849 = 43*43
1853 = 17*109
1861
1867
1871
1873
1877
1879
1883 = 7*269
1889
1891 = 31*61
1897 = 7*271
1901
1907
1909 = 23*83
1913
1919 = 19*101
1921 = 17*113
1927 = 41*47
1931
1933
1937 = 13*149
1939 = 7*277
1943 = 29*67
1949
1951
1957 = 19*103
1961 = 37*53
1963 = 13*151
1967 = 7*281
1973
1979
1981 = 7*283
1987
1993
1997
1999
2003
2009 = 7*7*41
2011
2017
2021 = 43*47
2023 = 7*17*17
2027
2029
2033 = 19*107
2039
2041 = 13*157
2047 = 23*89
2051 = 7*293
2053
2059 = 29*71
2063
2069
2071 = 19*109
2077 = 31*67
2081
2083
2087
2089
2093 = 7*13*23
2099
2107 = 7*7*43
2111
2113
2117 = 29*73
2119 = 13*163
2129
2131
2137
2141
2143
2147 = 19*113
2149 = 7*307
2153
2159 = 17*127
2161
2171 = 13*167
2173 = 41*53
2177 = 7*311
2179
2183 =37*59
2191 = 7*313
2197 =13*13*13
2201 =31*71
2203
2207
2209 = 47*47
2213
2219 = 7*317
2221
2227 = 17*131
2231 = 23*97
2237
2239
2243
2249 = 13*173
2251
2257 = 37*61
2261 = 7*17*19
2263 = 31*73
2267
2269
2273
2279 = 43*53
2281
2287
2291 = 29*79
2293
2297
2303 = 7*7*47
2309
2311
2317 = 7*331
2323 = 23*101
2327 = 13*179

2329 = 17*137
2333
2339
2341
2347
2351
2353 = 13*181
2357
2359 = 7*337
2363 = 17*139
2369 = 23*103
2371
2377
2381
2383
2389
2393
2399
2401 = 7*7*7*7
2407 = 29*83
2411
2413 = 19*127
2417
2419 = 41*59
2423
2429 = 7*347
2437
2441
2443 = 7*349
2447
2449 = 31*79
2459
2461 = 23*107
2467
2471 = 7*353
2473
2477
2479 = 37*67
2483 = 13*191
2489 = 19*131
2491 = 47*53
2501 = 41*61
2503
2507 = 23*109
2509 = 13*193
2513 = 7*359
2521
2527 = 7*19*19
2531
2533 = 17*149
2537 = 43*59
2539
2543
2549
2551
2557
2561 = 13*197
2567 = 17*151
2569 = 7*367
2573 = 31*83
2579
2581 = 29*89
2587 = 13*199
2591
2593
2597 = 7*7*53
2599 = 23*113
2603 = 19*137
2609
2611 = 7*373
2617
2621
2623 = 43*61
2627 = 37*71
2633
2639 = 7*13*29
2641 = 19*139
2647
2653 = 7*379
2657
2659
2663
2669 = 17*157
2671
2677
2681 = 7*383
2683
2687
2689
2693
2699
2701 = 37*73
2707
2711
2713
2719
2723 = 7*389
2729
2731
2737 = 7*17*23
2741
2743 = 13*211
2747 = 41*67
2749
2753
2759 = 31*89
2767
2771 = 17*163
2773 = 47*59
2777
2779 = 7*397
2789
2791
2797
2801
2803
2807 = 7*401
2809 = 53*53
2813 = 29*97
2819
2821 = 7*13*31
2831 = 19*149
2833
2837
2839 = 17*167
2843
2851
2857
2861
2863 = 7*409
2867 = 47*61
2869 = 19*151
2873 =13*13*17
2879
2881 = 43*67
2887
2891 = 7*7*59
2897
2899 = 13*223
2903
2909
2911 = 41*71
2917
2921 = 23*127
2923 = 37*79
2927
2929 = 29*101
2933 = 7*419
2939
2941 = 17*173
2947 = 7*421
2951 = 13*227
2953
2957
2963
2969
2971
2977 = 13*229
2983 = 19*157
2987 = 29*103
2989 = 7*7*61
2993 = 41*73
2999
3001
3007 = 31*97
3011
3013 = 23*131
3017 = 7*431
3019
3023
3029 = 13*233
3031 = 7*433
3037
3041
3043 = 17*179
3049
3053 = 43*71
3059 = 7*19*23
3061
3067
3071 = 37*83
3073 = 7*439
3077 = 17*181
3079
3083
3089
3097 = 19*163
3101 = 7*443
3103 = 29*107
3107 = 13*239
3109
3119
3121
3127 = 53*59
3131 = 31*101
3133 = 13*241
3137
3139 = 43*73
3143 = 7*449
3149 = 47*67
3151 = 23*137
3161 = 29*109
3163
3167
3169
3173 = 19*167
3181
3187
3191
3193 = 31*103
3197 = 23*139
3199 = 7*457
3203
3209
3211 =13*13*19
3217
3221
3227 = 7*461
3229
3233 = 53*61
3239 = 41*79
3241 = 7*463
3247 = 17*191
3251
3253
3257
3259
3263 = 13*251
3269 = 7*467
3271
3277 = 29*113
3281 = 17*193
3283 = 7*7*67
3287 = 19*173
3293 = 37*89
3299
3301
3307
3313
3317 = 31*107
3319
3323
3329
3331
3337 = 47*71
3341 = 13*257
3343
3347
3349 = 17*197
3353 = 7*479
3359
3361
3367 = 7*13*37
3371
3373
3379 = 31*109
3383 = 17*199
3389
3391
3397 = 43*79
3401 = 19*179
3403 = 41*83
3407
3409 = 7*487
3413
3419 = 13*263
3427 = 23*149
3431 = 47*73
3433
3437 = 7*491
3439 = 19*181
3449
3451 = 7*17*29
3457
3461
3463
3467
3469
3473 = 23*151
3479 = 7*7*71

3481 = 59*59
3491
3493 = 7*499
3497 = 13*269
3499
3503 = 31*113
3511
3517
3521 = 7*503
3523 = 13*271
3527
3529
3533
3539
3541
3547
3551 = 53*67
3557
3559
3563 = 7*509
3569 = 43*83
3571
3577 = 7*7*73
3581
3583
3587 = 17*211
3589 = 37*97
3593
3599 = 59*61
3601 = 13*277
3607
3611 = 23*157
3613
3617
3623
3629 = 19*191
3631
3637
3643
3647 = 7*521
3649 = 41*89
3653 = 13*281
3659
3661 = 7*523
3667 = 19*193
3671
3673
3677
3679 = 13*283
3683 = 29*127
3689 = 7*17*31
3691
3697
3701
3703 = 7*23*23
3709
3713 = 47*79
3719
3721 = 61*61
3727
3731 = 7*13*41
3733
3737 = 37*101
3739
3743 = 19*197
3749 = 23*163
3757 =13*17*17
3761
3763 = 53*71
3767

3769
3779
3781 = 19*199
3787 = 7*541
3791 = 17*223
3793
3797
3799 = 29*131
3803
3809 = 13*293
3811 = 37*103
3821
3823
3827 = 43*89
3829 = 7*547
3833
3841 = 23*167
3847
3851
3853
3857 = 7*19*29
3859 = 17*227
3863
3869 = 53*73
3871 = 7*7*79
3877
3881
3887 =13*13*23
3889
3893 = 17*229
3899 = 7*557
3901 = 47*83
3907
3911
3913 =
7*13*43*
3917
3919
3923
3929
3931
3937 = 31*127
3941 = 7*563
3943
3947
3953 = 59*67
3959 = 37*107
3961 = 17*233
3967
3973 = 29*137
3977 = 41*97
3979 = 23*173
3983 = 7*569
3989
3991 = 13*307
3997 = 7*571
4001
4003
4007
4009 = 19*211
4013
4019
4021
4027
4031 = 29*139
4033 = 37*109
4039 = 7*577
4043 = 13*311
4049
4051

4057
4061 = 31*131
4063 = 17*239
4067 = 7*7*83
4069 = 13*313
4073
4079
4087 = 61*67
4091
4093
4097 = 17*241
4099
4109 = 7*587
4111
4117 = 23*179
4121 = 13*317
4123 = 7*19*31
4127
4129
4133
4139
4141 = 41*101
4151 = 7*593
4153
4157
4159
4163 = 23*181
4171 = 43*97
4177
4181 = 37*113
4183 = 47*89
4187 = 53*79
4189 = 59*71
4193 = 7*599
4199 =
13*17*19*
4201
4207 = 7*601
4211
4217
4219
4223 = 41*103
4229
4231
4237 = 19*223
4241
4243
4247 = 31*137
4249 = 7*607
4253
4259
4261
4267 = 17*251
4271
4273
4277 = 7*13*47
4283
4289
4291 = 7*613
4297
4303 = 13*331
4307 = 59*73
4309 = 31*139
4313 = 19*227
4319 = 7*617
4321 = 29*149
4327
4331 = 61*71
4333 = 7*619
4337

4339
4343 = 43*101
4349
4351 = 19*229
4357
4361 = 7*7*89
4363
4369 = 17*257
4373
4379 = 29*151
4381 = 13*337
4387 = 41*107
4391
4393 = 23*191
4397
4399 = 53*83
4403 = 7*17*37
4409
4417 = 7*631
4421
4423
4427 = 19*233
4429 = 43*103
4439 = 23*193
4441
4447
4451
4453 = 61*73
4457
4459 =7*7*7*13
4463
4469 = 41*109
4471 = 17*263
4481
4483
4487 = 7*641
4489 = 67*67
4493
4501 = 7*643
4507
4511 = 13*347
4513
4517
4519
4523
4529 = 7*647
4531 = 23*197
4537 = 13*349
4541 = 19*239
4547
4549
4553 = 29*157
4559 = 47*97
4561
4567
4571 = 7*653
4573 = 17*269
4577 = 23*199
4579 = 19*241
4583
4589 = 13*353
4591
4597
4601 = 43*107
4603
4607 = 17*271
4613 = 7*659
4619 = 31*149
4621
4627 = 7*661

4633 = 41*113
4637
4639
4643
4649
4651
4657
4661 = 59*79
4663
4667 = 13*359
4669 = 7*23*29
4673
4679
4681 = 31*151
4687 = 43*109
4691
4693 =13*19*19
4699 =37*127
4703
4709 = 17*277
4711 = 7*673
4717 = 53*89
4721
4723
4727 = 29*163
4729
4733
4739 = 7*677
4747 = 47*101
4751
4753 = 7*7*97
4757 = 67*71
4759
4769 = 19*251
4771 = 13*367
4777 = 17*281
4781 = 7*683
4783
4787
4789
4793
4799
4801
4811 = 17*283
4813
4817
4819 = 61*79
4823 = 7*13*53
4831
4837 = 7*691
4841 = 47*103
4843 = 29*167
4847 = 37*131
4849 = 13*373
4853 = 23*211
4859 = 43*113
4861
4867 = 31*157
4871
4877
4879 = 7*17*41
4883 = 19*257
4889
4891 = 67*73
4897 = 59*83
4901 =13*13*29
4903
4907 = 7*701
4909
4913 =17*17*17
4919
4921 = 7*19*37
4927 = 13*379
4931
4933
4937
4943
4949 = 7*7*101
4951
4957
4963 = 7*709
4967
4969
4973
4979 = 13*383
4981 = 17*293
4987
4991 = 7*23*31
4993
4997 = 19*263
4999
5003
5009
5011
5017 = 29*173
5021
5023
5029 = 47*107
5033 = 7*719
5039
5041 = 71*71
5047 = 7*7*103
5051
5053 = 31*163
5057 = 13*389
5059
5063 = 61*83
5069 = 37*137
5077
5081
5083 =13*17*23
5087
5089 = 7*727
5099
5101
5107
5111 = 19*269
5113
5117 = 7*17*43
5119
5123 = 47*109
5129 = 23*223
5131 = 7*733
5141 = 53*97
5143 = 37*139
5147
5149 = 19*271
5153
5161 = 13*397
5167
5171
5173 = 7*739
5177 = 31*167
5179
5183 = 71*73
5189
5191 = 29*179
5197
5201 = 7*743
5207 = 41*127
5209
5213 = 13*401
5219 = 17*307
5221 = 23*227
5227
5231
5233
5237
5239 =13*13*31
5243 = 7*7*107
5249 = 29*181
5251 = 59*89
5257 = 7*751
5261
5263 = 19*277
5267 = 23*229
5273
5279
5281
5287 = 17*311
5293 = 67*79
5297
5299 = 7*757
5303
5309
5311 = 47*113
5317 = 13*409
5321 = 17*313
5323
5327 = 7*761
5329 = 73*73
5333
5339 = 19*281
5341 = 7*7*109
5347
5351
5353 = 53*101
5359 = 23*233
5363 = 31*173
5369 = 7*13*59
5371 = 41*131
5377 = 19*283
5381
5383 = 7*769
5387
5389 = 17*317
5393
5399
5407
5411 = 7*773
5413
5417
5419
5429 = 61*89
5431
5437
5441
5443
5447 = 13*419
5449
5453 = 7*19*41
5459 = 53*103
5461 = 43*127
5471
5473 = 13*421
5477
5479
5483
5491 =17*17*19
5497 =23*239
5501
5503
5507
5509 = 7*787
5513 = 37*149
5519
5521
5527
5531
5537 = 7*7*113
5539 = 29*191
5543 = 23*241
5549 = 31*179
5551 = 7*13*61
5557
5561 = 67*83
5563
5567 = 19*293
5569
5573
5579 = 7*797
5581
5587 = 37*151
5591
5593 = 7*17*47
5597 = 29*193
5603 = 13*431
5609 = 71*79
5611 = 31*181
5617 = 41*137
5623
5627 = 17*331
5629 = 13*433
5633 = 43*131
5639
5641
5647
5651
5653
5657
5659
5663 = 7*809
5669
5671 = 53*107
5677 = 7*811
5681 =13*19*23
5683
5689
5693
5699 = 41*139
5701
5707 = 13*439
5711
5713 = 29*197
5717
5719 = 7*19*43
5723 = 59*97
5729 = 17*337
5737
5741
5743
5747 = 7*821
5749
5759 = 13*443
5761 = 7*823
5767 = 73*79
5771 = 29*199
5773 = 23*251
5777 = 53*109
5779

5783
5789 = 7*827
5791
5801
5803 = 7*829
5807
5809 = 37*157
5813
5821
5827
5831 =7*7*7*17
5833 = 19*307
5837 = 13*449
5839
5843
5849
5851
5857
5861
5867
5869
5873 = 7*839
5879
5881
5887 = 7*29*29
5891 = 43*137
5893 = 71*83
5897
5899 = 17*347
5903
5909 = 19*311
5911 = 23*257
5917 = 61*97
5921 = 31*191
5923
5927
5933 = 17*349
5939
5941 = 13*457
5947 = 19*313
5953
5957 = 7*23*37
5959 = 59*101
5963 = 67*89
5969 = 47*127
5971 = 7*853
5977 = 43*139
5981
5983 = 31*193
5987
5989 = 53*113
5993 = 13*461
5999 = 7*857
6001 = 17*353
6007
6011
6013 = 7*859
6019 = 13*463
6023 = 19*317
6029
6031 = 37*163
6037
6041 = 7*863
6043
6047
6049 = 23*263
6053
6059 = 73*83
6067
6071 = 13*467
6073
6077 = 59*103
6079
6089
6091
6097 = 7*13*67
6101
6103 = 17*359
6107 = 31*197
6109 = 41*149
6113
6119 = 29*211
6121
6131
6133
6137 =17*19*19
6139 = 7*877
6143
6151
6157 = 47*131
6161 = 61*101
6163
6167 = 7*881
6169 = 31*199
6173
6179 = 37*167
6181 = 7*883
6187 = 23*269
6191 = 41*151
6197
6199
6203
6209 = 7*887
6211
6217
6221
6223 = 7*7*127
6227 = 13*479
6229
6233 = 23*271
6239 = 17*367
6241 = 79*79
6247
6251 = 7*19*47
6253 =13*13*37
6257
6263
6269
6271
6277
6283 = 61*103
6287
6289 = 19*331
6293 = 7*29*31
6299
6301
6307 = 7*17*53
6311
6313 = 59*107
6317
6319 = 71*89
6323
6329
6331 = 13*487
6337
6341 = 17*373
6343
6349 = 7*907
6353
6359
6361
6367
6371 = 23*277
6373
6377 = 7*911
6379
6383 = 13*491
6389
6397
6401 = 37*173
6403 = 19*337
6407 = 43*149
6409 =13*17*29
6419 = 7*7*131
6421
6427
6431 = 59*109
6433 = 7*919
6437 = 41*157
6439 = 47*137
6443 = 17*379
6449
6451
6461 = 7*13*71
6463 = 23*281
6467 = 29*223
6469
6473
6481
6487 = 13*499
6491
6493 = 43*151
6497 = 73*89
6499 = 67*97
6503 = 7*929
6509 = 23*283
6511 = 17*383
6517 =7*7*7*19
6521
6527 = 61*107
6529
6533 = 47*139
6539 = 13*503
6541 = 31*211
6547
6551
6553
6557 = 79*83
6559 = 7*937
6563
6569
6571
6577
6581
6583 = 29*227
6587 = 7*941
6593 = 19*347
6599
6601 = 7*23*41
6607
6613 = 17*389
6617 = 13*509
6619
6623 = 37*179
6629 = 7*947
6631 = 19*349
6637
6641 = 29*229
6643 = 7*13*73
6647 =17*17*23
6649 =61*109
6653
6659
6661
6667 = 59*113
6671 = 7*953
6673
6679
6683 = 41*163
6689
6691
6697 = 37*181
6701
6703
6707 = 19*353
6709
6713 = 7*7*137
6719
6727 = 7*31*31
6731 = 53*127
6733
6737
6739 = 23*293
6749 = 17*397
6751 = 43*157
6757 = 29*233
6761
6763
6767 = 67*101
6769 = 7*967
6773 = 13*521
6779
6781
6791
6793
6797 = 7*971
6799 = 13*523
6803
6811 = 7*7*139
6817 = 17*401
6821 = 19*359
6823
6827
6829
6833
6839 = 7*977
6841
6847 = 41*167
6851 =13*17*31
6857
6859 =19*19*19
6863
6869
6871
6877 =13*23*23
6881 = 7*983
6883
6887 = 71*97
6889 = 83*83
6893 = 61*113
6899
6901 = 67*103
6907
6911
6913 = 31*223
6917
6923 = 7*23*43
6929 =13*13*41
6931 = 29*239
6937 = 7*991

6943 = 53*131
6947
6949
6953 = 17*409
6959
6961
6967
6971
6973 = 19*367
6977
6979 = 7*997
6983
6989 = 29*241
6991
6997
7001
7003 = 47*149
7009 = 43*163
7013
7019
7021 = 7*17*59
7027
7031 = 79*89
7033 = 13*541
7037 = 31*227
7039
7043
7049 = 7*19*53
7057
7061 = 23*307
7063 = 7*1009
7067 = 37*191
7069
7079
7081 = 73*97
7087 = 19*373
7091 = 7*1013
7093 = 41*173
7097 = 47*151
7099 = 31*229
7103
7109
7111 = 13*547
7121
7123 = 17*419
7127
7129
7133 = 7*1019
7141 = 37*193
7147 = 7*1021
7151
7153 = 23*311
7157 = 17*421
7159
7163 =13*19*29
7169 =67*107
7171 =71*101
7177
7181 = 43*167
7187
7189 = 7*13*79
7193
7199 = 23*313
7201 = 19*379
7207
7211
7213
7217 = 7*1031
7219
7223 = 31*233
7229
7231 = 7*1033
7237
7241 = 13*557
7243
7247
7253
7259 = 7*17*61
7261 = 53*137
7267 =13*13*43
7273 = 7*1039
7277 = 19*383
7279 = 29*251
7283
7289 = 37*197
7291 = 23*317
7297
7301 = 7*7*149
7303 = 67*109
7307
7309
7313 = 71*103
7319 = 13*563
7321
7327 = 17*431
7331
7333
7339 = 41*179
7343 = 7*1049
7349
7351
7357 = 7*1051
7361 = 17*433
7363 = 37*199
7367 = 53*139
7369
7373 = 73*101
7379 = 47*157
7387 = 83*89
7391 = 19*389
7393
7397 = 13*569
7399 = 7*7*151
7409 = 31*239
7411
7417
7421 = 41*181
7423 = 13*571
7427 = 7*1061
7429 =17*19*23
7433
7439 = 43*173
7441 = 7*1063
7451
7453 = 29*257
7457
7459
7463 = 17*439
7471 = 31*241
7477
7481
7483 = 7*1069
7487
7489
7493 = 59*127
7499
7501 = 13*577
7507
7511 = 7*29*37
7517
7519 = 73*103
7523
7529
7531 = 17*443
7537
7541
7543 = 19*397
7547
7549
7553 = 7*13*83
7559
7561
7567 = 7*23*47
7571 = 67*113
7573
7577
7583
7589
7591
7597 = 71*107
7603
7607
7609 = 7*1087
7613 = 23*331
7619 = 19*401
7621
7627 = 29*263
7631 = 13*587
7633 = 17*449
7637 = 7*1091
7639
7643
7649
7651 = 7*1093
7657 =13*19*31
7661 = 47*163
7663 = 79*97
7669
7673
7679 = 7*1097
7681
7687
7691
7693 = 7*7*157
7697 = 43*179
7699
7703
7709 = 13*593
7717
7721 = 7*1103
7723
7727
7729 = 59*131
7739 = 71*109
7741
7747 = 61*127
7751 = 23*337
7753
7757
7759
7763 = 7*1109
7769 = 17*457
7771 = 19*409
7781 = 31*251
7783 = 43*181
7787 = 13*599
7789
7793
7801 = 29*269
7807 = 37*211
7811 = 73*107
7813 = 13*601
7817
7819 = 7*1117
7823
7829
7831 = 41*191
7837 = 17*461
7841
7847 = 7*19*59
7849 = 47*167
7853
7859 = 29*271
7861 = 7*1123
7867
7871 = 17*463
7873
7877
7879
7883
7889 =7*7*7*23
7891 = 13*607
7897 = 53*149
7901
7903 = 7*1129
7907
7913 = 41*193
7919
7921 = 89*89
7927
7933
7937
7939 = 17*467
7943 =13*13*47
7949
7951
7957 = 73*109
7961 = 19*419
7963
7967 = 31*257
7969 = 13*613
7973 = 7*17*67
7979 = 79*101
7981 = 23*347
7987 = 7*7*163
7991 = 61*131
7993
7999 = 19*421
8003 = 53*151
8009
8011
8017
8021 = 13*617
8023 = 71*113
8027 = 23*349
8029 = 7*31*37
8033 = 29*277
8039
8047 = 13*619
8051 = 83*97
8053
8057 = 7*1151
8059
8069
8071 = 7*1153
8077 = 41*197
8081
8083 = 59*137
8087
8089

8093
8099 = 7*13*89
8101
8111
8113 = 7*19*61
8117
8119 = 23*353
8123
8131 = 47*173
8137 = 79*103
8141 = 7*1163
8143 = 17*479
8147
8149 = 29*281
8153 = 31*263
8159 = 41*199
8161
8167
8171
8177 =13*17*37
8179
8183 = 7*7*167
8189 = 19*431
8191
8197 = 7*1171
8201 = 59*139
8203 = 13*631
8207 = 29*283
8209
8213 = 43*191
8219
8221
8227 = 19*433
8231
8233
8237
8243
8249 = 73*113
8251 = 37*223
8257 = 23*359
8263
8267 = 7*1181
8269
8273
8279 = 17*487
8281 = 7^2*13^2
8287
8291
8293
8297
8299 = 43*193
8303 =19*19*23
8309 = 7*1187
8311
8317
8321 = 53*157
8323 = 7*29*41
8329
8333 = 13*641
8339 = 31*269
8341 = 19*439
8347 = 17*491
8351 = 7*1193
8353
8357 = 61*137
8359 = 13*643
8363
8369
8377
8381 =17*17*29
8383 =83*101
8387
8389
8399 = 37*227
8401 = 31*271
8407 = 7*1201
8411 = 13*647
8413 = 47*179
8417 = 19*443
8419
8423
8429
8431
8441 = 23*367
8443
8447
8449 = 7*17*71
8453 = 79*107
8461
8467
8471 = 43*197
8473 = 37*229
8477 = 7*7*173
8479 = 61*139
8483 = 17*499
8489 = 13*653
8491 = 7*1213
8497 = 29*293
8501
8507 = 47*181
8509 = 67*127
8513
8519 = 7*1217
8521
8527
8531 = 19*449
8533 = 7*23*53
8537
8539
8543
8549 = 83*103
8551 = 17*503
8557 = 43*199
8561 = 7*1223
8563
8567 = 13*659
8573
8579 = 23*373
8581
8587 = 31*277
8593 = 13*661
8597
8599
8603 = 7*1229
8609
8611 = 79*109
8617 = 7*1231
8621 = 37*233
8623
8627
8629
8633 = 89*97
8639 = 53*163
8641
8647
8651 = 41*211
8653 = 17*509
8659 = 7*1237
8663
8669
8671 =13*23*29
8677
8681
8683 = 19*457
8687 = 7*17*73
8689
8693
8699
8707
8711 = 31*281
8713
8717 = 23*379
8719
8729 = 7*29*43
8731
8737
8741
8743 = 7*1249
8747
8749 = 13*673
8753
8759 = 19*461
8761
8771 = 7*7*179
8773 = 31*283
8777 = 67*131
8779
8783
8791 = 59*149
8797 = 19*463
8801 = 13*677
8803
8807
8809 = 23*383
8813 = 7*1259
8819
8821
8827 = 7*13*97
8831
8837
8839
8843 = 37*239
8849
8851 = 53*167
8857 = 17*521
8861
8863
8867
8869 = 7*7*181
8873 = 19*467
8879 = 13*683
8881 = 83*107
8887
8891 = 17*523
8893
8897 = 7*31*41
8903 = 29*307
8909 = 59*151
8911 = 7*19*67
8917 = 37*241
8923
8927 = 79*113
8929
8933
8939 = 7*1277
8941
8947 = 23*389
8951
8953 = 7*1279
8957 =13*13*53
8959 =17*17*31
8963
8969
8971
8977 = 47*191
8981 = 7*1283
8983 = 13*691
8989 = 89*101
8993 =17*23*23
8999
9001
9007
9011
9013
9017 = 71*127
9019 = 29*311
9023 = 7*1289
9029
9037 = 7*1291
9041
9043
9047 = 83*109
9049
9059
9061 =13*17*41
9067
9071 = 47*193
9073 = 43*211
9077 = 29*313
9079 = 7*1297
9083 = 31*293
9089 = 61*149
9091
9101 = 19*479
9103
9107 = 7*1301
9109
9113 = 13*701
9121 = 7*1303
9127
9131 = 23*397
9133
9137
9139 =13*19*37
9143 = 41*223
9149 = 7*1307
9151
9157
9161
9167 = 89*103
9169 = 53*173
9173
9179 = 67*137
9181
9187
9191 =7*13*101
9193 = 29*317
9197 = 17*541
9199
9203
9209
9211 = 61*151
9217 = 13*709
9221
9223 = 23*401
9227
9233 = 7*1319
9239
9241
9247 = 7*1321

9253 = 19*487
9257
9259 =47*197
9263 =59*157
9269 =13*23*31
9271 =73*127
9277
9281
9283
9287 = 37*251
9289 = 7*1327
9293
9299 = 17*547
9301 = 71*131
9307 = 41*227
9311
9313 = 67*139
9319
9323
9329 = 19*491
9331 = 7*31*43
9337
9341
9343
9347 = 13*719
9349
9353 = 47*199
9359 = 7*7*191
9367 =17*19*29
9371
9373 =7*13*103
9377
9379 = 83*113
9389 = 41*229
9391
9397
9401 = 7*17*79
9403
9407 = 23*409
9409 = 97*97
9413
9419
9421
9431
9433
9437
9439
9443 = 7*19*71
9451 = 13*727
9457 = 7*7*193
9461
9463
9467
9469 = 17*557
9473
9479
9481 = 19*499
9487 = 53*179
9491
9497
9499 = 7*23*59
9503 =13*17*43
9509 = 37*257
9511
9517 = 31*307
9521
9523 = 89*107
9527 = 7*1361
9529 = 13*733
9533
9539
9541 = 7*29*47
9547
9551
9553 = 41*233
9557 = 19*503
9563 = 73*131
9569 = 7*1367
9571 = 17*563
9577 = 61*157
9583 = 7*37*37
9587
9589 = 43*223
9593 = 53*181
9599 = 29*331
9601
9607 = 13*739
9611 = 7*1373
9613
9617 = 59*163
9619
9623
9629
9631
9637 = 23*419
9641 = 31*311
9643
9649
9653 = 7*7*197
9659 = 13*743
9661
9667 = 7*1381
9671 = 19*509
9673 = 17*569
9677
9679
9683 = 23*421
9689
9697
9701 = 89*109
9703 = 31*313
9707 = 17*571
9709 = 7*19*73
9719
9721
9727 = 71*137
9731 = 37*263
9733
9737 =7*13*107
9739
9743
9749
9751 = 7*7*199
9761 = 43*227
9763 = 13*751
9767
9769
9773 = 29*337
9781
9787
9791
9793 = 7*1399
9797 = 97*101
9799 = 41*239
9803
9809 = 17*577
9811
9817
9821 = 7*23*61
9827 = 31*317
9829
9833
9839
9841 = 13*757
9847 = 43*229
9851
9853 = 59*167
9857
9859
9863 = 7*1409
9869 = 71*139
9871
9877 = 7*17*83
9881 = 41*241
9883
9887
9893 = 13*761
9899 = 19*521
9901
9907
9913 = 23*431
9917 = 47*211
9919 =7*13*109
9923
9929
9931
9937 = 19*523
9941
9943 = 61*163
9947 =7*7*7*29
9949
9953 = 37*269
9959 = 23*433
9961 = 7*1423
9967
9971 =13*13*59
9973
9979 = 17*587
9983 = 67*149
9989 = 7*1427
9991 = 97*103
9997 = 13*769
10001 = 73*137
10003 = 7*1429
10007
10009
10013 =17*19*31
10019 = 43*233
10027 = 37*271
10031 = 7*1433
10033 = 79*127
10037
10039
10049 =13*773
10051 =19*23*23
10057 =89*113
10061
10063 = 29*347
10067
10069
10073 = 7*1439
10079
10081 = 17*593
10091
10093
10097 = 23*439
10099
10103
10111
10117 = 67*151
10121 = 29*349
10123 = 53*191
10127 =13*19*41
10129 = 7*1447
10133
10139
10141
10147 = 73*139
10151
10157 = 7*1451
10159
10163
10169
10171 = 7*1453
10177
10181
10183 = 17*599
10187 = 61*167
10189 = 23*443
10193
10199 = 7*31*47
10201 = 101*101
10207 = 59*173
10211
10213 = 7*1459
10217 = 17*601
10223
10229 = 53*193
10231 = 13*787
10237 = 29*353
10243
10247
10249 = 37*277
10253
10259
10261 = 31*331
10267
10271
10273
10277 = 43*239
10279 = 19*541
10283 =7*13*113
10289
10291 = 41*251
10297 = 7*1471
10301
10303
10309 =13*13*61
10313
10319 = 17*607
10321
10327 = 23*449
10331
10333
10337
10339 = 7*7*211
10343
10349 = 79*131
10357
10361 = 13*797
10363 = 43*241
10367 = 7*1481
10369
10379 = 97*107
10381 = 7*1483
10387 =13*17*47
10391
10393 = 19*547
10397 = 37*281
10399

10403 =101*103
10409 = 7*1487
10411 = 29*359
10421 = 17*613
10423 = 7*1489
10427
10429
10433
10441 = 53*197
10447 = 31*337
10451 = 7*1493
10453
10457
10459
10463
10469 =19*19*29
10471 =37*283
10477
10481 = 47*223
10487
10489 = 17*617
10493 = 7*1499
10499
10501
10507 = 7*19*79
10511 = 23*457
10513
10517 = 13*809
10519 = 67*157
10523 = 17*619
10529
10531
10537 = 41*257
10541 = 83*127
10543 = 13*811
10547 = 53*199
10553 = 61*173
10559
10561 = 59*179
10567
10573 = 97*109
10577 = 7*1511
10579 = 71*149
10583 = 19*557
10589
10591 = 7*17*89
10597
10601
10603 = 23*461
10607
10609 = 103*103
10613
10619 = 7*37*41
10621 =13*19*43
10627
10631
10633 =7*7*7*31
10639
10643 = 29*367
10649 = 23*463
10651
10657
10661 = 7*1523
10663
10667
10669 = 47*227
10673 = 13*821
10679 = 59*181
10687
10691

10693 =17*17*37
10697 =19*563
10699 =13*823
10709
10711
10717 = 7*1531
10721 = 71*151
10723
10727 = 17*631
10729
10733
10739
10741 = 23*467
10751 = 13*827
10753
10757 = 31*347
10759 = 7*29*53
10763 = 47*229
10771
10777 = 13*829
10781
10783 = 41*263
10787 = 7*23*67
10789
10793 = 43*251
10799
10801 = 7*1543
10807 = 101*107
10811 = 19*569
10817 = 29*373
10819 = 31*349
10823 = 79*137
10829 =7^2*13*17
10831
10837
10841 = 37*293
10843 = 7*1549
10847
10849 = 19*571
10853
10859
10861
10867
10871 = 7*1553
10873 = 83*131
10877 = 73*149
10883
10889
10891
10897 = 17*641
10903
10907 = 13*839
10909
10913 = 7*1559
10919 = 61*179
10921 = 67*163
10927 = 7*7*223
10931 = 17*643
10933 =13*29*29
10937
10939
10943 = 31*353
10949
10951 = 47*233
10957
10961 = 97*113
10963 = 19*577
10969 = 7*1567
10973
10979

10981 = 79*139
10987
10991 = 29*379
10993
10997 = 7*1571
10999 = 17*647
11003
11009 =101*109
11017 = 23*479
11021 =103*107
11023 = 73*151
11027
11029 = 41*269
11039 = 7*19*83
11041 = 61*181
11047
11051 = 43*257
11053 = 7*1579
11057
11059
11063 =13*23*37
11069
11071
11081 = 7*1583
11083
11087
11089 = 13*853
11093
11101 = 17*653
11107 = 29*383
11111 = 41*271
11113
11117
11119
11123 = 7*7*227
11129 = 31*359
11131
11137 = 7*37*43
11141 = 13*857
11147 = 71*157
11149
11153 = 19*587
11159
11161
11167 = 13*859
11171
11173
11177
11179 = 7*1597
11183 = 53*211
11189 = 67*167
11191 =19*19*31
11197
11201 = 23*487
11203 = 17*659
11207 = 7*1601
11213
11219 = 13*863
11221 = 7*7*229
11227 =
103*109
11233 = 47*239
11237 = 17*661
11239
11243
11249 = 7*1607
11251
11257
11261
11263 = 7*1609

11267 = 19*593
11269 = 59*191
11273
11279
11281 = 29*389
11287
11291 = 7*1613
11293 = 23*491
11299
11303 = 89*127
11309 = 43*263
11311
11317
11321
11323 =13*13*67
11327 = 47*241
11329
11333 = 7*1619
11339 =17*23*29
11347 = 7*1621
11351
11353
11357 = 41*277
11359 = 37*307
11369
11371 = 83*137
11377 = 31*367
11381 = 19*599
11383
11387 = 59*193
11389 = 7*1627
11393
11399
11401 = 13*877
11411
11413 = 101*113
11417 = 7*7*233
11419 = 19*601
11423
11431 = 7*23*71
11437
11441 = 17*673
11443
11447
11449 =107*107
11453 = 13*881
11459 = 7*1637
11461 = 73*157
11467
11471
11477 = 23*499
11479 = 13*883
11483
11489
11491
11497
11501 = 7*31*53
11503
11507 = 37*311
11509 = 17*677
11513 = 29*397
11519
11521 = 41*281
11527
11531 = 13*887
11533 = 19*607
11537 = 83*139
11543 = 7*17*97
11549
11551

11557 =7*13*127
11563 = 31*373
11567 = 43*269
11569 = 23*503
11573 = 71*163
11579
11581 = 37*313
11587
11591 = 67*173
11593
11597
11599 = 7*1657
11603 =41*283
11609 =13*19*47
11611 =17*683
11617
11621
11623 = 59*197
11629 = 29*401
11633
11639 =103*113
11641 = 7*1663
11647 = 19*613
11651 = 61*191
11653 = 43*271
11657
11659 = 89*131
11663 = 107*109
11669 = 7*1667
11677
11681
11683 = 7*1669
11687 =13*29*31
11689
11699
11701
11707 = 23*509
11711 = 7*7*239
11713 =13*17*53
11717
11719
11723 = 19*617
11729 = 37*317
11731
11741 = 59*199
11743
11747 = 17*691
11749 = 31*379
11753 = 7*23*73
11761 = 19*619
11767 = 7*41*41
11771 = 79*149
11773 = 61*193
11777
11779
11783
11789
11791 = 13*907
11797 = 47*251
11801
11807
11809 = 7*7*241
11813
11819 = 53*223
11821
11827
11831
11833
11837 = 7*19*89
11839
11843 =13*911
11849 =17*17*41
11851 = 7*1693
11857 =71*167
11861 =29*409
11863
11867
11873 = 31*383
11879 = 7*1697
11881 =109*109
11887
11893 = 7*1699
11897
11899 = 73*163
11903
11909
11911 = 43*277
11917 = 17*701
11921 =7*13*131
11923
11927
11929 = 79*151
11933
11939
11941
11947 = 13*919
11951 =17*19*37
11953
11959
11963 = 7*1709
11969
11971
11977 = 7*29*59
11981
11983 = 23*521
11987
11989 = 19*631
11993 = 67*179
11999 =13*13*71
12007
12011
12013 = 41*293
12017 = 61*197
12019 =7*17*101
12029 = 23*523
12031 = 53*227
12037
12041
12043
12047 = 7*1721
12049
12053 = 17*709
12059 = 31*389
12061 = 7*1723
12071
12073
12077 = 13*929
12079 = 47*257
12083 = 43*281
12091 =107*113
12097
12101
12103 =7^2*13*19
12107
12109
12113
12119
12121 =17*23*31
12127 =67*181
12131 = 7*1733
12137 =53*229
12139 =61*199
12143
12149
12151 = 29*419
12157
12161
12163
12167 = 23^3
12169 = 43*283
12173 = 7*37*47
12179 = 19*641
12181 = 13*937
12187 = 7*1741
12191 = 73*167
12193 = 89*137
12197
12203
12209 = 29*421
12211
12217 = 19*643
12223 = 17*719
12227
12229 = 7*1747
12233 = 13*941
12239
12241
12247 = 37*331
12251
12253
12257 =7*17*103
12259 =13*23*41
12263
12269
12271 = 7*1753
12277
12281
12283 = 71*173
12289
12293 = 19*647
12299 = 7*7*251
12301
12307 = 31*397
12311 = 13*947
12313 = 7*1759
12317 =109*113
12319 = 97*127
12323
12329
12337 =13*13*73
12341 = 7*41*43
12343
12347
12349 = 53*233
12359 = 17*727
12361 = 47*263
12367 = 83*149
12371 = 89*139
12373
12377
12379
12383 = 7*29*61
12389 = 13*953
12391
12401
12403 = 79*157
12407 = 19*653
12409
12413
12421
12427 =17*17*43
12431 =31*401
12433
12437
12439 = 7*1777
12443 = 23*541
12449 = 59*211
12451
12457
12461 = 17*733
12467 =7*13*137
12469 = 37*337
12473
12479
12481 = 7*1783
12487
12491
12493 =13*31*31
12497
12499 =29*431
12503
12509 = 7*1787
12511
12517
12521 = 19*659
12523 = 7*1789
12527
12533 = 83*151
12539
12541
12547
12553
12557 = 29*433
12559 = 19*661
12563 = 17*739
12569
12571 = 13*967
12577
12581 = 23*547
12583
12587 = 41*307
12589
12593 = 7*7*257
12599 = 43*293
12601
12607 = 7*1801
12611
12613
12619
12623 = 13*971
12629 = 73*173
12631 = 17*743
12637
12641
12643 = 47*269
12647
12649 =7*13*139
12653
12659
12667 = 53*239
12671
12673 =19*23*29
12677 = 7*1811
12679 =31*409
12689
12691 =7*7*7*37
12697
12701 = 13*977
12703

12707 = 97*131
12709 = 71*179
12713
12719 = 7*23*79
12721
12731 = 29*439
12733 =7*17*107
12737 = 47*271
12739
12743
12751 = 41*311
12757
12761 = 7*1823
12763
12767 = 17*751
12769 =113*113
12773 = 53*241
12779 = 13*983
12781
12787 = 19*673
12791
12797 = 67*191
12799
12803 = 7*31*59
12809
12811 = 23*557
12817 = 7*1831
12821
12823
12827 =101*127
12829
12833 = 41*313
12839 = 37*347
12841
12847 = 29*443
12851 = 71*181
12853
12857 =13*23*43
12863 = 19*677
12869 = 17*757
12871 = 61*211
12877 = 79*163
12883 = 13*991
12887 = 7*7*263
12889
12893
12899
12901 = 7*19*97
12907
12911
12913 = 37*349
12917
12919
12923
12929 = 7*1847
12931 = 67*193
12937 = 17*761
12941
12943 = 7*43*43
12949 = 23*563
12953
12959
12961 = 13*997
12967
12971 =7*17*109
12973
12977 = 19*683
12979
12983
12989 = 31*419
12997 = 41*317
13001
13003
13007
13009
13019 = 47*277
13021 = 29*449
13027 = 7*1861
13031 = 83*157
13033
13037
13039 =13*17*59
13043
13049
13051 = 31*421
13061 = 37*353
13063
13067 = 73*179
13069 = 7*1867
13073 = 17*769
13081 =103*127
13087 = 23*569
13091 =13*19*53
13093
13097 = 7*1871
13099
13103
13109
13111 = 7*1873
13117 = 13*1009
13121
13127
13129 = 19*691
13133 = 23*571
13139 = 7*1877
13141 = 17*773
13147
13151
13153 = 7*1879
13157 = 59*223
13159
13163
13169 = 13*1013
13171
13177
13181 = 7*7*269
13183
13187
13193 = 79*167
13199 = 67*197
13201 = 43*307
13207 = 47*281
13213 = 73*181
13217
13219
13223 = 7*1889
13229
13231 = 101*131
13237 = 7*31*61
13241
13243 =17*19*41
13247 =13*1019
13249
13253 = 29*457
13259
13261 = 89*149
13267
13271 = 23*577
13273 = 13*1021
13279 = 7*7*271
13283 = 37*359
13289 = 97*137
13291
13297
13301 = 47*283
13303 = 53*251
13307 = 7*1901
13309
13313
13319 = 19*701
13327
13331
13333 = 67*199
13337
13339
13349 = 7*1907
13351 =13*13*79
13357 =19*19*37
13361 =31*431
13363 = 7*23*83
13367
13369 = 29*461
13373 = 43*311
13379 = 17*787
13381
13391 = 7*1913
13393 = 59*227
13397
13399
13403 = 13*1031
13411
13417
13421
13423 = 31*433
13427 = 29*463
13429 = 13*1033
13433 =7*19*101
13439 = 89*151
13441
13447 =7*17*113
13451
13457
13459 = 43*313
13463
13469
13471 = 19*709
13477
13481 =13*17*61
13483 =97*139
13487
13489 = 7*41*47
13493 = 103*131
13499
13501 = 23*587
13507 = 13*1039
13511 = 59*229
13513
13517 = 7*1931
13523
13529 = 83*163
13531 = 7*1933
13537
13543 =29*467
13547 =19*23*31
13549 =17*797
13553
13559 =7*13*149
13561 = 71*191
13567
13571 = 41*331
13573 = 7*7*277
13577
13579 =37*367
13583 =17*17*47
13589 = 107*127
13591
13597
13601 = 7*29*67
13603 = 61*223
13609 = 31*439
13613
13619
13621 = 53*257
13627
13631 = 43*317
13633
13637 = 13*1049
13639 = 23*593
13643 = 7*1949
13649
13657 = 7*1951
13661 = 19*719
13663 = 13*1051
13667 = 79*173
13669
13679
13681
13687
13691
13693
13697
13699 =7*19*103
13703 = 71*193
13709
13711
13721
13723
13727 = 7*37*53
13729
13733 = 31*443
13741 =7*13*151
13747 = 59*233
13751
13753 = 17*809
13757
13759
13763
13769 = 7*7*281
13771 = 47*293
13777 = 23*599
13781
13787 = 17*811
13789
13793 = 13*1061
13799
13801 = 37*373
13807
13811 = 7*1973
13813 = 19*727
13817 = 41*337
13819 = 13*1063
13823 = 23*601
13829
13831
13837 =101*137
13841
13843 =109*127
13847 = 61*227
13853 = 7*1979
13859

13861 = 83*167
13867 = 7*7*283
13873
13877
13879
13883
13889 =17*19*43
13891 =29*479
13897 =13*1069
13901
13903
13907
13909 = 7*1987
13913
13919 = 31*449
13921
13927 = 19*733
13931
13933
13939 = 53*263
13943 = 73*191
13949 =13*29*37
13951 = 7*1993
13957 = 17*821
13961 = 23*607
13963
13967
13969 = 61*229
13973 = 89*157
13979 = 7*1997
13987 = 71*197
13991 = 17*823
13993 = 7*1999
13997
13999
14009
14011
14017 =107*131
14021 = 7*2003
14023 = 37*379
14027 =13*13*83
14029
14033
14039 =101*139
14041 = 19*739
14051
14053 =13*23*47
14057
14059 =17*827
14063 =7*7*7*41
14071
14077 = 7*2011
14081
14083
14087
14089 = 73*193
14093 = 17*829
14099 = 23*613
14101 = 59*239
14107
14111 =103*137
14117 = 19*743
14119 = 7*2017
14123 = 29*487
14129 = 71*199
14131 = 13*1087
14137 = 67*211
14141 = 79*179
14143
14147 = 7*43*47
14149
14153
14159
14161 = 7^2*17^2
14167 = 31*457
14171 = 37*383
14173
14177
14183 = 13*1091
14189 = 7*2027
14191 = 23*617
14197
14203 = 7*2029
14207
14209 = 13*1093
14213 = 61*233
14219 = 59*241
14221
14227 = 41*347
14231 =7*19*107
14233 = 43*331
14237 = 23*619
14239 = 29*491
14243
14249
14251
14257 = 53*269
14261 = 13*1097
14263 = 17*839
14269 = 19*751
14273 = 7*2039
14279 =109*131
14281
14287 =7*13*157
14291 = 31*461
14293
14297 =17*29*29
14299 =79*181
14303
14309 = 41*349
14317 =103*139
14321
14323
14327
14329 = 7*23*89
14339 = 13*1103
14341
14347
14351 =113*127
14353 = 31*463
14357 = 7*7*293
14359 = 83*173
14363 = 53*271
14369
14371 = 7*2053
14381 = 73*197
14383 = 19*757
14387
14389
14393 = 37*389
14401
14407
14411
14413 = 7*29*71
14417 = 13*1109
14419
14423
14429 = 47*307
14431
14437
14441 = 7*2063
14447
14449
14453 = 97*149
14459 = 19*761
14461
14467 =17*23*37
14471 = 29*499
14473 = 41*353
14477 = 31*467
14479
14483 = 7*2069
14489
14491 = 43*337
14497 =7*19*109
14501 = 17*853
14503
14507 = 89*163
14513 = 23*631
14519
14521 = 13*1117
14527 = 73*199
14533
14537
14539 = 7*31*67
14543
14549
14551
14557
14561
14563
14567 = 7*2081
14569 = 17*857
14573 =13*19*59
14579 = 61*239
14581 = 7*2083
14587 = 29*503
14591
14593
14599 = 13*1123
14603 = 17*859
14609 = 7*2087
14611 = 19*769
14617 = 47*311
14621
14623 = 7*2089
14627
14629
14633
14639
14647 = 97*151
14651 =7^2*13*23
14653
14657
14659 = 107*137
14669
14671 = 17*863
14677 = 13*1129
14681 = 53*277
14683
14687 = 19*773
14689 = 37*397
14693 = 7*2099
14699
14701 = 61*241
14711 = 47*313
14713
14717
14719 = 41*359
14723
14731
14737
14741
14743 = 23*641
14747
14749 = 7^3*43
14753
14759
14761 = 29*509
14767
14771
14777 = 7*2111
14779
14783
14789 = 23*643
14791 = 7*2113
14797
14801 =19*19*41
14803 = 113*131
14807 =13*17*67
14809 = 59*251
14813
14819 = 7*29*73
14821
14827
14831
14833 =7*13*163
14837 = 37*401
14843
14849 = 31*479
14851
14857 = 83*179
14863 = 89*167
14867
14869
14873 =107*139
14879
14881 = 23*647
14887
14891
14893 = 53*281
14897
14899 = 47*317
14903 = 7*2129
14909 = 17*877
14911 =13*31*37
14917 = 7*2131
14921 = 43*347
14923
14929
14933 = 109*137
14939
14941 = 67*223
14947
14951
14953 = 19*787
14957
14959 = 7*2137
14963 = 13*1151
14969
14977 = 17*881
14981 = 71*211
14983
14987 = 7*2141
14989 = 13*1153
14999 = 53*283
15001 = 7*2143
15007 = 43*349
15011 = 17*883
15013

15017
15019 = 23*653
15023 = 83*181
15029 =7*19*113
15031
15041 =13*13*89
15043 = 7*7*307
15047 = 41*367
15049 = 101*149
15053
15061
15067 =13*19*61
15071 = 7*2153
15073
15077
15079 = 17*887
15083
15089 = 79*191
15091
15097 = 31*487
15101
15107
15109 = 29*521
15113 =7*17*127
15119 = 13*1163
15121
15127 = 7*2161
15131
15133 = 37*409
15137
15139
15143 = 19*797
15149
15151 =109*139
15157 = 23*659
15161
15163 = 59*257
15167 = 29*523
15173
15179 = 43*353
15181 =17*19*47
15187
15193
15197 =7*13*167
15199
15203 = 23*661
15209 = 67*227
15211 = 7*41*53
15217
15221 = 31*491
15223 = 13*1171
15227
15229 = 97*157
15233
15239 = 7*7*311
15241
15247 = 79*193
15251 =101*151
15253 = 7*2179
15259
15263
15269
15271
15277
15281 = 7*37*59
15283 =17*29*31
15287
15289
15293 = 41*373
15299
15307
15311 = 61*251
15313
15317 =17*17*53
15319
15329
15331
15337 = 7*7*313
15341 =23*23*29
15343 = 67*229
15347 =103*149
15349
15353 = 13*1181
15359
15361
15371 = 19*809
15373
15377
15379 = $7*13^3$
15383
15391
15397 = 89*173
15401
15403 = 73*211
15407 = 7*31*71
15409 = 19*811
15413
15419 = 17*907
15421 = 7*2203
15427
15431 = 13*1187
15437 = 43*359
15439
15443
15449 = 7*2207
15451
15457 =13*29*41
15461
15463 = 7*47*47
15467
15469 = 31*499
15473
15479 = 23*673
15481 =
113*137
15487 = 17*911
15491 = 7*2213
15493
15497
15503 = 37*419
15509 = 13*1193
15511
15517 = 59*263
15523 =19*19*43
15527
15529 = 53*293
15533 = 7*7*317
15539 = 41*379
15541
15547 = 7*2221
15551
15553 =103*151
15557 = 47*331
15559
15563 = 79*197
15569
15571 = 23*677
15577 = 37*421
15581
15583
15589 =7*17*131
15593 = 31*503
15599 = 19*821
15601
15607
15611 = 67*233
15613 = 13*1201
15617 = 7*23*97
15619
15623 = 17*919
15629
15637 = 19*823
15641
15643
15647
15649
15659 = 7*2237
15661
15667
15671
15673 = 7*2239
15677 = 61*257
15679
15683
15689 = 29*541
15691 =13*17*71
15701 = 7*2243
15703 = 41*383
15707 =113*139
15709 = 23*683
15713 = 19*827
15721 = 79*199
15727
15731
15733
15737
15739
15743 =7*13*173
15749
15751 = 19*829
15757 = 7*2251
15761
15767
15769 = 13*1213
15773
15779 = 31*509
15781 = 43*367
15787
15791
15793 = 17*929
15797
15799 = 7*37*61
15803
15809
15811 = 97*163
15817
15821 = 13*1217
15823
15827 =7^2*17*19
15833 = 71*223
15839 = 47*337
15841 = 7*31*73
15847 =13*23*53
15853 = 83*191
15857 =101*157
15859
15863 = 29*547
15869 = 7*2267
15871 = 59*269
15877
15881
15883 = 7*2269
15887
15889
15893 = 23*691
15899 = 13*1223
15901
15907
15911 = 7*2273
15913
15919
15923
15929 = 17*937
15931 = 89*179
15937
15941 = 19*839
15943 =107*149
15947 = 37*431
15949 = 41*389
15953 = 7*43*53
15959
15967 = 7*2281
15971
15973
15977 = 13*1229
15979 =19*29*29
15989 = 59*271
15991
15997 = 17*941
16001
16003 = 13*1231
16007
16009 = 7*2287
16013 = 67*239
16019 = 83*193
16021 = 37*433
16031 =17*23*41
16033
16037 = 7*29*79
16039 = 43*373
16043 = 61*263
16051 = 7*2293
16057
16061
16063
16067
16069
16073
16079 = 7*2297
16081 = 13*1237
16087
16091
16097
16099 = 17*947
16103
16109 = 89*181
16111
16117 = 71*227
16121 =7*7*7*47
16123 = 23*701
16127
16129 =127*127
16133 =13*17*73
16139
16141
16147 = 67*241
16151 = 31*521
16153 = 29*557
16157 =107*151
16163 = 7*2309

16169 =19*23*37
16171 =103*157
16177 = 7*2311
16183
16187
16189
16193
16199 = 97*167
16201 = 17*953
16207 = 19*853
16211 =13*29*43
16213 = 31*523
16217
16219 = 7*7*331
16223
16229
16231
16237 = 13*1249
16241 = 109*149
16243 = 37*439
16249
16253
16259 = 71*229
16261 =7*23*101
16267
16271 = 53*307
16273
16277 = 41*397
16279 = 73*223
16283 = 19*857
16289 =7*13*179
16297 = 43*379
16301
16303 =7*17*137
16307 = 23*709
16309 = 47*347
16319
16321 = 19*859
16327 = 29*563
16331 = 7*2333
16333
16337 =17*31*31
16339
16343 = 59*277
16349
16351 = 83*197
16361
16363
16367 = 13*1259
16369
16373 = 7*2339
16381
16387 = 7*2341
16391 = 37*443
16393 =13*13*97
16397 =19*863
16399 =23*23*31
16403 = 47*349
16409 = 61*269
16411
16417
16421
16427
16429 = 7*2347
16433
16439 = 17*967
16441 = 41*401
16447
16451
16453
16457 = 7*2351
16459 =109*151
16463 =101*163
16469 = 43*383
16471 =7*13*181
16477
16481
16483 = 53*311
16487
16493
16499 = 7*2357
16501 = 29*569
16507 = 17*971
16513 = 7*7*337
16517 = 83*199
16519
16523 =13*31*41
16529
16531 = 61*271
16537 = 23*719
16541 =7*17*139
16543 = 71*233
16547
16549 =13*19*67
16553
16559 = 29*571
16561
16567
16571 = 73*227
16573
16579 = 59*281
16583 =7*23*103
16589 = 53*313
16591 = 47*353
16597 = 7*2371
16601 = 13*1277
16603
16607
16609 = 17*977
16613 = 37*449
16619
16627 = 13*1279
16631
16633
16637 =127*131
16639 = 7*2377
16649
16651
16657
16661
16663 = 19*877
16667 = 7*2381
16669 = 79*211
16673
16679 = 13*1283
16681 = 7*2383
16691
16693
16697 = 59*283
16699
16703
16711 = 17*983
16717 = 73*229
16721 = 23*727
16723 = 7*2389
16727 = 43*389
16729
16733 = 29*577
16739 = 19*881
16741
16747
16751 = 7*2393
16757 = 13*1289
16759
16763
16769 = 41*409
16771 = 31*541
16777 = 19*883
16781 = 97*173
16783 = 13*1291
16787
16789 =103*163
16793 = 7*2399
16799 =107*157
16801 = 53*317
16807 = 7^5
16811
16813 =17*23*43
16817 =67*251
16823
16829
16831
16837 =113*149
16843
16847 = 17*991
16849 = 7*29*83
16853 = 19*887
16859 = 23*733
16861 = 13*1297
16867 =101*167
16871
16873 = 47*359
16877 = 7*2411
16879
16883
16889
16891 =7*19*127
16897 = 61*277
16901
16903
16909 = 37*457
16913 = 13*1301
16919 = 7*2417
16921
16927
16931
16933 = 7*41*59
16937
16939 = 13*1303
16943
16949 = 17*997
16957 = 31*547
16961 = 7*2423
16963
16967 =19*19*47
16969 =71*239
16979
16981
16987
16991 = 13*1307
16993
16997 = 23*739
16999 = 89*191
17003 = 7*7*347
17009 = 73*233
17011
17021
17023 = 29*587
17027
17029
17033
17041
17047
17051 =17*17*59
17053
17057 = 37*461
17059 = 7*2437
17063 =113*151
17069 = 13^2*101
17071 = 43*397
17077
17081 =19*29*31
17087 = 7*2441
17089 = 23*743
17093
17099
17101 = 7*7*349
17107
17111 = 71*241
17113 =109*157
17117
17119 =17*19*53
17123
17129 = 7*2447
17131 = 37*463
17137
17141 = 61*281
17143 = 7*31*79
17147 = 13*1319
17153 = 17*1009
17159
17161 =131*131
17167
17173 = 13*1321
17177 = 89*193
17179 = 41*419
17183
17189
17191
17197 = 29*593
17201 =103*167
17203
17207
17209
17213 = 7*2459
17219 = 67*257
17221 = 17*1013
17227 =7*23*107
17231
17233 = 19*907
17239
17243 = 43*401
17249 = 47*367
17251 = 13*1327
17257
17261 = 41*421
17263 = 61*283
17267 = 31*557
17269 = 7*2467
17273 = 23*751
17279 = 37*467
17287 = 59*293
17291
17293
17297 = 7*7*353
17299
17309 = 19*911
17311 = 7*2473
17317

17321
17323 = 17*1019
17327
17329 =13*31*43
17333
17339 = 7*2477
17341
17351
17353 = 7*37*67
17357 = 17*1021
17359
17363 = 97*179
17371 = 29*599
17377
17381 =7*13*191
17383
17387
17389
17393
17399 =127*137
17401
17407 = 13^2*103
17411 = 23*757
17417
17419
17423 =7*19*131
17429 = 29*601
17431
17437 = 7*47*53
17441 =107*163
17443
17447 = 73*239
17449
17453 = 31*563
17459 =13*17*79
17461 =19*919
17467
17471
17473 =101*173
17477
17483
17489
17491
17497
17503 = 23*761
17507 = 7*41*61
17509
17513 = 83*211
17519
17521 = 7*2503
17527 = 17*1031
17531 = 47*373
17533 = 89*197
17537 =13*19*71
17539
17543 = 53*331
17549 =7*23*109
17551
17557 = 97*181
17561 = 17*1033
17563 =7*13*193
17569
17573
17579
17581
17587 = 43*409
17591 = 7*7*359
17593 = 73*241
17597
17599
17603 = 29*607
17609
17617 = 79*223
17621 = 67*263
17623
17627
17629 =17*17*61
17639 =31*569
17641 =13*23*59
17647 = 7*2521
17651 = 19*929
17653 =127*139
17657
17659
17663 = 17*1039
17669
17671 = 41*431
17681
17683
17687 = 23*769
17689 = 7^2*19^2
17693 = 13*1361
17701 = 31*571
17707
17711 = 89*199
17713
17717 = 7*2531
17719 =13*29*47
17723 = 37*479
17729
17731 =7*17*149
17737
17741 =113*157
17747
17749
17753 = 41*433
17759 = 7*43*59
17761
17767 =109*163
17771 = 13*1367
17773 = 7*2539
17777 = 29*613
17779 = 23*773
17783
17789
17791
17797 =13*37*37
17801 = 7*2543
17803 = 19*937
17807
17813 = 47*379
17819 =
103*173
17821 = 71*251
17827
17833 = 17*1049
17837
17839
17843 = 7*2549
17849 = 13*1373
17851
17857 = 7*2551
17861 = 53*337
17863
17867 = 17*1051
17869 =107*167
17873 = 61*293
17879 = 19*941
17881
17887 = 31*577
17891
17893 = 29*617
17899 = 7*2557
17903
17909
17911
17917 =19*23*41
17921
17923
17927 =7*13*197
17929
17933 =79*227
17939
17947 =131*137
17951 = 29*619
17953 = 13*1381
17957
17959
17969 =7*17*151
17971
17977
17981
17983 = 7*7*367
17987
17989
17993 = 19*947
17999 = 41*439
18001 = 47*383
18011 = 7*31*83
18013
18017 = 43*419
18019 = 37*487
18023 = 67*269
18031 =13*19*73
18037 = 17*1061
18041
18043
18047
18049
18053 = 7*2579
18059
18061
18067 = 7*29*89
18071 =17*1063
18077
18079 =101*179
18083 = 13^2*107
18089
18091 = 79*229
18097
18101 = 23*787
18103 = 43*421
18107 = 19*953
18109 =7*13*199
18113 = 59*307
18119
18121
18127
18131
18133
18137 = 7*2591
18143
18149
18151 = 7*2593
18157 = 67*271
18163 = 41*443
18167 = 37*491
18169
18173 = 17*1069
18179 = 7^3*53
18181
18187 = 13*1399
18191
18193 =7*23*113
18197 = 31*587
18199
18203 =109*167
18209 =131*139
18211
18217
18221 =7*19*137
18223
18229
18233
18239 =13*23*61
18241 =17*29*37
18247 =71*257
18251
18253
18257
18259 =19*31*31
18263 = 7*2609
18269
18277 = 7*7*373
18281 =101*181
18283 = 47*389
18287
18289
18299 = 29*631
18301
18307
18311
18313
18317 = 13*1409
18319 = 7*2617
18323 = 73*251
18329
18331 = 23*797
18341
18343 =13*17*83
18347 = 7*2621
18349 = 59*311
18353
18361 = 7*43*61
18367
18371
18373 =19*967
18377 =17*23*47
18379
18383 = 31*593
18389 = 7*37*71
18391 = 53*347
18397
18401
18407 = 79*233
18409 = 41*449
18413
18419 =113*163
18421 =13^2*109
18427
18431 = 7*2633
18433
18437 =103*179
18439
18443
18449 = 19*971
18451
18457
18461
18463 = 37*499

18467 = 59*313
18473 =7^2*13*29
18479 = 17*1087
18481
18487 =7*19*139
18493
18497 = 53*349
18499 = 13*1423
18503
18509 = 83*223
18511 =107*173
18517
18521
18523
18527 = 97*191
18529 = 7*2647
18533 = 43*431
18539
18541
18547 = 17*1091
18551 = 13*1427
18553
18559 = 67*277
18563 = 19*977
18569 = 31*599
18571 = 7*7*379
18577 = 13*1429
18581 = 17*1093
18583
18587
18589 = 29*641
18593
18599 = 7*2657
18607 = 23*809
18611 = 37*503
18613 = 7*2659
18617
18619 = 43*433
18629 = 13*1433
18631 = 31*601
18637
18641 = 7*2663
18643 =103*181
18647 = 29*643
18649 = 17*1097
18653 = 23*811
18659 = 47*397
18661
18671
18673 = 71*263
18677 = 19*983
18679
18683 =7*17*157
18691
18697 = 7*2671
18701
18703 = 59*317
18707 = 13*1439
18709 = 53*353
18713
18719
18721 = 97*193
18727 = 61*307
18731
18737 = 41*457
18739 = 7*2677
18743
18749
18751 = 17*1103
18757
18761 = 73*257
18763 = 29*647
18767 = 7*7*383
18769 =137*137
18773
18779 = 89*211
18781 = 7*2683
18787
18791 =19*23*43
18793
18797
18803
18809 = 7*2687
18811 = 13*1447
18817 = 31*607
18823 = 7*2689
18827 = 67*281
18829 = 19*991
18833 = 37*509
18839
18841 = 83*227
18847 = 47*401
18851 = 7*2693
18853 = 17*1109
18857 =109*173
18859
18863 = 13*1451
18869
18871 =113*167
18877 = 43*439
18881 = 79*239
18883 = 23*821
18889 = 13*1453
18893 = 7*2699
18899
18901 = 41*461
18907 = 7*37*73
18911
18913
18917
18919
18923 =127*149
18929 = 23*823
18937 = 29*653
18941 =13*31*47
18943 = 19*997
18947
18949 = 7*2707
18959
18961 = 67*283
18967 = 13*1459
18971 = 61*311
18973
18977 = 7*2711
18979
18983 = 41*463
18989 = 17*1117
18991 = 7*2713
19001
19003 = 31*613
19007 = 83*229
19009
19013
19021 = 23*827
19027 = 53*359
19031
19033 = 7*2719
19037
19039 = 79*241
19043 =137*139
19049 = 43*443
19051
19057 =17*19*59
19061 = 7*7*389
19067 =23*829
19069
19073
19079
19081
19087
19091 = 17*1123
19093 = 61*313
19097 = 13^2*113
19099 = 71*269
19103 = 7*2729
19109 = 97*197
19111 = 29*659
19117 = 7*2731
19121
19123 = 13*1471
19127 = 31*617
19133 =19*19*53
19139
19141
19147 = 41*467
19153 =107*179
19157
19159 =7^2*17*23
19163
19169 = 29*661
19171 = 19*1009
19177 =127*151
19181
19183
19187 = 7*2741
19189 = 31*619
19193 = 17*1129
19199 = 73*263
19201 =7*13*211
19207
19211
19213
19219
19223 = 47*409
19229 =7*41*67*
19231
19237
19241 = 71*271
19243 = 7*2749
19247 = 19*1013
19249
19253 = 13*1481
19259
19267
19271 = 7*2753
19273
19277 = 37*521
19279 = 13*1483
19289
19291 =101*191
19297 = 23*839
19301
19303 = 97*199
19307 = 43*449
19309
19313 = 7*31*89
19319
19321 =139*139
19331 = 13*1487
19333
19337 = 61*317
19339 = 83*233
19343 =23*29*29
19351 = 37*523
19357 = 13*1489
19361 = 19*1019
19363 =17*17*67
19367 =107*181
19369 = 7*2767
19373
19379
19381
19387
19391
19397 =7*17*163
19399 = 19*1021
19403
19409 = 13*1493
19411 = 7*47*59
19417
19421
19423
19427
19429
19433
19439 = 7*2777
19441
19447
19451 = 53*367
19453 = 7*7*397
19457
19463
19469
19471
19477
19483
19487 = 13*1499
19489
19493 =101*193
19499 =17*31*37
19501
19507
19511 =109*179
19513 =13*19*79
19517 = 29*673
19519 =131*149
19523 = 7*2789
19529 = 59*331
19531
19537 = 7*2791
19541
19543
19549 =113*173
19553
19559
19561 = 31*631
19567 = 17*1151
19571
19573 =23*23*37
19577
19579 = 7*2797
19583
19589 = 19*1031
19597
19601 = 17*1153
19603
19607 = 7*2801
19609
19619 = 23*853
19621 = 7*2803

19627 = 19*1033
19631 = 67*293
19633 = 29*677
19637 = 73*269
19639 = 41*479
19643 = 13*1511
19649 = 7*7*401
19651 = 43*457
19661
19663 = 7*53*53
19667 = 71*277
19669 =13*17*89
19673 =103*191
19681
19687
19691 = 7*29*97
19693 =47*419
19697
19699
19703 =17*19*61
19709
19711 = 23*857
19717
19721 =13*37*41
19727
19729 =
109*181
19733 = 7*2819
19739
19741 = 19*1039
19747 =7^2*13*31
19751
19753
19757 = 23*859
19759
19763
19769 = 53*373
19771 = 17*1163
19777
19781 =131*151
19783 = 73*271
19787 = 47*421
19793
19799 = 13*1523
19801
19807 = 29*683
19813
19817 =7*19*149
19819
19823 = 43*461
19829 = 79*251
19831 = 7*2833
19837 = 83*239
19841
19843
19847 = 89*223
19849 = 23*863
19853
19859 = 7*2837
19861
19867
19871 = 31*641
19873 =7*17*167
19879 =103*193
19883 = 59*337
19889
19891
19897 =101*197
19901 = 7*2843
19903 = 13*1531
19907 = 17*1171
19909 = 43*463
19913
19919
19927
19931 = 19*1049
19933 = 31*643
19937
19939 =127*157
19949
19951 = 71*281
19957 = 7*2851
19961
19963
19967 = 41*487
19969 = 19*1051
19973
19979
19981 =13*29*53
19991
19993
19997
19999 = 7*2857
20003 = 83*241
20011
20017 = 37*541
20021
20023
20027 = 7*2861
20029
20033 =13*23*67
20039 =29*691
20041 = 7*7*409
20047
20051
20057 = 31*647
20059 = 13*1543
20063
20069 = 7*47*61
20071
20077 = 17*1181
20081 = 43*467
20083 =7*19*151
20087 = 53*379
20089
20093 = 71*283
20099 =101*199
20101
20107
20111 =7*13^2*17
20113
20117
20123
20129
20131 = 41*491
20137 = 13*1549
20143
20147
20149
20153 = 7*2879
20159 = 19*1061
20161
20167 = 7*43*67
20171 = 23*877
20173
20177
20179 = 17*1187
20183
20189 = 13*1553
20191 = 61*331
20197 = 19*1063
20201
20203 = 89*227
20209 = 7*2887
20213 =17*29*41
20219
20221 = 73*277
20227 =113*179
20231
20233
20237 =7*7*7*59
20239 = 37*547
20243 = 31*653
20249
20257 = 47*431
20261
20263 = 23*881
20267 = 13*1559
20269
20279 = 7*2897
20281 = 17*1193
20287
20291 =103*197
20293 =7*13*223
20297
20299 = 53*383
20303 = 79*257
20309 = 23*883
20311 = 19*1069
20321 = 7*2903
20323
20327
20329 = 29*701
20333
20341
20347
20351 = 47*433
20353
20357
20359
20363 = 7*2909
20369
20371 =13*1567
20377 = 7*41*71
20381 =89*229
20387 =19*29*37
20389
20393
20399
20401 = 23*887
20407
20411
20413 =137*149
20417 = 17*1201
20419 = 7*2917
20423 = 13*1571
20429 = 31*659
20431
20437 =107*191
20441
20443
20447 =7*23*127
20453 =113*181
20459 = 41*499
20461 = 7*37*79
20467 = 97*211
20473 = 59*347
20477
20479
20483
20489 = 7*2927
20491 = 31*661
20497 =103*199
20501 =13*19*83
20503 =7*29*101
20507
20509
20513 =73*281
20519 =17*17*71
20521
20527 =13*1579
20531 = 7*7*419
20533
20539 =19*23*47
20543
20549
20551
20557 = 61*337
20561 = 29*709
20563
20567 =131*157
20569 = 67*307
20573 = 7*2939
20579 = 13*1583
20587 =7*17*173
20591 = 59*349
20593
20597 = 43*479
20599
20609 = 37*557
20611
20617 = 53*389
20621 = 17*1213
20623 = 41*503
20627
20629 = 7*7*421
20633 = 47*439
20639
20641
20651 =107*193
20653 = 19*1087
20657 =7*13*227
20659 = 73*283
20663
20671 = 7*2953
20677 =23*29*31
20681
20683 =13*37*43
20687 =137*151
20689 = 17*1217
20693
20699 = 7*2957
20701 =127*163
20707
20711 =139*149
20717
20719
20723 =17*23*53
20729 = 19*1091
20731
20737 = 89*233
20741 = 7*2963
20743
20747
20749
20753
20759
20761 = 13*1597
20767 = 19*1093
20771

20773
20777 = 79*263
20783 = 7*2969
20789
20791 = 17*1223
20797 = 7*2971
20803 = 71*293
20807
20809
20813 = 13*1601
20819 =109*191
20821 = 47*443
20827 = 59*353
20831 = 37*563
20833 = 83*251
20837 = 67*311
20839 =7*13*229
20843 = 19*1097
20849
20851 = 29*719
20857
20861 = 23*907
20863 = 31*673
20869 = 41*509
20873
20879
20881 =7*19*157
20887
20891 = 13*1607
20893 = 17*1229
20897
20899
20903
20909 =7*29*103
20917 = 13*1609
20921
20923 =7*7*7*61
20927 = 17*1231
20929
20939
20941 = 43*487
20947
20951 = 7*41*73
20953 = 23*911
20957 = 19*1103
20959
20963
20969 = 13*1613
20971 = 67*313
20981
20983
20987 = 31*677
20989 =139*151
20993 = 7*2999
21001
21007 = 7*3001
21011
21013
21017
21019
21023
21029 = 17*1237
21031
21037 =109*193
21041 = 53*397
21047 = 13*1619
21049 = 7*31*97
21053 = 37*569
21059
21061
21067
21071 = 19*1109
21073 = 13*1621
21077 = 7*3011
21079 =107*197
21083 = 29*727
21089
21091 =7*23*131
21097 =17*17*73
21101
21103 = 47*449
21107
21113 = 43*491
21119 = 7*7*431
21121
21127 = 37*571
21133 = 7*3019
21137 = 23*919
21139
21143
21149
21151 = 13*1627
21157
21161 = 7*3023
21163
21167 = 61*347
21169
21173 = 31*683
21179
21181 = 59*359
21187
21191
21193
21199 =17*29*43
21203 =7*13*233
21209 = 127*167
21211
21217 = 7*7*433
21221
21223 = 19*1117
21227
21229 =13*23*71
21233 = 17*1249
21239 = 67*317
21247
21251 = 79*269
21253 = 53*401
21257 = 29*733
21259 = 7*3037
21269
21271 = 89*239
21277
21281 = 13*1637
21283
21287 = 7*3041
21289 = 61*349
21293 =107*199
21299 =19*19*59
21301 =7*17*179
21311 =101*211
21313
21317
21319
21323
21331 = 83*257
21337 = 19*1123
21341
21343 = 7*3049
21347
21349 = 37*577
21353 =131*163
21359 =13*31*53
21361 = 41*521
21367 = 23*929
21371 = 7*43*71
21377
21379
21383
21389 = 73*293
21391
21397
21401
21403 = 17*1259
21407
21409 = 79*271
21413 =7^2*19*23
21419
21421 = 31*691
21427 = 7*3061
21431 = 29*739
21433
21437 =13*17*97
21443 = 41*523
21449 = 89*241
21451 = 19*1129
21457 = 43*499
21463 = 13^2*127
21467
21469 = 7*3067
21473 =109*197
21479 = 47*457
21481
21487
21491
21493
21497 = 7*37*83
21499
21503
21509 =137*157
21511 = 7*7*439
21517
21521
21523
21529
21533 = 61*353
21539 =7*17*181
21541 = 13*1657
21547 = 29*743
21551 = 23*937
21553 = 7*3079
21557
21559
21563
21569
21577
21581 = 7*3083
21583 =113*191
21587
21589
21599
21601
21607 =17*31*41
21611
21613
21617
21619 = 13*1663
21623 = 7*3089
21629 = 43*503
21631 = 97*223
21641 =17*19*67
21643 = 23*941
21647
21649
21653 = 59*367
21661
21667 = 47*461
21671 = 13*1667
21673
21677 = 53*409
21679 =7*19*163
21683
21689 =23*23*41
21691 =109*199
21697 = 13*1669
21701
21707 = 7*7*443
21709 = 17*1277
21713
21719 = 37*587
21721 =7*29*107
21727
21731 = 31*701
21733 =103*211
21737
21739
21743 = 17*1279
21749 =7*13*239
21751
21757
21761 = 47*463
21763 = 7*3109
21767
21773
21779 = 29*751
21781 = 23*947
21787
21793 =19*31*37
21797 = 71*307
21799
21803
21809 =113*193
21811 = 17*1283
21817
21821
21823 =139*157
21827 =13*23*73
21829 = 83*263
21833 = 7*3119
21839
21841
21847 = 7*3121
21851
21853 =13*41*41
21859
21863
21869 = 19*1151
21871
21877 =131*167
21881
21883 = 79*277
21887 = 43*509
21889 = 7*53*59
21893
21899 = 61*359
21907 = 19*1153
21911
21913 = 17*1289
21917 =7*31*101
21919 = 23*953
21929

21931 =7*13*241
21937
21941 = 37*593
21943
21947 = 17*1291
21949 = 47*467
21953 = 29*757
21959 = 7*3137
21961
21971 =127*173
21973 = 7*43*73
21977
21979 = 31*709
21983 =13*19*89
21991
21997
22001 = 7*7*449
22003
22007 = 59*373
22009 = 13*1693
22013
22019 = 97*227
22021 =19*19*61
22027
22031
22037
22039
22043 = 7*47*67
22049 = 17*1297
22051
22057 =7*23*137
22061 = 13*1697
22063
22067
22069 = 29*761
22073
22079
22081 = 71*311
22087 = 13*1699
22091
22093
22097 = 19*1163
22103 =23*31*31
22109
22111
22117 = 17*1301
22123
22127 =7*29*109
22129
22133
22139 = 13^2*131
22141 = 7*3163
22147
22151 = 17*1303
22153
22157
22159
22163 = 37*599
22169 = 7*3167
22171
22177 = 67*331
22181 = 41*541
22183 = 7*3169
22189
22193
22199 = 79*281
22201 =149*149
22207 = 53*419
22211 =7*19*167
22213 = 97*229
22217 = 13*1709
22219 = 17*1307
22223 = 71*313
22229
22237 = 37*601
22241 = 23*967
22243 =13*29*59
22247
22249 = 19*1171
22259
22261 =113*197
22267 = 7*3181
22271
22273
22277
22279
22283
22289 = 31*719
22291
22301 = 29*769
22303
22307
22309 = 7*3187
22313 = 53*421
22321=13*17*101
22327 = 83*269
22331 =137*163
22333 = 23*971
22337 = 7*3191
22339 = 89*251
22343
22349
22351 =7*31*103
22357 = 79*283
22361 = 59*379
22367
22369
22373 = 13*1721
22379 =7*23*139
22381
22387 = 61*367
22391
22393 = 7*7*457
22397
22399 = 13*1723
22403 = 43*521
22409
22411 = 73*307
22417 = 29*773
22421 = 7*3203
22423 = 17*1319
22427 = 41*547
22433
22439 = 19*1181
22441
22447
22453
22457 = 17*1321
22459 = 37*607
22463 = 7*3209
22469
22471 = 23*977
22477 =7*13^2*19
22481
22483
22487 =113*199
22489 = 43*523
22493 = 83*271
22499 =149*151
22501
22507 = 71*317
22511
22513 = 47*479
22519 = 7*3217
22523 =
101*223
22529 = 13*1733
22531
22537 = 31*727
22541
22543
22547 = 7*3221
22549
22553 = 19*1187
22559 = 17*1327
22567
22571
22573
22577 =107*211
22579 = 67*337
22589 = 7*7*461
22591 =19*29*41
22597 = 59*383
22601 = 97*233
22603 = 7*3229
22607 =13*37*47
22609 = 23*983
22613
22619
22621
22631 = 7*53*61
22633 = 13*1741
22637
22639
22643
22651
22657 =139*163
22661 =17*31*43
22663 =131*173
22667 = 19*1193
22669
22673 = 7*41*79
22679
22681 = 37*613
22687 = 7*7*463
22691
22697
22699
22703 = 73*311
22709
22711 = 13*1747
22717
22721
22723 = 31*733
22727
22729 =7*17*191
22733 = 127*179
22739
22741
22747 =23*23*43
22751
22753 = 61*373
22757 = 7*3251
22763=13*17*103
22769
22771 = 7*3253
22777
22783
22787
22789 = 13*1753
22793 = 23*991
22799 = 7*3257
22801 =151*151
22807
22811
22813 = 7*3259
22817
22819 = 19*1201
22823 = 29*787
22829 = 37*617
22831 =17*17*79
22837 = 41*557
22841 =7*13*251
22843 = 53*431
22849 = 73*313
22853
22859
22861
22867 = 13*1759
22871
22873 = 89*257
22877
22879 =137*167
22883 = 7*7*467
22889 = 47*487
22897 = 7*3271
22901
22903 = 37*619
22907
22909 = 31*739
22919 =13*41*43
22921
22927 =101*227
22931 = 23*997
22933 =17*19*71
22937
22939 =7*29*113
22943
22949 = 53*433
22951 = 59*389
22961
22963
22967 =7*17*193
22969 =103*223
22973
22981 = 7^3*67
22987 =127*181
22991 = 83*277
22993
22997 =13*29*61
22999 =109*211
23003
23009 =7*19*173
23011
23017
23021
23027
23029
23033 = 31*743
23039
23041
23047 = 19*1213
23051 = 7*37*89
23053
23057
23059
23063
23069 =17*23*59
23071
23077 = 47*491

23081
23083 = 41*563
23087
23093 = 7*3299
23099
23101 = 13*1777
23107 = 7*3301
23113 = 29*797
23117
23119 = 61*379
23123 = 19*1217
23129 =101*229
23131
23137 = 17*1361
23141 = 73*317
23143
23147 = 79*293
23149 = 7*3307
23153 = 13^2*137
23159
23161 =19*23*53
23167
23171 =17*29*47
23173
23179 = 13*1783
23183 = 97*239
23189
23191 = 7*3313
23197
23201
23203
23207 = 23*1009
23209
23213 =139*167
23219 =7*31*107
23227
23231 = 13*1787
23233 = 7*3319
23237 = 19*1223
23239 = 17*1367
23249 = 67*347
23251
23257 = 13*1789
23261 = 7*3323
23263 = 43*541
23267 = 53*439
23269
23273 =17*37*37
23279
23281 = 31*751
23291
23293
23297
23299 = 23*1013
23303 = 7*3329
23311
23317 = 7*3331
23321
23323 = 83*281
23327
23329 = 41*569
23333
23339
23341 = 17*1373
23347 = 37*631
23351 = 19*1229
23357
23359 = 7*47*71
23363 = 61*383
23369

23371
23377 = 97*241
23381 =103*227
23383 = 67*349
23387 =7*13*257
23389 = 19*1231
23393 =149*157
23399
23401 = 7*3343
23407 = 89*263
23411 = 41*571
23413 = 13*1801
23417
23423 = 59*397
23429 = 7*3347
23431
23437 = 23*1019
23443 =7*17*197
23447
23449 =131*179
23453 = 47*499
23459
23461 = 29*809
23467 = 31*757
23471 = 7*7*479
23473
23477 = 17*1381
23479 = 53*443
23483 = 23*1021
23489 = 83*283
23491 = 13^2*139
23497
23501 = 71*331
23503 = 19*1237
23509
23513 = 7*3359
23519 = 29*811
23521 = 43*547
23527 = 7*3361
23531
23533 =101*233
23537
23539
23543 = 13*1811
23549
23557
23561
23563
23567
23569 =7^2*13*37
23579 =17*19*73
23581
23587 =103*229
23591 = 31*761
23593
23597 = 7*3371
23599
23603
23609
23611 = 7*3373
23621 =13*23*79
23623
23627
23629
23633
23641 = 47*503
23647=13*17*107
23651 = 67*353
23653 =7*31*109
23657 = 41*577

23659 = 59*401
23663
23669
23671
23677
23681 =7*17*199
23687
23689
23693 =19*29*43
23699 = 13*1823
23701 =137*173
23707 =151*157
23711 =131*181
23713 = 23*1031
23717 = 37*641
23719
23723 = 7*3389
23729 = 61*389
23731 = 19*1249
23737 = 7*3391
23741
23743
23747
23753
23759 = 23*1033
23761
23767
23773
23777 =13*31*59
23779 = 7*43*79
23783 = 17*1399
23789
23791 = 37*643
23797 = 53*449
23801
23803 = 13*1831
23807 =7*19*179
23809 = 29*821
23813
23819
23821 = 7*41*83
23827
23831
23833
23839 = 31*769
23843 =113*211
23849 = 7*3407
23851 =17*23*61
23857
23861 =107*223
23863 = 7*7*487
23867 = 29*823
23869
23873
23879
23887
23891 = 7*3413
23893
23897 = 23*1039
23899
23909
23911
23917
23921 = 19*1259
23923 = 47*509
23927 = 71*337
23929
23933 =7*13*263
23939 = 37*647
23941 = 89*269

23951 = 43*557
23953 = 17*1409
23957
23959 =13*19*97
23963 = 31*773
23971
23977
23981
23983 = 29*827
23987 =17*17*83
23989 =7*23*149
23993
23999 =103*233
24001
24007
24011 = 13*1847
24017 = 7*47*73
24019
24023
24029
24031 = 7*3433
24037 =13*43*43
24041 = 29*829
24043
24047 =139*173
24049
24053 = 67*359
24059 = 7*7*491
24061
24067 = 41*587
24071
24073 =7*19*181
24077
24083
24089=13*17*109
24091
24097
24103
24107
24109
24113
24119 = 89*271
24121
24127 = 23*1049
24131 = 59*409
24133
24137
24139 =101*239
24143 = 7*3449
24149 =19*31*41
24151
24157 =7^2*17*29
24161 = 37*653
24163 = 73*331
24169
24173 = 23*1051
24179
24181
24187 =19*19*67
24191 = 17*1423
24193 = 13*1861
24197
24199 = 7*3457
24203
24209 = 43*563
24217 = 61*397
24221 = 53*457
24223
24227 = 7*3461
24229

24239
24241 = 7*3463
24247
24251
24253 = 79*307
24257 =127*191
24259 = 17*1427
24263 = 19*1277
24269 = 7*3467
24271 = 13*1867
24281
24283 = 7*3469
24287 =149*163
24289 =107*227
24293 = 17*1429
24301 = 19*1279
24307 =109*223
24311 =7*23*151
24313 = 41*593
24317
24319 = 83*293
24323 = 13*1871
24329
24331 = 29*839
24337
24341 =101*241
24347 = 97*251
24349 = 13*1873
24353 = 7^3*71
24359
24361 = 17*1433
24367 = 7*59*59
24371
24373
24377 = 19*1283
24379
24383 = 37*659
24389 =29*29*29
24391
24397 = 31*787
24401 = 13*1877
24403 = 23*1061
24407
24413
24419
24421
24427 = 13*1879
24433 = 53*461
24437 = 7*3491
24439
24443
24449 = 23*1063
24451 = 7*7*499
24457 = 37*661
24461 = 61*401
24463 = 17*1439
24467 = 43*569
24469
24473
24479 =7*13*269
24481
24487 = 47*521
24491 = 19*1289
24493 = 7*3499
24499
24503 =107*229
24509
24511 =127*193
24517
24521 =7*31*113
24523 =137*179
24527
24529 = 19*1291
24533
24539 = 53*463
24547
24551
24553 = 43*571
24557 = 13*1889
24559 = 41*599
24569 = 79*311
24571
24577 = 7*3511
24581 = 47*523
24583 =13*31*61
24587 = 23*1069
24589 = 67*367
24593
24599 = 17*1447
24601 = 73*337
24611
24613 =151*163
24617 =103*239
24619 = 7*3517
24623
24631
24637 = 71*347
24641 = 41*601
24643 = 19*1297
24647 = 7*7*503
24649 =157*157
24653 = 89*277
24659
24661 =7*13*271
24667 = 17*1451
24671
24677
24679 =23*29*37
24683
24689 = 7*3527
24691
24697
24701 = 17*1453
24703 = 7*3529
24707 = 31*797
24709
24713 = 13*1901
24719 = 19*1301
24721 = 59*419
24727 = 79*313
24731 = 7*3533
24733
24737 = 29*853
24743 =109*227
24749
24751 = 53*467
24757 = 19*1303
24763
24767
24769 =17*31*47
24773 = 7*3539
24779 =71*349
24781
24787 = 7*3541
24791 = 13*1907
24793
24797 =137*181
24799
24803 = 17*1459
24809
24811 = 43*577
24817 =13*23*83
24821
24823 =103*241
24829 = 7*3547
24833 = 19*1307
24839 = 59*421
24841
24847
24851
24853 =29*857
24857 = 7*53*67
24859
24863 =23*23*47
24869 =13*1913
24877
24881 =139*179
24883 =149*167
24887 = 41*607
24889
24899 = 7*3557
24901 = 37*673
24907
24911 = 29*859
24913 = 7*3559
24917
24919
24923
24929 = 97*257
24931 =107*233
24941 = 7*7*509
24943
24947=13*19*101
24949 = 61*409
24953
24961 =109*229
24967
24971
24973=13*17*113
24977
24979
24983 = 7*43*83
24989
24991 = 67*373
24997 = 7*3571
25001 = 23*1087
25007 = 17*1471
25009 = 89*281
25013
25019 =127*197
25021 =131*191
25027 = 29*863
25031
25033
25037
25039 = 7^3*73
25043 = 79*317
25049 = 37*677
25051 =13*41*47
25057
25061 = 19*1319
25063 = 71*353
25067 = 7*3581
25073
25079 = 31*809
25081 = 7*3583
25087
25093 = 23*1091
25097
25099 = 19*1321
25103 = 13*1931
25109 =7*17*211
25111
25117
25121
25123 = 7*37*97
25127
25129 = 13*1933
25133 = 41*613
25139 = 23*1093
25141 = 31*811
25147
25151 = 7*3593
25153
25159 =139*181
25163
25169
25171
25177 = 17*1481
25181 = 13^2*149
25183
25187 = 89*283
25189
25193 = 7*59*61
25199 =113*223
25207 =7*13*277
25211 = 17*1483
25213 = 19*1327
25217 =151*167
25219
25229
25231 = 23*1097
25237
25241 = 43*587
25243
25247
25249 = 7*3607
25253
25259 =13*29*67
25261
25271 = 37*683
25273 =127*199
25277 =7*23*157
25279 = 17*1487
25283 =131*193
25291 = 7*3613
25297 = 41*617
25301
25303
25307
25309
25313 = 17*1489
25319 = 7*3617
25321
25327 =19*31*43
25331 = 73*347
25337 = 13*1949
25339
25343
25349
25351 =101*251
25357
25361 = 7*3623
25363 = 13*1951
25367
25369 = 23*1103
25373
25379 = 41*619
25381 = 17*1493
25387 = 53*479

25391
25393 = 67*379
25397 =109*233
25403 =7*19*191
25409
25411
25417 = 7*3631
25423
25427 = 47*541
25429 = 59*431
25433 = 29*877
25439
25441=13*19*103
25447
25451 = 31*821
25453
25457
25459 = 7*3637
25463
25469
25471
25477 = 73*349
25481 = 83*307
25483 = 17*1499
25489 = 71*359
25493 =13*37*53
25499 = 43*593
25501 = 7*3643
25507 = 23*1109
25511 = 97*263
25513 = 31*823
25517 =17*19*79
25519 = 13^2*151
25523
25529 = 7*7*521
25537
25541
25543 = 7*41*89
25547 = 59*433
25549 = 29*881
25559 = 61*419
25561
25567 = 37*691
25571 =7*13*281
25573 =107*239
25577
25579
25583
25589
25591 =157*163
25601
25603
25607 = 29*883
25609
25613 = 7*3659
25621
25627 = 7*7*523
25631 =19*19*71
25633
25637 = 31*827
25639
25643
25649 = 13*1973
25651 =113*227
25657
25661 = 67*383
25667
25669 =7*19*193
25673
25679
25681 = 61*421
25687 = 17*1511
25691 = 23*1117
25693
25697 = 7*3671
25699 = 31*829
25703
25709 = 47*547
25711 = 7*3673
25717
25721 =17*17*89
25723 = 29*887
25727 = 13*1979
25733
25739 = 7*3677
25741
25747
25753 =7*13*283
25757 = 43*599
25759
25763
25769 = 73*353
25771
25777 =149*173
25781 =7*29*127
25783 =19*23*59
25787 =107*241
25789 =17*37*41
25793
25799
25801
25807 =131*197
25811 = 53*487
25813 = 83*311
25819
25823 =7^2*17*31
25829 = 23*1123
25831 = 13*1987
25837 = 7*3691
25841
25843 = 43*601
25847
25849
25853 =103*251
25859 = 19*1361
25867
25871 = 41*631
25873
25877 =113*229
25879 = 7*3697
25889
25891 = 17*1523
25897 =19*29*47
25901 = 59*439
25903
25907 = 7*3701
25909 = 13*1993
25913
25919
25921 =7^2*23*23
25931
25933
25937 = 37*701
25939
25943
25951
25957 =101*257
25961 = 13*1997
25963 = 7*3709
25967 = 23*1129
25969
25973 = 19*1367
25979 = 83*313
25981
25987 = 13*1999
25991 = 7*47*79
25997
25999
26003
26009 = 31*839
26011 =19*37*37
26017
26021
26023 = 53*491
26027 = 17*1531
26029
26033 = 7*3719
26039 = 13*2003
26041
26047 = 7*61*61
26051 =109*239
26053
26057 = 71*367
26063 = 67*389
26069 =131*199
26071 =29*29*31
26077 = 89*293
26083
26087 = 19*1373
26089 = 7*3727
26093 = 97*269
26099
26101 = 43*607
26107
26111
26113
26117 =7^2*13*41
26119
26123 =151*173
26129 =17*29*53
26131 = 7*3733
26137 = 59*443
26141
26143 = 13*2011
26149 = 79*331
26153
26159 =7*37*101
26161
26167 =137*191
26171
26173 = 7*3739
26177
26179 = 47*557
26183
26189
26197 =17*23*67
26201 =7*19*197
26203
26207 = 73*359
26209
26219 =157*167
26221 = 13*2017
26227
26231 = 17*1543
26233 = 37*709
26237
26239 = 19*1381
26243 =7*23*163
26249
26251
26261
26263
26267
26269 =109*241
26273 =13*43*47
26281 = 41*641
26287 = 97*271
26291 = 61*431
26293
26297
26299 =7*13*17^2
26303 = 29*907
26309
26311 = 83*317
26317
26321
26327 = 7*3761
26329 =113*233
26333 = 17*1549
26339
26341 = 7*53*71
26347
26351 = 13*2027
26353 =19*19*73
26357
26359 = 43*613
26363 = 41*643
26369 = 7*3767
26371
26377 = 13*2029
26381 =23*31*37
26383 = 7*3769
26387
26393
26399
26401 = 17*1553
26407
26413 = 61*433
26417
26419 = 29*911
26423
26429=13*19*107
26431
26437
26441 =137*193
26443 = 31*853
26447 = 53*499
26449
26453 = 7*3779
26459
26461 = 47*563
26467 =7*19*199
26471 =103*257
26473 = 23*1151
26479
26483 = 71*373
26489
26491 = 59*449
26497
26501
26503 = 17*1559
26507 = 13*2039
26509 = 7*7*541
26513
26519 = 23*1153
26527 = 41*647
26531 = 43*617
26533=13*13*157
26537 =7*17*223
26539

26549 =139*191
26551 = 7*3793
26557
26561
26563 =101*263
26567 = 31*857
26569 =163*163
26573
26579 = 7*3797
26581 = 19*1399
26591
26593 =7*29*131
26597
26599 = 67*397
26603 = 37*719
26611 =13*23*89
26617 = 43*619
26621 = 7*3803
26623 = 79*337
26627
26629 = 31*859
26633
26639 = 17*1567
26641
26647
26651 = 29*919
26657 =19*23*61
26659 = 53*503
26663 =7*13*293
26669
26671 =149*179
26677 =7*37*103
26681
26683
26687
26689 = 13*2053
26693
26699
26701
26707 = 17*1571
26711
26713
26717
26723
26729
26731
26737
26743 = 47*569
26747 = 7*3821
26749 = 23*1163
26753 = 31*863
26759
26761 = 7*3823
26767 =13*29*71
26771 = 19*1409
26773 = 41*653
26777
26779 = 61*439
26783
26789 = 7*43*89
26791 = 73*367
26797 =127*211
26801
26803 = 7*7*547
26809 =17*19*83
26813
26819 = 13*2063
26821
26827 =139*193
26831 = 7*3833
26833
26837 = 47*571
26839
26843 = 17*1579
26849
26857 =107*251
26861
26863
26867 = 67*401
26869 = 97*277
26879
26881
26887 =7*23*167
26891
26893
26897 = 13*2069
26899 = 37*727
26903
26909 = 71*379
26911 = 17*1583
26921
26923=13*19*109
26927
26929 = 7*3847
26933 = 23*1171
26941 = 29*929
26947
26951
26953
26957 = 7*3851
26959
26963 = 59*457
26969 =149*181
26971 = 7*3853
26977 = 53*509
26981
26987
26989 =137*197
26993
26999 =7^2*19*29
27001 =13*31*67
27007 =113*239
27011
27013 =7*17*227
27017
27019 = 41*659
27023 = 61*443
27029 =151*179
27031
27037 = 19*1423
27041 = 7*3863
27043
27047 =17*37*43
27053 = 13*2081
27059
27061
27067
27073
27077
27079 = 13*2083
27083 = 7*53*73
27089 =103*263
27091
27097 =7*7*7*79
27101 = 41*661
27103
27107
27109
27113 = 19*1427
27119 = 47*577
27121 = 37*733
27127
27131 = 13*2087
27133 = 43*631
27139 = 7*3877
27143
27149 = 17*1597
27151 = 19*1429
27157 = 13*2089
27161 =157*173
27163 = 23*1181
27167 = 7*3881
27169 =101*269
27173 = 29*937
27179
27187 = 31*877
27191
27193 = 71*383
27197
27199 = 59*461
27209 =7*13^2*23
27211
27217 = 17*1601
27221 =163*167
27223 = 7*3889
27227 = 19*1433
27229 = 73*373
27233 =113*241
27239
27241
27251 =7*17*229
27253
27257 = 97*281
27259
27263 =137*199
27271
27277
27281
27283
27287 = 13*2099
27289 = 29*941
27293 = 7*7*557
27299
27301 = 23*1187
27307 = 7*47*83
27311 = 31*881
27317 = 59*463
27319 = 17*1607
27323 = 89*307
27329
27331 =151*181
27337
27341 = 19*1439
27343 = 37*739
27347 =23*29*41
27349 = 7*3907
27353 = 17*1609
27359 =109*251
27361
27367
27371 =101*271
27373 = 31*883
27377 = 7*3911
27383 =139*197
27389 = 61*449
27391 =7^2*13*43
27397
27403 = 67*409
27407
27409
27413 = 79*347
27419 = 7*3917
27421 = 17*1613
27427
27431
27433 = 7*3919
27437
27439 = 23*1193
27443 = 13*2111
27449
27451 = 97*283
27457
27461 = 7*3923
27463 = 29*947
27469 = 13*2113
27473 = 83*331
27479
27481
27487
27491 = 37*743
27493 = 19*1447
27497 = 31*887
27499 =107*257
27503 = 7*3929
27509
27517 = 7*3931
27521 =13*29*73
27523 = 17*1619
27527
27529
27539
27541
27547 = 13^2*163
27551
27553 = 59*467
27557 = 17*1621
27559 =7*31*127
27563 = 43*641
27569 = 19*1451
27571 = 79*349
27581
27583
27587 = 7*7*563
27589 = 47*587
27593 = 41*673
27601 = 7*3943
27607 = 19*1453
27611
27613 = 53*521
27617
27619 = 71*389
27623 = 23*1201
27629 = 7*3947
27631
27637 = 29*953
27641 =131*211
27647
27649 = 43*643
27653
27659 = 17*1627
27661 =139*199
27667 = 73*379
27671 = 7*59*67
27673
27677 = 13*2129
27679 = 89*311
27683 =19*31*47
27689
27691
27697

27701
27703 = 13*2131
27707 =103*269
27713 =7*37*107
27719 = 53*523
27721 = 19*1459
27727 =7*17*233
27733
27737
27739
27743
27749
27751
27757 = 41*677
27761 =17*23*71
27763
27767
27769 = 7*3967
27773
27779
27781 = 13*2137
27787 = 37*751
27791
27793
27799
27803
27809
27811 =7*29*137
27817
27821 = 43*647
27823
27827
27829 = 17*1637
27833 = 13*2141
27839 = 7*41*97
27847
27851
27853 =7*23*173
27857 = 89*313
27859 = 13*2143
27869 =29*31*31
27871 = 47*593
27877 = 61*457
27881 = 7*7*569
27883
27887 = 79*353
27889 =167*167
27893
27899 = 23*1213
27901
27911=13*19*113
27913 =103*271
27917
27919
27923 = 7*3989
27931 =17*31*53
27937 =7*13*307
27941
27943
27947
27949 = 19*1471
27953
27959 = 73*383
27961
27967
27971 = 83*337
27977 =101*277
27979 = 7*7*571
27983
27989 = 13*2153
27991 = 23*1217
27997
28001
28003 = 41*683
28007 = 7*4001
28009 = 37*757
28013 =109*257
28019
28021 = 7*4003
28027
28031
28033 =17*17*97
28037 =23*23*53
28043 = 29*967
28049 = 7*4007
28051
28057
28063 =7*19*211
28067=13*17*127
28069
28073 = 67*419
28079 = 43*653
28081
28087
28091 = 7*4013
28093 = 13*2161
28097
28099
28103 =157*179
28109
28111
28117 = 31*907
28121 = 61*461
28123
28129 = 23*1223
28133 = 7*4019
28139 = 19*1481
28141 =107*263
28147 = 7*4021
28151
28153 = 47*599
28157 = 37*761
28159 = 29*971
28163
28169 = 17*1657
28177 = 19*1483
28181
28183
28187 = 71*397
28189 = 7*4027
28199 =163*173
28201
28207 = 67*421
28211
28213 = 89*317
28217 =7*29*139
28219
28223 = 13^2*167
28229
28231 =7*37*109
28241 = 31*911
28243 = 61*463
28247 = 47*601
28249 =13*41*53
28253 = 19*1487
28261 = 59*479
28267 = 23*1229
28271 = 17*1663
28273 = 7*7*577
28277
28279
28283
28289
28291 = 19*1489
28297
28301 =7*13*311
28307
28309
28313 = 23*1231
28319
28321 =127*223
28327 = 13*2179
28331 = 41*691
28333 = 29*977
28337 = 43*659
28339 = 17*1667
28343 = 7*4049
28349
28351
28357 = 7*4051
28361 = 79*359
28363 =113*251
28367 = 19*1493
28373 = 17*1669
28379 =13*37*59
28381 =101*281
28387
28393
28397 = 73*389
28399 = 7*4057
28403
28409
28411
28417 =157*181
28421 = 97*293
28423 = 43*661
28427 =7*31*131
28429
28433
28439
28441 =7*17*239
28447
28451 = 23*1237
28453 = 37*769
28459 =149*191
28463
28469 =7*7*7*83
28471 = 71*401
28477
28481 = 19*1499
28483 =7*13*313
28487 = 61*467
28489 = 31*919
28493
28499
28507 = 29*983
28511 = 7*4073
28513
28517
28519 =19*19*79
28529 = 47*607
28531 =103*277
28537
28541
28543 =17*23*73
28547
28549
28553 = 7*4079
28559
28561 = 13^4
28571
28573
28577 =17*41*41
28579
28583 =101*283
28591
28597
28601 = 37*773
28603
28607
28609 = 7*61*67
28613 =13*31*71
28619
28621
28627
28631
28637 = 7*4091
28639 = 13*2203
28643
28649
28651 = 7*4093
28657
28661
28663
28667 =109*263
28669
28673 = 53*541
28679 =7*17*241
28681 =23*29*43
28687
28691 = 13*2207
28693 = 7*4099
28697
28703
28709 = 19*1511
28711
28717 =13*47*47
28723
28727 = 23*1249
28729
28733 = 59*487
28739 = 29*991
28741 = 41*701
28747 =17*19*89
28751
28753
28757 =149*193
28759
28763 = 7*7*587
28769 = 13*2213
28771
28777 = 7*4111
28781 = 17*1693
28783 =107*269
28789
28793
28799 = 31*929
28801 = 83*347
28807
28811 = 47*613
28813
28817
28819 =7*23*179
28823 =19*37*41
28829 =127*227
28837
28841 =151*191
28843
28847 =7*13*317
28849 = 17*1697

28859
28861 =7^2*19*31
28867
28871
28873 = 13*2221
28877 = 67*431
28879
28883 = 17*1699
28889 = 7*4127
28891 =167*173
28901
28903 = 7*4129
28907 =137*211
28909
28913 = 29*997
28921
28927
28931 = 7*4133
28933
28937 = 19*1523
28939 = 43*673
28943 =103*281
28949
28951=13*17*131
28957 = 23*1259
28961
28967 = 83*349
28969 = 59*491
28973 = 7*4139
28979
28981 = 73*397
28987 =7*41*101
28991 = 53*547
28993 = 79*367
28997 =107*271
28999 = 47*617
29003 =13*23*97
29009
29011 = 67*433
29017
29021
29023
29027
29033
29039 = 71*409
29041 =113*257
29047 = 31*937
29053 = 17*1709
29057 = 7*7*593
29059
29063
29069 = 41*709
29071 = 7*4153
29077
29081 = 13*2237
29083 =127*229
29087 =17*29*59
29089 = 19*1531
29093 = 47*619
29099 = 7*4157
29101
29107 = 13*2239
29111 = 43*677
29113 = 7*4159
29119 = 37*787
29123
29129
29131
29137
29141 =7*23*181
29143 =151*193
29147
29149 =103*283
29153
29159 = 13*2243
29167
29171 = 31*941
29173
29177 =163*179
29179
29189 = 17^2*101
29191
29197 = 7*43*97
29201
29203 =19*29*53
29207
29209
29213 =131*223
29219 = 61*479
29221
29231
29233 =23*31*41
29237 = 13^2*173
29239 = 7*4177
29243
29251
29257 = 17*1721
29261 = 29*1009
29263 = 13*2251
29267 =7*37*113
29269
29273 = 73*401
29279 =19*23*67
29281 = 7*47*89
29287
29291 = 17*1723
29297
29299 = 83*353
29303
29309 = 7*53*79
29311
29317 = 19*1543
29321 =109*269
29323 = 7*59*71
29327
29329 =139*211
29333
29339
29341 =13*37*61
29347
29351 = 7*7*599
29353 =149*197
29357 = 31*947
29363
29369 = 43*683
29371 = 23*1277
29377 = 29*1013
29383
29387
29389
29393 =
= 7*13*17*19
29399
29401
29407 = 7*4201
29411
29413 = 67*439
29417 = 23*1279
29419 =13*31*73
29423
29429
29431 = 19*1549
29437
29441 = 59*499
29443
29449 = 7*7*601
29453
29459 = 89*331
29461 = 17*1733
29467 = 79*373
29471 = 13*2267
29473
29477 = 7*4211
29479 = 41*719
29483
29489 = 37*797
29497 = 13*2269
29501
29503 =163*181
29507 = 19*1553
29509 = 23*1283
29519 = 7*4217
29521 = 53*557
29527
29531
29533 = 7*4219
29537
29539 =109*271
29543 = 31*953
29549 = 13*2273
29551 = 29*1019
29561 =7*41*103
29563 =17*37*47
29567
29569
29573
29581
29587
29591 =127*233
29593 =101*293
29597 = 17*1741
29599
29603 = 7*4229
29609 = 29*1021
29611
29617 = 7*4231
29621 = 19*1559
29627 =13*43*53
29629
29633
29639 =107*277
29641
29647 = 23*1289
29651 =149*199
29653 = 13*2281
29657 = 47*631
29659 =7*19*223
29663
29669
29671
29677 = 59*503
29681 = 67*443
29683
29687 = 7*4241
29693 = 23*1291
29699 = 17*1747
29701 = 7*4243
29707 = 61*487
29713 = 43*691
29717
29719 =113*263
29723
29729 =7*31*137
29731 = 13*2287
29737 =131*227
29741
29743 = 7*7*607
29747 =151*197
29749 = 71*419
29753
29759
29761
29767 = 17^2*103
29771 = 7*4253
29773 = 19*1567
29779 = 97*307
29783 =13*29*79
29789
29791 =31*31*31
29797 = 83*359
29801 = 17*1753
29803
29807 = 41*727
29809 = 13*2293
29813 = 7*4259
29819
29827 = 7*4261
29831 = 23*1297
29833
29837
29839 = 53*563
29849 = 19*1571
29851
29857 = 73*409
29861 = 13*2297
29863
29867
29869 =7*17*251
29873
29879
29881
29891 = 71*421
29893 =167*179
29897 = 7*4271
29899 = 29*1031
29903 = 17*1759
29911 = 7*4273
29917
29921
29923 = 23*1301
29927
29929 =173*173
29933 = 37*809
29939 =7^2*13*47
29941 = 79*379
29947
29951 = 61*491
29957 = 29*1033
29959
29963 =19*19*83
29969 = 23*1303
29971 =17*41*43
29977 = 31*967
29981 = 7*4283
29983
29987 =157*191
29989
29993 = 89*337
29999 = 131*229
30001 = 19*1579

.3. Primitív gyökök és index táblák mod $\mathbb{Z}_n$

Az 1000-nél kisebb prímszámok
és ezek legkisebb primitív gyökei

p	g	p	g	p	g	p	g	p	g
2	1	151	6	353	3	577	5	811	3
3	2	157	5	359	7	587	2	821	2
5	2	163	2	367	6	593	3	823	3
7	3	167	5	373	2	599	7	827	2
11	2	173	2	379	2	601	7	829	2
13	2	179	2	383	5	607	3	839	11
17	3	181	2	389	2	613	2	853	2
19	2	191	19	397	5	617	3	857	3
23	5	193	5	401	3	619	2	859	2
29	2	197	2	409	21	631	3	863	5
31	3	199	3	419	2	641	3	877	2
37	2	211	2	421	2	643	11	881	3
41	6	223	3	431	7	647	5	883	2
43	3	227	2	433	5	653	2	887	5
47	5	229	6	439	15	659	2	907	2
53	2	233	3	443	2	661	2	911	17
59	2	239	7	449	3	673	5	919	7
61	2	241	7	457	13	677	2	929	3
67	2	251	6	461	2	683	5	937	5
71	7	257	3	463	3	691	3	941	2
73	5	263	5	467	2	701	2	947	2
79	3	269	2	479	13	709	2	953	3
83	2	271	6	487	3	719	11	967	5
89	3	277	5	491	2	727	5	971	6
97	5	281	3	499	7	733	6	977	3
101	2	283	3	503	5	739	3	983	5
103	5	293	2	509	2	743	5	991	6
107	2	307	5	521	3	751	3	997	7
109	6	311	17	523	2	757	2	1009	11
113	3	313	10	541	2	761	6		
127	3	317	2	547	2	769	11		
131	2	331	3	557	2	773	2		
137	3	337	10	563	2	787	2		
139	2	347	2	569	3	797	2		
149	2	349	2	571	3	809	3		

MAGYARÁZAT: Az első táblázatban $x = ind_p^{(g)}(a)$ olyan, mint a logaritmus: $g^x \equiv a \pmod{p}$, amely értékeket a második táblázatban láthatunk.

Index- és hatványtáblázatok (mod p)

Indexek

Hatványok

p = 3, g = 2.

Szám	0	1	2	3	4	5	6	7	8	9
0		2	1							

Ind	0	1	2	3	4	5	6	7	8	9
0		2	1							

p = 5, g = 2.

Szám	0	1	2	3	4	5	6	7	8	9
0		4	1	3	2					

Ind.	0	1	2	3	4	5	6	7	8	9
0		2	4	3	1					

p = 7, g = 3.

Szám	0	1	2	3	4	5	6	7	8	9
0		6	2	1	4	5	3			

Ind.	0	1	2	3	4	5	6	7	8	9
0		3	2	6	4	5	1			

p = 11, g = 2.

Szám	0	1	2	3	4	5	6	7	8	9
0		10	1	8	2	4	9	7	3	6
1	5									

Ind.	0	1	2	3	4	5	6	7	8	9
0		2	4	8	5	10	9	7	3	6
1	1									

p = 13, g = 2.

Szám	0	1	2	3	4	5	6	7	8	9
0		12	1	4	2	9	5	11	3	8
1	10	7	6							

Ind.	0	1	2	3	4	5	6	7	8	9
0		2	4	8	3	6	12	11	9	5
1	10	7	1							

p = 17, g = 3.

Szám	0	1	2	3	4	5	6	7	8	9
0		16	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

Ind.	0	1	2	3	4	5	6	7	8	9
0		3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6	1			

p = 19, g = 2.

Szám	0	1	2	3	4	5	6	7	8	9
0		18	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

Ind.	0	1	2	3	4	5	6	7	8	9
0		2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10	1	

p = 23, g = 5.

Szám	0	1	2	3	4	5	6	7	8	9
0		22	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

Ind.	0	1	2	3	4	5	6	7	8	9
0		5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14	1							

Indexek Hatványok

p = 29, g = 2.

Szám	0	1	2	3	4	5	6	7	8	9
0		28	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

Ind.	0	1	2	3	4	5	6	7	8	9
0		2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15	1	

p = 31, g = 3.

Szám	0	1	2	3	4	5	6	7	8	9
0		30	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

Ind.	0	1	2	3	4	5	6	7	8	9
0		3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21
3	1									

p = 37, g = 2.

Szám	0	1	2	3	4	5	6	7	8	9
0		36	1	26	2	23	27	32	3	15
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

Ind.	0	1	2	3	4	5	6	7	8	9
0		2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19	1			

p = 41, g = 6.

Szám	0	1	2	3	4	5	6	7	8	9
0		40	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

Ind.	0	1	2	3	4	5	6	7	8	9
0		6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7
4	1									

p = 43, g = 3.

Szám	0	1	2	3	4	5	6	7	8	9
0		42	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

Ind.	0	1	2	3	4	5	6	7	8	9
0		3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29	1							

p = 47, g = 5.

Szám	0	1	2	3	4	5	6	7	8	9
0		46	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

Ind.	0	1	2	3	4	5	6	7	8	9
0		5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19	1			

.4. Irreducibilis polinomok mod $\mathbb{Z}_n$

Irreducibilis polinomok mod Z_n

Z_2[x] –ben:

$f_7(x) = x^2+x+1$
$f_{11}(x)= x^3+x+1$
$f_{13}(x)= x^3+x^2+1$.
$f_{19}(x)= x^4+x^2+1$
$f_{25}(x)= x^4+x^3+1$
$f_{31}(x)= x^4+x^3+x^2+x+1$

Z_3[x] –ben:

$f_{10}(x)= x^2+1$
$f_{14}(x)= x^2+x+2$
$f_{17}(x)= x^2+2x+2$

$f_{34}(x)= x^3+2x+1$
$f_{35}(x)= x^3+2x+2$
$f_{38}(x)= x^3+x^2+2$
$f_{41}(x)= x^3+x^2+x+2$
$f_{43}(x)= x^3+x^2+2x+1$
$f_{46}(x)= x^3+2x^2+1$
$f_{49}(x)= x^3+2x^2+x+1$
$f_{53}(x)= x^3+2x^2+2x+2$

$f_{86}(x)= x^4+x+2$
$f_{89}(x)= x^4+2x+2$
$f_{92}(x)= x^4+x^2+2$
$f_{94}(x)= x^4+x^2+x+1$
$f_{97}(x)= x^4+x^2+x+1$
$f_{101}(x)= x^4+2x^2+2$
$f_{110}(x)= x^4+x^3+2$
$f_{115}(x)= x^4+x^3+2x+1$
$f_{118}(x)= x^4+x^3+x^2+1$
$f_{121}(x)= x^4+x^3+x^2+x+1$
$f_{125}(x)= x^4+x^3+x^2+2x+2$
$f_{134}(x)= x^4+x^3+2x^2+2x+2$
$f_{137}(x)= x^4+2x^3+2$
$f_{139}(x)= x^4+2x^3+x+1$
$f_{145}(x)= x^4+2x^3+x^2+1$
$f_{149}(x)= x^4+2x^3+x^2+x+2$
$f_{151}(x)= x^4+2x^3+x^2+2x+1$
$f_{158}(x)= x^4+2x^3+2x^2+x+2$

Z_4[x] –ben:

$f_{17}(x)= x^2+1$
$f_{18}(x)= x^2+2$
$f_{21}(x)= x^2+x+1$
$f_{23}(x)= x^2+x+3$
$f_{26}(x)= x^2+2x+2$
$f_{27}(x)= x^2+2x+3$
$f_{29}(x)= x^2+3x+1$
$f_{31}(x)= x^2+3x+3$
$f_{33}(x)= 2x^2+1$
$f_{41}(x)= 2x^2+2x+1$

$f_{66}(x)= x^3+2$
$f_{69}(x)= x^3+x+1$
$f_{71}(x)= x^3+x+3$
$f_{74}(x)= x^3+2x+2$
$f_{77}(x)= x^3+3x+1$
$f_{79}(x)= x^3+3x+3$
$f_{81}(x)= x^3+x^2+1$
$f_{83}(x)= x^3+x^2+3$
$f_{87}(x)= x^3+x^2+x+3$
$f_{89}(x)= x^3+x^2+2x+1$
$f_{91}(x) = x^3+x^2+2x+3$
$f_{93}(x) = x^3+x^2+3x+1$
$f_{98}(x) = x^3+2x^2+2$
$f_{101}(x)= x^3+2x^2+x+1$
$f_{103}(x)= x^3+2x^2+x+3$
$f_{106}(x)= x^3+2x^2+2x+2$
$f_{109}(x)= x^3+2x^2+3x+1$
$f_{111}(x)= x^3+2x^2+3x+3$
$f_{113}(x)= x^3+3x^2+1$
$f_{115}(x)= x^3+3x^2+3$
$f_{117}(x)= x^3+3x^2+x+1$
$f_{121}(x)= x^3+3x^2+2x+1$
$f_{123}(x)= x^3+3x^2+2x+3$
$f_{127}(x)= x^3+3x^2+3x+3$
$f_{129}(x)= 2x^3+1$
$f_{137}(x)= 2x^3+2x+1$
$f_{161}(x)= 2x^3+2x^2+1$
$f_{169}(x)= 2x^3+2x^2+2x+1$

$f_{257}(x)= x^4+1$
$f_{258}(x)= x^4+2$
$f_{261}(x)= x^4+x+1$
$f_{263}(x)= x^4+x+3$
$f_{266}(x)= x^4+2x+2$
$f_{267}(x)= x^4+2x+3$
$f_{269}(x)= x^4+3x+1$
$f_{271}(x)= x^4+3x+3$
$f_{275}(x)= x^4+x^2+3$
$f_{281}(x)= x^4+x^2+2x+1$
$f_{283}(x)= x^4+x^2+2x+3$
$f_{290}(x)= x^4+2x^2+2$
$f_{291}(x)= x^4+2x^2+3$
$f_{293}(x)= x^4+2x^2+x+1$
$f_{295}(x)= x^4+2x^2+x+3$
$f_{297}(x)= x^4+2x^2+2x+1$
$f_{298}(x)= x^4+2x^2+2x+2$
$f_{301}(x)= x^4+2x^2+3x+1$
$f_{303}(x)= x^4+2x^2+3x+3$
$f_{305}(x)= x^4+3x^2+1$
$f_{307}(x)= x^4+3x^2+3$
$f_{313}(x)= x^4+3x^2+2x+1$
$f_{321}(x)= x^4+x^3+1$

$f_{323}(x)= x^4+x^3+3$
$f_{329}(x)= x^4+x^3+2x+1$
$f_{331}(x)= x^4+x^3+2x+3$
$f_{341}(x)= x^4+x^3+x^2+x+1$
$f_{343}(x)= x^4+x^3+x^2+x+3$
$f_{349}(x)= x^4+x^3+x^2+3x+1$
$f_{351}(x)= x^4+x^3+x^2+3x+3$
$f_{353}(x)= x^4+x^3+2x^2+1$
$f_{355}(x)= x^4+x^3+2x^2+3$
$f_{361}(x)= x^4+x^3+2x^2+2x+1$
$f_{363}(x)= x^4+x^3+2x^2+2x+3$
$f_{373}(x)= x^4+x^3+3x^2+x+1$
$f_{375}(x)= x^4+x^3+3x^2+x+3$
$f_{381}(x)= x^4+x^3+3x^2+3x+1$
$f_{383}(x)= x^4+x^3+3x^2+3x+3$
$f_{386}(x)= x^4+2x^3+2$
$f_{387}(x)= x^4+2x^3+3$
$f_{389}(x)= x^4+2x^3+x+1$
$f_{391}(x)= x^4+2x^3+x+3$
$f_{393}(x)= x^4+2x^3+2x+1$
$f_{394}(x)= x^4+2x^3+2x+2$
$f_{397}(x)= x^4+2x^3+3x+1$
$f_{399}(x)= x^4+2x^3+3x+3$
$f_{401}(x)= x^4+2x^3+x^2+1$
$f_{409}(x)= x^4+2x^3+x^2+2x+1$
$f_{411}(x)= x^4+2x^3+x^2+2x+3$
$f_{417}(x)= x^4+2x^3+2x^2+1$
$f_{418}(x)= x^4+2x^3+2x^2+2$
$f_{421}(x)= x^4+2x^3+2x^2+x+1$
$f_{423}(x)= x^4+2x^3+2x^2+x+3$
$f_{426}(x)= x^4+2x^3+2x^2+2x+2$
$f_{427}(x)= x^4+2x^3+2x^2+2x+3$
$f_{429}(x)= x^4+2x^3+2x^2+3x+1$
$f_{431}(x)= x^4+2x^3+2x^2+3x+3$
$f_{433}(x)= x^4+2x^3+3x^2+1$
$f_{435}(x)= x^4+2x^3+3x^2+3$
$f_{443}(x)= x^4+2x^3+3x^2+2x+3$
$f_{449}(x)= x^4+3x^3+1$
$f_{451}(x)= x^4+3x^3+3$
$f_{457}(x)= x^4+3x^3+2x+1$
$f_{459}(x)= x^4+3x^3+2x+3$
$f_{469}(x)= x^4+3x^3+x^2+x+1$
$f_{471}(x)= x^4+3x^3+x^2+x+3$
$f_{477}(x)= x^4+3x^3+x^2+3x+1$
$f_{479}(x)= x^4+3x^3+x^2+3x+3$
$f_{481}(x)= x^4+3x^3+2x^2+1$
$f_{483}(x)= x^4+3x^3+2x^2+3$
$f_{489}(x)= x^4+3x^3+2x^2+2x+1$
$f_{491}(x)= x^4+3x^3+2x^2+2x+3$
$f_{501}(x)= x^4+3x^3+3x^2+x+1$
$f_{503}(x)= x^4+3x^3+3x^2+x+3$
$f_{509}(x)= x^4+3x^3+3x^2+3x+1$
$f_{511}(x)= x^4+3x^3+3x^2+3x+3$
$f_{513}(x)= 2x^4+1$
$f_{521}(x)= 2x^4+2x+1$
$f_{545}(x)= 2x^4+2x^2+1$
$f_{553}(x)= 2x^4+2x^2+2x,1$
$f_{641}(x)= 2x^4+2x^3+1$
$f_{649}(x)= 2x^4+2x^3+2x+1$
$f_{673}(x)= 2x^4+2x^3+2x^2+1$
$f_{681}(x)=2x^4+2x^3+2x^2+2x+1$

$Z_5[x]$ –ben:

$f_{27}(x)= x^2+2$
$f_{28}(x)= x^2+3$
$f_{31}(x)= x^2+x+1$
$f_{32}(x)= x^2+x+2$
$f_{38}(x)= x^2+2x+3$
$f_{39}(x)= x^2+2x+4$
$f_{43}(x)= x^2+3x+3$
$f_{44}(x)= x^2+3x+4$
$f_{46}(x)= x^2+4x+1$
$f_{47}(x)= x^2+4x+2$

$f_{131}(x)= x^3+x+1$
$f_{134}(x)= x^3+x+4$
$f_{136}(x)= x^3+2x+1$
$f_{139}(x)= x^3+2x+4$
$f_{142}(x)= x^3+3x+2$
$f_{143}(x)= x^3+3x+3$
$f_{147}(x)= x^3+4x+2$
$f_{148}(x)= x^3+4x+3$
$f_{151}(x)= x^3+x^2+1$
$f_{152}(x)= x^3+x^2+2$
$f_{158}(x)= x^3+x^2+x+3$
$f_{159}(x)= x^3+x^2+x+4$
$f_{166}(x)= x^3+x^2+3x+1$
$f_{169}(x)= x^3+x^2+3x+4$
$f_{171}(x)= x^3+x^2+4x+1$
$f_{173}(x)= x^3+x^2+4x+3$
$f_{176}(x)= x^3+2x^2+1$
$f_{178}(x)= x^3+2x^2+3$
$f_{183}(x)= x^3+2x^2+x+3$
$f_{184}(x)= x^3+2x^2+x+4$
$f_{187}(x)= x^3+2x^2+2x+2$
$f_{188}(x)= x^3+2x^2+2x+3$
$f_{197}(x)= x^3+2x^2+4x+2$
$f_{199}(x)= x^3+2x^2+4x+4$
$f_{202}(x)= x^3+3x^2+2$
$f_{204}(x)= x^3+3x^2+4$
$f_{206}(x)= x^3+3x^2+x+1$
$f_{207}(x)= x^3+3x^2+x+2$
$f_{212}(x)= x^3+3x^2+2x+2$
$f_{213}(x)= x^3+3x^2+2x+3$
$f_{221}(x)= x^3+3x^2+4x+1$
$f_{223}(x)= x^3+3x^2+4x+3$
$f_{228}(x)= x^3+4x^2+3$
$f_{229}(x)= x^3+4x^2+4$
$f_{231}(x)= x^3+4x^2+x+1$
$f_{232}(x)= x^3+4x^2+x+2$
$f_{241}(x)= x^3+4x^2+3x+1$
$f_{244}(x)= x^3+4x^2+3x+4$
$f_{247}(x)= x^3+4x^2+4x+2$
$f_{249}(x)= x^3+4x^2+4x+4$
$f_{627}(x)= x^4+2$
$f_{628}(x)= x^4+3$
$f_{634}(x)= x^4+x+4$
$f_{639}(x)= x^4+2x+4$
$f_{644}(x)= x^4+3x+4$
$f_{649}(x)= x^4+4x+4$
$f_{652}(x)= x^4+x^2+2$
$f_{656}(x)= x^4+x^2+x+1$
$f_{662}(x)= x^4+x^2+2x+2$
$f_{663}(x)= x^4+x^2+2x+3$
$f_{667}(x)= x^4+x^2+3x+2$
$f_{668}(x)= x^4+x^2+3x+3$
$f_{671}(x)= x^4+x^2+4x+1$
$f_{678}(x)= x^4+2x^2+3$
$f_{686}(x)= x^4+2x^2+2x+1$
$f_{688}(x)= x^4+2x^2+2x+3$
$f_{691}(x)= x^4+2x^2+3x+1$
$f_{693}(x)= x^4+2x^2+3x+3$
$f_{703}(x)= x^4+3x^2+3$
$f_{706}(x)= x^4+3x^2+x+1$
$f_{708}(x)= x^4+3x^2+x+3$
$f_{721}(x)= x^4+3x^2+4x+1$
$f_{723}(x)= x^4+3x^2+4x+3$
$f_{727}(x)= x^4+4x^2+2$

.5. A GF(8), GF(9) és GF(25) véges testek

A GF(4) testet az 5.1.4) feladat megoldásában közöltük. Emlékeztetünk továbbá arra, hogy minden $p \in \mathbb{P}$ prímszám esetén $(\mathbb{Z}_p, +, \cdot)$ egy p -elemű test.

$GF(8)=Z_2[x]/_{(x^3+x+1)}=(\{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1\},+,\bullet)$

+	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	x+1	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	x+1	0	1	x^2+x	x^2+x+1	x^2	x^2+1
x+1	x+1	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	x+1
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	x+1	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	x+1	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	x+1	x	1	0

•	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	x+1	1	x^2+x+1	x^2+1
x+1	0	x+1	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	x+1	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	x+1	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	x+1	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	x+1

MAGYARÁZAT: A 2-vel osztható algebrai kifejezések (pl: $2x^2$, 2x, 2) és maga a faktorizáló polinom maradéka 0, ezért a műveletek elvégzése után a polinomokhoz ezek hozzáadhatók és kivonhatók anélkül, hogy a maradék megváltozna. ($x^3 + x + 1 \equiv 2x^2 \equiv 2x \equiv 2 \equiv 0$)

$\mathbf{x^3} \equiv x^3 + 2x + 2 = (x^3 + x + 1) + x + 1 \equiv \mathbf{x + 1}$

$x^3 + x + 1 \equiv (x^3 + x + 1)x = x^4 + x^2 + x \equiv 0 \Rightarrow \mathbf{x^4} \equiv x^4 + 2x^2 + 2x = (x^4 + x^2 + x) + x^2 + x \equiv \mathbf{x^2 + x}$

pl. $(x^2 + x + 1)(x^2 + x + 1) = x^4 + 2x^3 + 3x^2 + 2x + 1 \equiv x^4 + x^2 + 1 \equiv x^2 + x + x^2 + 1 \equiv x + 1$

$(x^2 + x)(x^2 + x + 1) = x^4 + 2x^3 + 2x^2 + x \equiv x^4 + x \equiv x^2 + x + x \equiv x^2$

+	0	1	2	x	2x	x+1	x+2	2x+1	2x+2
0	0	1	2	x	2x	x+1	x+2	2x+1	2x+2
1	1	2	0	x+1	2x+1	x+2	x	2x+2	2x
2	2	0	1	x+2	2x+2	x	x+1	2x	2x+1
x	x	x+1	x+2	2x	0	2x+1	2x+2	1	2
2x	2x	2x+1	2x+2	0	x	1	2	x+1	x+2
x+1	x+1	x+2	x	2x+1	1	2x+2	2x	2	0
x+2	x+2	x	x+1	2x+2	2	2x	2x+1	0	1
2x+1	2x+1	2x+2	2x	1	x+1	2	0	x+2	x
2x+2	2x+2	2x	2x+1	2	x+2	0	1	x	x+1

•	0	1	2	x	2x	x+1	x+2	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	2x	x+1	x+2	2x+1	2x+2
2	0	2	1	2x	x	2x+2	2x+1	x+2	x+1
x	0	x	2x	2	1	x+2	2x+2	x+1	2x+1
2x	0	2x	x	1	2	2x+1	x+1	2x+2	x+2
x+1	0	x+1	2x+2	x+2	2x+1	2x	1	2	x
x+2	0	x+2	2x+1	2x+2	x+1	1	x	2x	2
2x+1	0	2x+1	x+2	x+1	2x+2	2	2x	x	1
2x+2	0	2x+2	x+1	2x+1	x+2	x	2	1	2x

$GF(9)=Z_3[x]/_{(x^2+1)}=(\{0,1,2,x,2x,x+1,x+2,2x+1,2x+2\},+,\bullet)$

$GF(25) = Z_5[x]/(x^2 + x + 2)$

+	0	1	2	3	4	x	x+1	x+2	x+3	x+4	2x	2x+1	2x+2	2x+3	2x+4	3x	3x+1	3x+2	3x+3	3x+4	4x	4x+1	4x+2	4x+3	4x+4
0	0	1	2	3	4	x	x+1	x+2	x+3	x+4	2x	2x+1	2x+2	2x+3	2x+4	3x	3x+1	3x+2	3x+3	3x+4	4x	4x+1	4x+2	4x+3	4x+4
1	1	2	3	4	0	x+1	x+2	x+3	x+4	x	2x+1	2x+2	2x+3	2x+4	2x	3x+1	3x+2	3x+3	3x+4	3x	4x+1	4x+2	4x+3	4x+4	4x
2	2	3	4	0	1	x+2	x+3	x+4	x	x+1	2x+2	2x+3	2x	2x	2x+1	3x+2	3x+3	3x+4	3x	3x+1	4x+2	4x+3	4x+4	4x	4x+1
3	3	4	0	1	2	x+3	x+4	x	x+1	x+2	2x+3	2x+4	2x	2x+1	2x+2	3x+3	3x+4	3x	3x+1	3x+2	4x+3	4x+4	4x	4x+1	4x+2
4	4	0	1	2	3	x+4	x	x+1	x+2	x+3	2x+4	2x	2x+1	2x+2	2x+3	3x+4	3x	3x+1	3x+2	3x+3	4x+4	4x	4x+1	4x+2	4x+3
x	x	x+1	x+2	x+3	x+4	2x	2x+1	2x+2	2x+3	2x+4	3x	3x+1	3x+2	3x+3	3x+4	4x	4x+1	4x+2	4x+3	4x+4	0	1	2	3	4
x+1	x+1	x+2	x+3	x+4	x	2x+1	2x+2	2x+3	2x+4	2x	3x+1	3x+2	3x+3	3x+4	3x	4x+1	4x+2	4x+3	4x+4	4x	1	2	3	4	0
x+2	x+2	x+3	x+4	x	x+1	2x+2	2x+3	2x+4	2x	2x+1	3x+2	3x+3	3x+4	3x	3x+1	4x+2	4x+3	4x+4	4x	4x+1	2	3	4	0	1
x+3	x+3	x+4	x	x+1	x+2	2x+3	2x+4	2x	2x+1	2x+2	3x+3	3x+4	3x	3x+1	3x+2	4x+3	4x+4	4x	4x+1	4x+2	3	4	0	1	2
x+4	x+4	x	x+1	x+2	x+3	2x+4	2x	2x+1	2x+2	2x+3	3x+4	3x	3x+1	3x+2	3x+3	4x+4	4x	4x+1	4x+2	4x+3	4	0	1	2	3
2x	2x	2x+1	2x+2	2x+3	2x+4	3x	3x+1	3x+2	3x+3	3x+4	4x	4x+1	4x+2	4x+3	4x+4	0	1	2	3	4	x	x+1	x+2	x+3	x+4
2x+1	2x+1	2x+2	2x+3	2x+4	2x	3x+1	3x+2	3x+3	3x+4	3x	4x+1	4x+2	4x+3	4x+4	4x	1	2	3	4	0	x+1	x+2	x+3	x+4	x
2x+2	2x+2	2x+3	2x+4	2x	2x+1	3x+2	3x+3	3x+4	3x	3x+1	4x+2	4x+3	4x+4	4x	4x+1	2	3	4	0	1	x+2	x+3	x+4	x	x+1
2x+3	2x+3	2x+4	2x	2x+1	2x+2	3x+3	3x+4	3x	3x+1	3x+2	4x+3	4x+4	4x	4x+1	4x+2	3	4	0	1	2	x+3	x+4	x	x+1	x+2
2x+4	2x+4	2x	2x+1	2x+2	2x+3	3x+4	3x	3x+1	3x+2	3x+3	4x+4	4x	4x+1	4x+2	4x+3	4	0	1	2	3	x+4	x	x+1	x+2	x+3
3x	3x	3x+1	3x+2	3x+3	3x+4	4x	4x+1	4x+2	4x+3	4x+4	0	1	2	3	4	x	x+1	x+2	x+3	x+4	2x	2x+1	2x+2	2x+3	2x+4
3x+1	3x+1	3x+2	3x+3	3x+4	3x	4x+1	4x+2	4x+3	4x+4	4x	1	2	3	4	0	x+1	x+2	x+3	x+4	x	2x+1	2x+2	2x+3	2x+4	2x
3x+2	3x+2	3x+3	3x+4	3x	3x+1	4x+2	4x+3	4x+4	4x	4x+1	2	3	4	0	1	x+2	x+3	x+4	x	x+1	2x+2	2x+3	2x+4	2x	2x+1
3x+3	3x+3	3x+4	3x	3x+1	3x+2	4x+3	4x+4	4x	4x+1	4x+2	3	4	0	1	2	x+3	x+4	x	x+1	x+2	2x+3	2x+4	2x	2x+1	2x+2
3x+4	3x+4	3x	3x+1	3x+2	3x+3	4x+4	4x	4x+1	4x+2	4x+3	4	0	1	2	3	x+4	x	x+1	x+2	x+3	2x+4	2x	2x+1	2x+2	2x+3
4x	4x	4x+1	4x+2	4x+3	4x+4	0	1	2	3	4	x	x+1	x+2	x+3	x+4	2x	2x+1	2x+2	2x+3	2x+4	3x	3x+1	3x+2	3x+3	3x+4
4x+1	4x+1	4x+2	4x+3	4x+4	4x	1	2	3	4	0	x+1	x+2	x+3	x+4	x	2x+1	2x+2	2x+3	2x+4	2x	3x+1	3x+2	3x+3	3x+4	3x
4x+2	4x+2	4x+3	4x+4	4x	4x+1	2	3	4	0	1	x+2	x+3	x+4	x	x+1	2x+2	2x+3	2x+4	2x	2x+1	3x+2	3x+3	3x+4	3x	3x+1
4x+3	4x+3	4x+4	4x	4x+1	4x+2	3	4	0	1	2	x+3	x+4	x	x+1	x+2	2x+3	2x+4	2x	2x+1	2x+2	3x+3	3x+4	3x	3x+1	3x+2
4x+4	4x+4	4x	4x+1	4x+2	4x+3	4	0	1	2	3	x+4	x	x+1	x+2	x+3	2x+4	2x	2x+1	2x+2	2x+3	3x+4	3x	3x+1	3x+2	3x+3

•	0	1	2	3	4	x	x+1	x+2	x+3	x+4	2x	2x+1	2x+2	2x+3	2x+4	3x	3x+1	3x+2	3x+3	3x+4	4x	4x+1	4x+2	4x+3	4x+4
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	x	x+1	x+2	x+3	x+4	2x	2x+1	2x+2	2x+3	2x+4	3x	3x+1	3x+2	3x+3	3x+4	4x	4x+1	4x+2	4x+3	4x+4
2	0	2	4	1	3	2x	2x+2	2x+4	2x+1	2x+3	4x	4x+2	4x+4	4x+1	4x+3	x	x+2	x+4	x+1	x+3	3x	3x+2	3x+4	3x+1	3x+3
3	0	3	1	4	2	3x	3x+3	3x+1	3x+4	3x+2	x	x+3	x+1	x+4	x+2	4x	4x+3	4x+1	4x+4	4x+2	2x	2x+3	2x+1	2x+4	2x+2
4	0	4	3	2	1	4x	4x+4	4x+3	4x+2	4x+1	3x	3x+4	3x+3	3x+2	3x+1	2x	2x+4	2x+3	2x+2	2x+1	x	x+4	x+3	x+2	x+1
x	0	x	2x	3x	4x	4x+3	3	x+3	2x+3	3x+3	3x+1	4x+1	1	x+1	2x+1	2x+4	3x+4	4x+4	4	x+4	x+2	2x+2	3x+2	4x+2	2
x+1	0	x+1	2x+2	3x+3	4x+4	3	x+4	2x	3x+1	4x+2	1	x+2	2x+3	3x+4	4x	4	x	2x+1	3x+2	4x+3	2	x+3	2x+4	3x	4x+1
x+2	0	x+2	2x+4	3x+1	4x+3	x+3	2x	3x+2	4x+4	1	2x+1	3x+3	4x	2	x+4	3x+4	4x+1	3	x	2x+2	4x+2	4	x+1	2x+3	3x
x+3	0	x+3	2x+1	3x+4	4x+2	2x+3	3x+1	4x+4	2	x	4x+1	4	x+2	2x	3x+3	x+4	2x+2	3x	4x+3	1	3x+2	4x	3	x+1	2x+4
x+4	0	x+4	2x+3	3x+2	4x+1	3x+3	4x+2	1	x	2x+4	x+1	2x	3x+4	4x+3	2	4x+4	3	x+2	2x+1	3x	2x+2	3x+1	4x	4	x+3
2x	0	2x	4x	x	3x	3x+1	1	2x+1	4x+1	x+1	x+2	3x+2	2	2x+2	4x+2	4x+3	x+3	3x+3	3	2x+3	2x+4	4x+4	x+4	3x+4	4
2x+1	0	2x+1	4x+2	x+3	3x+4	4x+1	x+2	3x+3	4	2x	3x+2	3	2x+4	4x	x+1	2x+3	4x+4	x	3x+1	3	x+4	3x	1	2x+2	4x+3
2x+2	0	2x+2	4x+4	x+1	3x+3	1	2x+3	4x	x+2	3x+4	2	2x+4	4x+1	x+3	3x	3	2x	4x+2	x+4	3x+1	4	2x+1	4x+3	x	3x+2
2x+3	0	2x+3	4x+1	x+4	3x+2	x+1	3x+4	2	2x	4x+3	2x+2	4x	x+3	3x+1	4	3x+3	1	2x+4	4x+2	x	4x+4	x+2	3x	3	2x+1
2x+4	0	2x+4	4x+3	x+2	3x+1	2x+1	4x	x+4	3x+3	2	4x+2	x+1	3x	4	2x+3	x+3	3x+2	1	2x	4x+4	3x+4	3	2x+2	4x+1	x
3x	0	3x	x	4x	2x	2x+4	4	3x+4	x+4	4x+4	4x+3	2x+3	3	3x+3	x+3	x+2	4x+2	2x+2	2	3x+2	3x+1	x+1	4x+1	2x+1	1
3x+1	0	3x+1	x+2	4x+3	2x+4	3x+4	x	4x+1	2x+2	3	x+3	4x+4	2x	1	3x+2	4x+2	2x+3	4	3x	x+1	2x+1	2	3x+3	x+4	4x
3x+2	0	3x+2	x+4	4x+1	2x+3	4x+4	2x+1	3	3x	x+2	3x+3	x	4x+2	2x+4	1	2x+2	4	3x+1	x+3	4x	x+1	4x+3	2x	2	3x+4
3x+3	0	3x+3	x+1	4x+4	2x+2	4	3x+2	x	4x+3	2x+1	3	3x+1	x+4	4x+2	2x	2	3x	x+3	4x+1	2x+4	1	3x+4	x+2	4x	2x+3
3x+4	0	3x+4	x+3	4x+2	2x+1	x+4	4x+3	2x+2	1	3x	2x+3	3	3x+1	x	4x+4	3x+2	x+1	4x	2x+4	2	4x+1	2x	4	3x+3	x+2
4x	0	4x	3x	2x	x	x+2	2	4x+2	3x+2	2x+2	2x+4	x+4	4	4x+4	3x+4	3x+1	2x+1	x+1	1	4x+1	4x+3	3x+3	2x+3	x+3	3
4x+1	0	4x+1	3x+2	2x+3	x+4	2x+2	x+3	4	4x	3x+1	4x+4	3x	2x+1	x+2	3	x+1	2	4x+3	3x+4	2x	3x+3	2x+4	x	1	4x+2
4x+2	0	4x+2	3x+4	2x+1	x+3	3x+2	2x+4	x+1	3	4x	x+4	1	4x+3	3x	2x+2	4x+1	3x+3	2x	x+2	4	2x+3	x	2	4x+4	3x+1
4x+3	0	4x+3	3x+1	2x+4	x+2	4x+2	3x	2x+3	x+1	4	3x+4	2x+2	x	3	4x+1	2x+1	x+4	2	4x	3x+3	x+3	1	4x+4	3x+2	2x
4x+4	0	4x+4	3x+3	2x+2	x+1	2	4x+1	3x	2x+4	x+3	4	4x+3	3x+2	2x+1	x	1	4x	3x+4	2x+3	x+2	3	4x+2	3x+1	2x	x+4

.6. Jelölések, definíciók

$\{\mathbf{x}\}$:=az $r \in \mathbb{R}$ valós szám tört része (ld. a 142 oldalon),

$\circ$:= függvények kompozíciója (összetett függvény képzése),

$\underline{\underline{0}}$, $\underline{\underline{1}}$:= az azonosan 0 ill. 1 mátrix,

$\underset{\sim}{0} := \underset{\sim}{c}$ az azonosan 0 függvény (ld. $\underset{\sim}{c}$),

$A^B := \{f : B \to A \mid f$ *függvény* $\}$ tetszőleges A halmazra,

$A^A := \{f : A \to A \mid f$ *függvény* $\}$,

$A^{\mathbb{N}} := \{s : \mathbb{N} \to A \mid s = (s_0, s_1, ...)$ *sorozat* $\}$ tetszőleges A halmazra,

$\mathcal{A}_\circ := \left(A^A, \circ\right)$ (félcsoport),

$A^n := A^{\mathbb{I}_n} = \{(a_1, ..., a_n) \mid a_i \in A\}$ = az A halmaz n -edik Descartes-hatványa ($n \in \mathbb{N}$) ,

$A^0 := \{\emptyset\}$,

$A^* := \bigcup_{n=0}^{\infty} A^n =$ az A (tetszőleges) halmaz elemeiből képezhető *összes* rendezett n -es (véges hosszú sorozat, string) halmaza,

$A_n := \{ \sigma \in S_n : \sigma$ páros $\}$,

$\mathcal{A}_n := (A_n, \circ)$ az n -edrendű **alternáló csoport**[3)] ,

$A \triangle B := (A \backslash B) \cup (B \backslash A)$ $\triangle$ = halmazok szimmetrikus differenciája,

$a \hat{} b :=$ az $a, b \in A^*$ sorozatok egymáshoz fűzése (összefűzése, konkatenációja),

$a|b :=$ a osztója b -nek, vagyis b osztható a -val,

$a \equiv_m b$ vagy $a \equiv b \pmod{m}$: $\overset{def}{\iff}$ $m|a-b$
($\Leftrightarrow$ a és b ugyanazt a maradékot adja m -el elosztva) ,

$a \approx b =$ asszociált elemek egységelemes gyűrűkben (ld.még $f(x) \approx g(x)$),

$(a, b) := lnko(a, b) :=$ a és b legnagyobb közös osztója,

[3)] **Definíció:** $\mathcal{A}_n \leq \mathcal{S}_n$ az n -edrendű **alternáló csoport**:
$A_n := \{\pi \in S_n \mid sgn(\pi) = 1\}$. $\square$

$[a,b] := lkkt(a,b) :=$ a és b legkisebb közös többszöröse,

$[H] :=$ a H részhalmaz által generált részstruktúra,

$[\underline{u}_1, ..., \underline{u}_k] :=$ az $\underline{u}_1, ..., \underline{u}_k$ vektorok által kifeszített (generált) altér,

$\underset{\sim}{c} :=$ az azonosan c függvény $(c \in A)$: $\underset{\sim}{c} : A \to A$, $\underset{\sim}{c}(x) := c$ minden $x \in A$ elemre,

$\mathbb{C}[x] :=$ komplex együtthatójú polinomok halmaza,

$\triangle =$ halmazok szimmetrikus differenciája: $A \triangle B := (A \backslash B) \cup (B \backslash A)$,

$D_n := [\{f,t\}] = \{id, f, f^2, ..., f^{n-1}, t, tf, tf^2, ..., tf^{n-1}\} =$ a szabályos n -szög transzformációcsoportja = az n -edrendű f forgatás és a másodrendű t tengelyes tükrözés által generált csoport, az ún. n -edrendű **diédercsoport**,

$D_\infty := [\{f,t\}] = \{f^r, tf^r : r \in \mathbb{R}\}$ = a *kör* transzformációcsoportja = a ∞ -edrendű f forgatás és a másodrendű tengelyes tükrözés által generált csoport, a ∞ -rendű **diédercsoport**,

$deg(p) :=$ a $p(x)$ polinom fokszáma,

$E \in \mathbb{R}^{n \times n} :=$ az egységmátrix,

$f(x) \approx g(x) \overset{def}{\iff} \lim\limits_{x \to \infty} \frac{f(x)}{g(x)} = 1$ = f és g "**aszimptotikusan egyenlőek**" $(f, g : \mathbb{R} \to \mathbb{R}$ függvények) (ld.még $a \approx b$),

$\mathcal{F}_X := (X^*, \hat{})$ az $X \neq \emptyset$ halmaz által generált **szabad félcsoport**,

$\varphi(n) =$ **Euler -féle φ függvény** := az n természetes számnál kisebb, hozzá relatív prím természetes számok száma,

$GF(q) :=$ a $q = p^n$ -edrendű véges test, azaz **Galois-test** ,

$\Gamma :=$ tetszőleges test,

$\Gamma[x] :=$ a Γ test feletti (együtthatójú) egyhatározatlanú (egyismeretlenes) polinomok halmaza,

$\Gamma_n[x] :=$ a legfeljebb n -edfokú, $\Gamma[x]$ -beli polinomok halmaza,

$\iota := \{ (a,a) \mid a \in A \}$ **egyenlőség** (reláció),

$id_A : A \to A$ az *identikus* leképezés (függvény): $id_A(a) = a$ minden $a \in A$ elemre,

$\mathbb{I}_n^0 := \{0, 1, ..., n-1\}$ ($n \in \mathbb{N}$ természetes szám),

$\mathbb{I}_n := \{1, 2, ..., n\}$ ($n \in \mathbb{N}$ természetes szám),

$\mathbb{I}_0 = \mathbb{I}_0^0 = \emptyset$ (az előzőből következik),

$\mathcal{I}_A := \{f : A \to A \mid f \text{ injektív}\}$

$(m) := \{m \cdot x : x \in \mathbb{Z}\}$ (m többszörösei) = az m által generált főideál $\mathbb{Z}$ -ben,

$o(a)$ = az a csoportelem **rendje** = legkisebb $m \in \mathbb{N}$ (ha van) amelyre $a^m = 1$,

$\mathcal{O}(g) = f$ ("**nagy ordó**"): $f, g : \mathbb{N} \to \mathbb{R}$ függvényekre: ha $c_1 g(n) < f(n) < c_2 g(n)$ valahányszor $n > n_0$ valamilyen $c_1, c_2 \in \mathbb{R}_+$ és $n_0 \in \mathbb{N}$ számokra, (ld.[$SzI'01$])

$\mathfrak{p}(x) := x$ prímosztóinak *halmaza* ($x \in \mathbb{N}$) ,

$\mathbb{P} :=$ prímszámok halmaza,

$P(X) := \{A \mid A \subseteqq X\}$ az X halmaz **hatványhalmaza** ("power set"). Néha $\mathcal{P}(X)$ -el jelöljük.

$\Pi := (T, \cdot)$ az 1-dimenziós **tórusz**, ahol $T := \{z \in \mathbb{C} \mid |z| = 1\}$.

$\mathbb{Q} :=$ racionális számok halmaza,

$\mathbb{Q}[\alpha] := \{ q_0 + q_1\alpha + q_2\alpha^2 + ... + q_{n-1}\alpha^{n-1} \mid q_i \in \mathbb{Q}\}$ a $\mathbb{Q}$ **test algebrai bővítése** *ha* $\alpha \in \mathbb{R}$ n -edrendű **algebrai szám**[4)] ,

$\mathbb{Q}(\beta) := \left\{\frac{x+\alpha\cdot y}{u+\alpha\cdot v} \mid x, y, u, v \in \mathbb{Z}\right\}$

$\mathbb{Q}_{növ} := \{f : \mathbb{Q} \to \mathbb{Q} \mid f \textit{ monoton növő függvény}\}$,

$\mathcal{Q}^{\cdot} := (\ \{1, -1, i, -i, j, -j, k, -k\}\ ,\ \cdot\ )$ a **kvaterniócsoport**: $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, a többi művelet értelemszerűen,

$\mathcal{Q} := (\ \{\ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\ \}\ ,\ +, \cdot\ )$ a **kvaterniók teste,**

[4)] **Definíció:** az $\alpha \in \mathbb{R}$ valós szám **n -edrendű algebrai szám a $\mathbb{Q}$ test felett**, ha α gyöke egy valamilyen n -edfokú racionális együtthatójú polinomnak. □

$\mathbb{R}_+ :=$ a pozitív valós számok halmaza,

$(\mathbb{R}/r, +, \cdot) := ([0, r), +, \cdot)$ a valós számok szokásos műveleteit modulo r végezzük,

$\mathbb{R}^{n\times n} :=$ $n \times n$ méretű (négyzetes) valós mátrixok halmaza,

$(\mathbb{R}^{n\times n})^* :=$ invertálható mátrixok halmaza,

$\mathbb{R}^{n\times n}_{\triangle} :=$ alsó háromszögmátrixok halmaza,

$(\mathbb{R}^{n\times n}_{\triangle})^* :=$ invertálható alsó háromszögmátrixok halmaza,

$\mathbb{R}^{n\times n}_{\nabla} :=$ felső háromszögmátrixok halmaza,

$\left(\mathbb{R}^{n\times n}_{\nabla}\right)^* :=$ invertálható felső háromszögmátrixok halmaza,

$\mathbb{R}^{n\times n}_{\diagdown} :=$ diagonális mátrixok halmaza,

$\left(\mathbb{R}^{n\times n}_{\diagdown}\right)^* :=$ invertálható diagonális mátrixok halmaza,

$\mathbb{R}^{\mathbb{R}} := \{f : \mathbb{R} \to \mathbb{R} \mid f \ \textit{függvény}\}$,

$\mathbb{R}[x] :=$ valós együtthatójú polinomok halmaza,

$\mathbb{R}[[x]] := \left\{ \sum_{n=0}^{\infty} a_n x^n : a_n \in \mathbb{R} \right\}$ valós együtthatójú, "végtelen fokú" polinomok (=**formális hatványsorok**[5]) halmaza,

$\mathbb{R}^{\mathbb{R}}_{Lin} := \{f : \mathbb{R} \to \mathbb{R} \mid f$ lineáris *függvény*[6] $\}$,

$\mathbb{R}^{\mathbb{R}}_{LinRac} :=$
$\{f : \mathbb{R} \to \mathbb{R} \mid f(x) = \frac{ax+b}{cx+d}$ lin. racionális tört*függvény*[7], $c \neq 0$ vagy $d \neq 0\}$,

$\mathbb{R}^{\mathbb{R}}_{Rac} :=$
$\{f : \mathbb{R} \to \mathbb{R} \mid f(x) = \frac{p(x)}{q(x)}$ racionális tört*függvény*[8], $c \neq 0$ vagy $d \neq 0\}$,

$S_A := \{f : A \to A \mid f$ bijekció$\}$ $(A \neq \emptyset$ tetszőleges halmaz$)$,

---

[5] vagyis a konvergenciát nem követeljük meg: $a_n \in \mathbb{R}$ *tetszőleges* számok.

[6] **Definíció:** $f : \mathbb{R} \to \mathbb{R}$ **lineáris függvény**, ha $f(x) = ax + b$ alakú $(a, b \in \mathbb{R})$.□

[7] **Definíció:** az $f(x) = \frac{ax+b}{cx+d}$ alakú $(a, b, c, d \in \mathbb{R}$, c és d egyszerre nem 0) függvényeket **lineáris racionális törtfüggvényeknek** hívjuk. □

[8] **Definíció:** az $f(x) = \frac{p(x)}{q(x)}$ alakú $(q(x) \neq 0)$ függvényeket **racionális törtfüggvényeknek** hívjuk. □

$\mathcal{S}_A := (S_A, \circ)$ = **szimmetrikus csoport** A -n,

$S_n := S_H$ ahol $H = \mathbb{I}_n = \{1, ..., n\}$,

$\mathcal{S}_n := (S_n, \circ)$ = n **-edrendű szimmetrikus csoport**,

$\mathcal{U} := A \times A = \{ (a, b) \mid a, b \in A \}$ = **teljes (univerzális) reláció**,

$\mathbb{Z}^- := \mathbb{Z} \backslash \{0\}$,

$\mathbb{Z}_m := \{0, 1, ..., m-1\}$ = a $(\mathrm{mod}\, m)$ - szerinti **maradékosztályok** ,

$\mathbb{Z}_m^* := \{ i < m : \ lnko(i, m) = 1 \}$ = mod m **redukált maradékosztályok,**

$\mathbb{Z}_{p^\infty} := \left\{ \overrightarrow{a} \in \mathbb{N}^{\mathbb{N}} : \ 0 \leq a_i < p \right\}$ = p**-adikus egészek** halmaza, rögzített (tetszőleges) $p \in \mathbb{P}$ prímszámra,

$\mathbb{Z}[\alpha] := \{a + b \cdot \alpha \mid a, b \in \mathbb{Z}\}$ = $\mathbb{Z}$ algebrai bővítése ahol $\alpha \in \mathbb{C}$ egy tetszőleges másodfokú algebrai szám (egy másodfokú valós együtthatójú egyenlet gyöke): - lásd még a 4.3.1 alfejezetet is,

$\mathbb{Z}[x]$:= egész együtthatójú polinomok halmaza

$\mathcal{Z}_A = \{f : A \to A \mid f \text{ szürjektív}\}$.

.7. Felhasznált és ajánlott irodalom

[$BCzSz$] **Bálintné Sz.Mária, Czédli Gábor, Szendrei Ágnes:** *Absztrakt algebrai feladatok*, Egyetemi jegyzet, JATE, Szeged, 1993.

[Cs] **Csákány Béla**: *Diszkrét matematikai játékok,* Polygon könyvtár, Szeged, 1998.

[FE] **Fried Ervin:** *Absztrakt algebra elemi úton*, Műszaki Kiadó, Budapest, 1975.

[J] **Jaglom,I.M.:** *Boole-struktúrák és modelljeik,* Műszaki Kiadó, Budapest, 1983.

[M] **Megyesi Zoltán:** *Titkosírások*, Polygon IV/2, (1994).

[$SA'76$] **Sárközy András:** *Számelmélet,* példatár, ("Bolyai Könyvek" sorozat), Műszaki Kiadó, Budapest, 1976.

[$SA'78$] **Sárközy András:** *Számelmélet és alkalmazásai,* ("Matematika műszakiaknak"), Műszaki Kiadó, Budapest, 1978.

[$SASJ$] **Sárközi András, Surányi János:** *Számelmélet feladatgyűjtemény*, Egyetemi jegyzet, ELTE, Budapest, 1979.

[$SzÁ$] **Szendrei Ágnes:** *Diszkrét matematika*, Polygon könyvtár, Szeged, 1994.

[$SzI'97$] **Szalkai István:** *Diszkrét matematika feladatgyűjtemény*, Veszprémi Egyetemi Kiadó, 1997.

[$SzI'01$] **Szalkai István:** *Diszkrét matematika és algoritmuselmélet alapjai*, Veszprémi Egyetemi Kiadó, 2001.

[$SzI'17$] **Szalkai István:** *Magasabbfokú kongruenciák megoldása*, Haladvány Kiadvány, 2017, http://math.bme.hu/~hujter/171229.pdf

[SzD] **Szalkai István, Dósa György:** *Algoritmikus számelmélet*, https://dtk.tankonyvtar.hu/handle/123456789/7516

[$SzSzGy$] **Szakadát István, Szőts Miklós, Gyepesi György:** *Magyar Egységes Ontológia, Extenzionális relációelmélet*, 2006, http://www.ontologia.hu/therelthe.pdf (letöltés: 2021.02.06.)

.8. Tárgymutató

(Lásd még a .6. "*Jelölések, definíciók*" c. fejezetet is.)

Tárgymutató