



Bevezetés az algebraba 1

BMETE92AX23



Egész számok 2

H406 2016-09-16



Wetttl Ferenc

ALGEBRA TANSZÉK

Prímszámok

Prímszámok

Felbonthatatlan számok, prímszámok

- D** Az 1-nél nagyobb p természetes számot **felbonthatatlan számnak** nevezzük, ha $p = ab$ ($a, b \in \mathbb{N}^+$) esetén a vagy b egyenlő eggyel.
- A 100 alattiak: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97. (OEIS A000040)
- D** Az egységtől különböző p egészt **felbonthatatlan számnak** nevezzük, ha $p = ab$ ($a, b \in \mathbb{Z}$) esetén a vagy b **egység**.
- ..., -5, -3, -2, 2, 3, 5,...
 - Az 1-nél nagyobb nem felbonthatatlan számokat **összetett számoknak** nevezzük (az első néhány: 4, 6, 8, 9, 10, 12, 14,...).
- T** Minden 1-nél nagyobb egésznek van felbonthatatlan osztója.
- B** Indirekt: t.f.h van olyan 1-nél nagyobb egész, melynek nincs felbonthatatlan osztója. Legyen n a legkisebb ilyen egész. $n \mid n$, tehát n nem felbonthatatlan $\rightsquigarrow n = ab$, ahol $1 < a < n \rightsquigarrow a$ -nak az indirekt feltevés szerint már van felbonthatatlan osztója, de az osztja n -et is, ellentmondás.

- D Az 1-nél nagyobb p természetes számot **prímszámnak** nevezzük, ha $p \mid ab$ ($a, b \in \mathbb{Z}$) esetén $p \mid a$ vagy $p \mid b$.
- D Az egészek körében az egységtől és nullától különböző p egészt **prímszámnak** nevezzük, ha $p \mid ab$ ($a, b \in \mathbb{Z}$) esetén $p \mid a$ vagy $p \mid b$.
- m A felbonthatatlanok definíciójából következik, hogy a 0 nem felbonthatatlan ($0 = 0 \cdot 2$), a prímek definíciójából azonban ki kell zárni ($0 \mid ab \rightsquigarrow ab = 0 \rightsquigarrow 0 \mid a$ vagy $0 \mid b$).
- F Mik a felbonthatatlan számok és mik a prímek a páros számok körében?

Tétel (F 1.4.3)

p pontosan akkor prím, ha felbonthatatlan.

m A tétel igaz a természetes számok és az egész számok körében is. A természetes számokra bizonyítjuk:

B (prím \Rightarrow felbonthatatlan) $p = ab \rightsquigarrow p \mid ab$, de p prím, így $p \mid a$ vagy $p \mid b$, azaz $ab \mid a$ vagy $ab \mid b \rightsquigarrow b = 1$ vagy $a = 1$, tehát p felbonthatatlan.

(felbonthatatlan \Rightarrow prím) $p \mid ab$ és $p \nmid a$ és p felbonthatatlan $\rightsquigarrow (p, a) \mid p$ miatt $(p, a) = 1 \rightsquigarrow p \mid b$.

F Mennyiben változik a fenti bizonyítás az egészek körében?

- A törzsszám, prímszám, felbonthatatlan szám kifejezéseket azonos értelemben használjuk.
- Egy bizonyítás a KÖNYV-ből:

Tétel (Euklidész)

A prímszámok száma végtelen.

Bizonyítás.

Indirekt: tegyük fel, hogy csak véges sok prím létezik: p_1, p_2, \dots, p_n . Tekintsük a $q = p_1 p_2 \dots p_n + 1$ számot. q -nak van prímosztója, de az nem egyezik meg a p_1, p_2, \dots, p_n egyikével sem, ellentmondás. □

Algoritmus (Eratoszthenészi szita)

- *Bemenet:* $[2, 3, \dots, n]$ egészek listája,
- *Kimenet:* az n -nél nem nagyobb prímek listája

1 $N \leftarrow [2, 3, \dots, n], i \leftarrow 1$

2 $p \leftarrow N[i]$

3 ha $p > \sqrt{n}$, akkor menj 6-ra

4 $j \leftarrow 2p, 3p, \dots : N[j - 1] \leftarrow 0$ (p -többszörösök kinullázása)

5 növeld i -t addig, míg $N[i] > 0$ nem lesz és menj 2-re

6 N pozitív elemeinek kiírása

T Ha $n \in \mathbb{N}^+$ összetett szám, akkor van \sqrt{n} -nél nem nagyobb prímtényezője.

B $n = ab, 1 < a \leq b < n \rightsquigarrow a \leq \sqrt{n}$.

- Eratoszthenészi szita [animáció](#)

- T Dirichlet tétel: ha a és b relatív prímek, akkor az $an + b$ ($n = 1, 2, 3, \dots$) sorozatban végtelen sok prímszám van.
- Ben Green, Terence Tao, 2006: létezik tetszőlegesen hosszú, csak prímekből álló számtani sorozat. (pl. 2, 3 – 3, 5, 7 – 5, 11, 17, 23, 29 – 7, 37, 67, 97, 127, 157 – 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089)
- T Prímszámtétel (Hadamard, de la Vallée-Poussin, 1896; elemi bizonyítás Selberg, Erdős, 1949) Az x -nél kisebb prímek $\pi(x)$ száma aszimptotikusan $x / \ln x$, azaz

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x} = 1.$$

Prímszámok

A számelmélet alaptétele

Tétel (A számelmélet alaptétele)

Minden 1-nél nagyobb természetes szám előáll véges sok felbonthatatlan természetes szám szorzataként, és e felbontás a tényezők sorrendjétől eltekintve egyértelmű.

- m A tétel kiterjeszhető az 1-re is, mint ami a prímek üres szorzatához rendelhető.
- m A „tényezők sorrendjétől eltekintve egyértelmű” helyett mondhatjuk, hogy a „felbontás egyértelmű a prímek monoton növekvő rendezése mellett”.
- D Az azonos prímek szorzatát hatvánnyal jelölve az 1-nél nagyobb egészek **kanonikus alakjához** jutunk: $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$.
- T Minden 0-tól és egységtől különböző *egész szám* sorrendtől és egységszeresektől eltekintve egyértelműen előáll felbonthatatlanok szorzataként. ($-6 = (-2) \cdot 3 = 2 \cdot (-3) = 3 \cdot (-2) = (-3) \cdot 2$)
- m Hasonló tétel nem igaz pl. a pozitív páros számok körében:
 $60 = 2 \cdot 30 = 6 \cdot 10$.

- B A felbonthatóság bizonyítása.** Indirekt: tegyük fel, hogy van olyan természetes szám, mely nem bontható fel. Legyen n közülük a legkisebb. n nem lehet felbonthatatlan, mert akkor az egyelemű szorzat a felbontás, tehát $n = ab$, ahol viszont a és b már felbonthatók, így a szorzatuk is. Ellentmondás.
- Az egyértelműség bizonyítása.** Indirekt: tegyük fel, hogy van olyan természetes szám, mely nem bontható fel egyértelműen. Legyen n közülük a legkisebb.

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s.$$

$p_i \neq q_j$ semmilyen $\{i, j\}$ párra, különben n nem volna a legkisebb. Ez ellentmond a felbonthatatlanok prímtulajdonságának, ugyanis ha $p_1 \mid q_1 q_2 \dots q_s$, akkor $p_1 \mid q_j$ valamilyen j -re, de akkor q_j felbonthatatlan volta miatt $p_1 = q_j$ vagy $p_1 = 1$. Ellentmondás.

Definíció

Két (több) nullától különböző egész szám **legkisebb közös többszöröse** az a legkisebb pozitív egész, melynek mindkét (mindegyik) szám osztója. Jelölései:

$[a, b] = \text{lkk}(a, b) = \text{lcm}(a, b)$ – least common multiple

$([a_1, a_2, \dots, a_n] = \text{lkk}(a_1, a_2, \dots, a_n) = \text{lcm}(a_1, a_2, \dots, a_n))$.

F Hogyan definiálnánk a **kitüntetett közös többszörös** fogalmát?

- Legyen $a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$, $b = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r}$ ($a_i, b_i \geq 0$,
 $i = 1, 2, \dots, r$). Ekkor

T $a \mid b \iff 0 \leq a_i \leq b_i$ ($i = 1, 2, \dots, r$).

T $(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_r^{\min(a_r, b_r)}$

T $[a, b] = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_r^{\max(a_r, b_r)}$

T Ha a és b pozitív egész, akkor $a, b = ab$.

B $\max(a_i, b_i) + \min(a_i, b_i) = a_i + b_i$,

$$p_i^{\max(a_i, b_i)} p_i^{\min(a_i, b_i)} = p_i^{\max(a_i, b_i) + \min(a_i, b_i)} = p_i^{a_i + b_i} = p_i^{a_i} p_i^{b_i}.$$

- F Mutassuk meg, hogy bármely pozitív a és b egészhez van olyan m és n egész, hogy $m \mid a$, $n \mid b$, $(m, n) = 1$ és $mn = [a, b]$.
- F **Legendre-formula:** Mutassuk meg, hogy $n!$ prímtényezős felbontásában a p prím kitevője

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

Számolás maradékokkal

Számolás maradékokkal

Kongruenciák

Definíció

$a \in \mathbb{Z}, m \in \mathbb{N}^+$. Az a -nak m -mel való osztási maradékát $a \bmod m$ jelöli. (Itt mod egy bináris, azaz kétváltozós művelet.)

P $12 \bmod 5 = 2, (-12) \bmod 5 = 3.$

Definíció

$a, b \in \mathbb{Z}, m \in \mathbb{N}^+$. Azt mondjuk, hogy a **kongruens** b -vel modulo m , ha $m \mid a - b$.

Jelölései: $a \equiv b \pmod{m}, a \equiv b \bmod m, a \equiv b (m).$

Á $m \mid a - b \iff m \mid b - a \iff a \bmod m = b \bmod m$

P $12 \equiv 107 \pmod{5}$, mert $5 \mid 107 - 12$; $-6 \equiv 99 \pmod{5}$, mert $5 \mid 99 - (-6)$.

P $13 \not\equiv 23 \pmod{9}$, mert $9 \nmid 23 - 13$.

Á $a \equiv b \pmod{m} \iff$ van olyan k egész, hogy $a = b + km$.

B $m \mid a - b \iff$ van olyan k , hogy $a - b = km \iff a = b + km.$ 12

Számolás maradékokkal

Maradékosztályok, maradékrendszerek

Tétel (A kongruencia ekvivalenciareláció)

Reflexív: $a \equiv a \pmod{m}$,

Szimmetrikus: $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$

Tranzitív: $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

- A kongruencia ekvivalenciareláció, tehát megad az egészek halmazán egy osztályozást (diszjunkt részhalmazok uniójára való felbontást): egy osztályba azok az egészek tartoznak, melyek azonos maradékot adnak a modulussal osztva. Pl.: modulo 3 a következő osztályozást adja:

$$\mathbb{Z} = \{\dots, -3, 0, 3, \dots\} \cup \{\dots, -2, 1, 4, \dots\} \cup \{\dots, -1, 2, 5, \dots\}$$

- D a fenti osztályozás osztályait **modulo m maradékosztályoknak** nevezzük.

Tétel (Műveletek és kongruenciák)

Ha $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}^+$, és $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, akkor

1. $a + c \equiv b + d \pmod{m}$ (spec. $a + c \equiv b + c \pmod{m}$)
2. $a - c \equiv b - d \pmod{m}$ (spec. $a - c \equiv b - c \pmod{m}$)
3. $ac \equiv bd \pmod{m}$ (spec. $ac \equiv bc \pmod{m}$)

P $7 \equiv 33 \pmod{13} \rightsquigarrow 27 \equiv 53 \pmod{13} \quad [+ 20]$

P $7 \equiv 33 \pmod{13} \rightsquigarrow 70 \equiv 330 \pmod{13} \quad [\cdot 10]$

P $7 \equiv 33 \pmod{13}$, $4 \equiv 30 \pmod{13} \rightsquigarrow 28 \equiv 990 \pmod{13}$

P $a \equiv b \pmod{m}$, $n \in \mathbb{N}^+ \rightsquigarrow a^n \equiv b^n \pmod{m}$

1M n -szer összeszorozva az $a \equiv b \pmod{m}$ kongruenciát;

2M az $a^n - b^n = (a - b)(a^{n-1} + \dots + b^{n-1})$ összefüggésből.

T **Mersenne-prímek:** mutassuk meg, hogy ha $a^n - 1$ prím, ahol a és n is 1-nél nagyobb egészek, akkor $a = 2$, és n prím.

Tétel (Egyszerűsítés kongruenciában)

Ha $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}^+$, $d = (c, m)$ és $ac \equiv bc \pmod{m}$,
akkor

$$a \equiv b \pmod{\frac{m}{d}}$$

Ha $(c, m) = 1$, akkor az $ac \equiv bc \pmod{m}$ kongruencia
egyszerűsíthető c -vel, azaz ekkor $a \equiv b \pmod{m}$.

- B** $ac \equiv bc \pmod{m} \rightsquigarrow m \mid (a - b)c \rightsquigarrow \exists k : (a - b)c = km \rightsquigarrow$
 $(a - b)\frac{c}{d} = k\frac{m}{d}$. $(\frac{c}{d}, \frac{m}{d}) = 1$, ezért $\frac{m}{d} \mid a - b \rightsquigarrow a \equiv b \pmod{\frac{m}{d}}$.
- P** $14 \equiv 40 \pmod{13} \rightsquigarrow 7 \equiv 20 \pmod{13} \quad [/2]$
- P** $18 \equiv 66 \pmod{24} \rightsquigarrow 3 \equiv 11 \pmod{4} \quad [/6] (6 = (18, 66))$

T Ha $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_n}$, ahol $a, b \in \mathbb{Z}$,
 $m_1, \dots, m_n \in \mathbb{N}^+$, akkor

$$a \equiv b \pmod{[m_1, m_2, \dots, m_n]}.$$

B $m_1 \mid (a - b), m_2 \mid (a - b), \dots, m_n \mid (a - b) \rightsquigarrow$
 $[m_1, m_2, \dots, m_n] \mid (a - b).$

P Oldjuk meg fejben a következő három kongruenciarendszert!

(a) $x \equiv 1 \pmod{3}$	(b) $x \equiv 2 \pmod{3}$	(c) $x \equiv 1 \pmod{3}$
$x \equiv 1 \pmod{5}$	$x \equiv 4 \pmod{5}$	$x \equiv 2 \pmod{4}$
$x \equiv 1 \pmod{7}$	$x \equiv 6 \pmod{7}$	$x \equiv 3 \pmod{5}$

Definíció

Egészek egy halmaza **teljes maradékrendszer modulo m** (**TMR mod m**), ha minden egész szám e halmaznak pontosan egy elemével kongruens mod m .

P A $\{0, 1, \dots, m - 1\}$ halmaz TMR modulo m .

P Ha m páros, akkor a $\{-\frac{m-2}{2}, \dots, 0, \dots, \frac{m-2}{2}, \frac{m}{2}\}$ halmaz, ha m páratlan, akkor a $\{-\frac{m-1}{2}, -\frac{m-3}{2}, \dots, 0, \dots, \frac{m-3}{2}, \frac{m-1}{2}\}$ halmaz TMR modulo m .

P A $\{0, 1, 2, 4, 8\}$ halmaz TMR modulo 5.

P A $\{0, 1, 3, 9, 27, 81, 243\}$ halmaz TMR mod 7.

Á m inkongruens egész szám halmaza TMR modulo m .

T Ha $\{t_1, t_2, \dots, t_m\}$ TMR modulo m , és $(a, m) = 1$, akkor $\{at_1 + b, at_2 + b, \dots, at_m + b\}$ is TMR mod m .

B $at_i + b \equiv at_j + b \pmod{m} \iff at_i \equiv at_j \pmod{m} \iff t_i \equiv t_j \pmod{m}$ (mert $(a, m) = 1$) $\iff i = j$. Így ez m inkongruens egész halmaza.

P Számítsuk ki $91^{89} \bmod 11$ értékét! $91^{89} = 22629966787881178104507938630530359755911966$
 $066400099150045124000595605179349487522472134992988$
 $960788694682422515792592896836945711385013041867663$
 $39290205991707879310835543611 \equiv 4 \pmod{11}$

1M $91 \bmod 11 = 3$, $89 = 1011001_2$, $3^2 \bmod 11 = 9$, $3^4 \bmod 11 = 4$,
 $3^8 \bmod 11 = 5$, $3^{16} \bmod 11 = 3$, $3^{32} \bmod 11 = 9$, $3^{64} \bmod 11 = 4$.
 $91^{89} \equiv 3^{89} = 3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3 \equiv 4 \cdot 3 \cdot 5 \cdot 3 \equiv 4 \pmod{11}$.

2M k a r megjegyzések

89	3	1	induló értékek	
88	3	3	$k \leftarrow k - 1, r \leftarrow r \cdot a \bmod m$	$a \leftarrow 3$
44	9	3	$k \leftarrow k/2, a \leftarrow a \cdot a \bmod m$	$a \leftarrow 3^2 \bmod 11$
22	4	3	$k \leftarrow k/2, a \leftarrow a \cdot a \bmod m$	$a \leftarrow 3^4 \bmod 11$
11	5	3	$k \leftarrow k/2, a \leftarrow a \cdot a \bmod m$	$a \leftarrow 3^8 \bmod 11$
10	5	4	$k \leftarrow k - 1, r \leftarrow r \cdot a \bmod m$	$r \leftarrow 3^8 \cdot 3 \bmod 11$
5	3	4	$k \leftarrow k/2, a \leftarrow a \cdot a \bmod m$	$a \leftarrow 3^{16} \bmod 11$
4	3	1	$k \leftarrow k - 1, r \leftarrow r \cdot a \bmod m$	$r \leftarrow 3^{16} \cdot 3^8 \cdot 3 \bmod 11$
2	9	1	$k \leftarrow k/2, a \leftarrow a \cdot a \bmod m$	$a \leftarrow 3^{32} \bmod 11$
1	4	1	$k \leftarrow k/2, a \leftarrow a \cdot a \bmod m$	$a \leftarrow 3^{64} \bmod 11$
0	4	4	$k \leftarrow k - 1, r \leftarrow r \cdot a \bmod m$	$r \leftarrow 3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3 \bmod 11$

Legyen $k = (b_n \dots b_1 b_0)_2$, ekkor $a^k = a^{\sum_{i=0}^n b_i 2^i} = \prod_{i=0}^n (a^{2^i})^{b_i}$, így

$$a^k \bmod m = \prod_{i=0}^n (a^{2^i})^{b_i} \bmod m = \prod_{i=0}^n \left((a^{2^i})^{b_i} \bmod m \right) \bmod m$$

Algoritmus (Moduláris hatványozás)

- *Bemenet:* a alap, k kitevő, m modulus, ahol $a, k, m \in \mathbb{N}_0$, $m > 1$
 - *Kimenet:* $r = a^k \bmod m$
- 1 $b \leftarrow b \bmod m, r = 1$
 - 2 ha $k = 0$, menj 6-ra
 - 3 ha $k \bmod 2 = 1$, akkor $r \leftarrow r \cdot a \bmod m$
 - 4 $k \leftarrow \lfloor k/2 \rfloor, a \leftarrow a \cdot a \bmod m$
 - 5 menj 2-re
 - 6 r kiírása

- Két egész szám összegének, különbségének, szorzatának, egy egész szám nemnegatív egész kitevős hatványának maradéka modulo m csak attól függ, hogy az összeadandók, a szorzandók, illetve a hatványozás alapja mely maradékosztályba tartoztak (a hatványozás kitevőjére ez nem igaz!).

D Legyen $\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}$ és definiáljuk a $\langle \mathbb{Z}_m, \oplus, \otimes \rangle$ struktúrát a következőképp: ha $a, b \in \mathbb{Z}_n$, akkor $a \oplus b := a + b \bmod m$, $a \otimes b := a \cdot b \bmod m$.

P Írjuk fel \mathbb{Z}_2 műveletábráit:

\oplus	0	1		\otimes	0	1
0	0	1		0	0	0
1	1	0		1	0	1

- A továbbiakban – ha félreértést nem okoz – \mathbb{Z}_n alatt a $\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ algebrai struktúrát értjük, amelynek műveleteire is inkább a '+' és '·' jeleket használjuk, azaz $\mathbb{Z}_n = \langle \mathbb{Z}_n, +, \cdot \rangle$.

P Írjuk fel \mathbb{Z}_3 , \mathbb{Z}_5 és \mathbb{Z}_6 műveletábráit:

+	0	1	2	×	0	1	2
0	0	1	2	0	0	0	0
1	1	2	0	1	0	1	2
2	2	0	1	2	0	2	1

+	0	1	2	3	4	×	0	1	2	3	4
0	0	1	2	3	4	0	0	0	0	0	0
1	1	2	3	4	0	1	0	1	2	3	4
2	2	3	4	0	1	2	0	2	4	1	3
3	3	4	0	1	2	3	0	3	1	4	2
4	4	0	1	2	3	4	0	4	3	2	1

+	0	1	2	3	4	5	·	0	1	2	3	4	5
0	0	1	2	3	4	5	0	0	0	0	0	0	0
1	1	2	3	4	5	0	1	0	1	2	3	4	5
2	2	3	4	5	0	1	2	0	2	4	0	2	4
3	3	4	5	0	1	2	3	0	3	0	3	0	3
4	4	5	0	1	2	3	4	0	4	2	0	4	2
5	5	0	1	2	3	4	5	0	5	4	3	2	1

- A fenti művelet táblákról leolvasható, hogy minden elemnek van **ellentettje (additív inverze)**. Ez általánosan is igaz minden \mathbb{Z}_n -ben ($n \in \mathbb{N}^+$).
- Sőt, az $a + x = b$ minden $n \in \mathbb{N}^+$ esetén megoldható tetszőleges $a, b \in \mathbb{Z}_n$ esetén.
- Az \mathbb{Z}_n -ben $n = 2, 3, 5$ esetén minden zérustól különböző elemnek van **reciproka (multiplikatív inverze)**.
- Az $a \cdot x = b$ ($a, b \in \mathbb{Z}_n, a \neq 0$) egyenletek $n = 2, 3, 5$ esetén egyértelműen megoldhatók.
- A $2 \cdot x = 3$ nem oldható meg \mathbb{Z}_6 -ban!

Á Az alábbi három állítás ekvivalens \mathbb{Z}_n -ben:

1. Bármely $a \in \mathbb{Z}_n, a \neq 0$ elemnek van multiplikatív inverze.
2. Bármely $a, b \in \mathbb{Z}_n, a \neq 0$ elemekre az $a \cdot x = b$ egyenlet megoldható (a szorzás invertálható).
3. n prím.

- Mivel $(a, m) = 1 \iff (a + km, m) = 1$, ezért ha egy modulo m maradékosztály egy eleme relatív prím m -hez, akkor az összes tagja is! Így beszélhetünk az m -hez relatív prím maradékosztályokról!

D **Modulo m redukált maradékrendszernek (RMR)** nevezzük egészek egy R halmazát, ha minden m -hez relatív prím maradékosztályból R pontosan egy elemet tartalmaz.

Á Az $\{1, 2, \dots, m - 1\}$ halmaz m -hez relatív prím elemei RMR-t alkotnak modulo m .

D Az m -hez relatív prím maradékosztályok számát $\varphi(m)$ -mel jelöljük, és Euler-féle φ -függvénynek nevezzük.

P $\{1, 5\}, \{5, 7\}, \{1, 11\}$ RMR-ek modulo 6, $\varphi(6) = 2$.

P $\{1, 5, 7, 11, 13, 17, 19, 23\}$ RMR mod 24, $\varphi(24) = 8$.

T Ha $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ egy redukált maradékrendszer modulo m , és $(a, m) = 1$, akkor $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$ is RMR modulo m .

B $(a, m) = 1$ és $(r_i, m) = 1 \rightsquigarrow (ar_i, m) = 1$,
 $ar_i \equiv ar_j \pmod{m}, (a, m) = 1 \rightsquigarrow r_i \equiv r_j \pmod{m}$,
tehát minden RMR-ből egyetlen reprezentánsunk van, tehát e halmaz RMR.

P $R_{12} = \{1, 5, 7, 11\}$ RMR mod 12. Mivel $(5, 12) = 1$, ezért $R'_{12} = \{5 \cdot 1, 5 \cdot 5, 5 \cdot 7, 5 \cdot 11\}$ is redukált maradékrendszer mod 12.

P $\prod R_{12} \equiv \prod R'_{12} \pmod{12}$, mivel a két halmaz azonos elemeket tartalmaz mod 12 (mindkettő RMR), azaz

$$1 \cdot 5 \cdot 7 \cdot 11 \equiv (5 \cdot 1) \cdot (5 \cdot 5) \cdot (5 \cdot 7) \cdot (5 \cdot 11) \pmod{12}$$

Ha egyszerűsítünk $1 \cdot 5 \cdot 7 \cdot 11$ -gyel, kapjuk

$$1 \equiv 5^4 \pmod{12}.$$

Tétel (Euler–Fermat-tétel)

Ha $m \in \mathbb{N}^+$, $a \in \mathbb{Z}$ és $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

- B** Legyen $R_m = \{r_1, r_2, \dots, r_{\varphi(m)}\}$ egy redukált maradékrendszer modulo m , és mivel $(a, m) = 1$, ezért $R'_m = \{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$ is RMR modulo m .

$$r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \equiv (ar_1) \cdot (ar_2) \cdot \dots \cdot (ar_{\varphi(m)}) \pmod{m},$$

egyszerűsítés után: $1 \equiv a^{\varphi(m)} \pmod{m}$.

Következmény („Kis” Fermat-tétel (első alak))

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

Következmény („Kis” Fermat-tétel (második alak))

Ha p prímszám, $a \in \mathbb{Z}$, akkor $a^p \equiv a \pmod{p}$.

Tétel

Ha $m = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$, ahol p_1, p_2, \dots, p_t prímszámok, akkor

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

B Logikai szita-formulával:

$$\varphi(m) = m - \frac{m}{p_1} - \dots - \frac{m}{p_t} + \frac{m}{p_1 p_2} + \dots = m \prod_{i=1}^t \left(1 - \frac{1}{p_i}\right).$$

Számolás maradékokkal

Lineáris kongruenciák

Tétel (Lineáris kongruenciák megoldhatósága és megoldásainak száma)

$a, b \in \mathbb{Z}$, $m \in \mathbb{N}^+$, $(a, m) = d$. Az $ax \equiv b \pmod{m}$ kongruencia pontosan akkor oldható meg, ha $d \mid b$. Ha megoldható, akkor pontosan d inkongruens megoldása van mod m .

B (Megoldhatóság) $ax \equiv b \pmod{m}$ megoldható \iff

$$\exists y : ax - my = b \iff d \mid b.$$

(Megoldások száma) $ax - my = b$ megoldásai: $x = x_0 + \frac{m}{d}t$,
 $y = y_0 + \frac{a}{d}t$. Meghatározandó, hogy az $x = x_0 + \frac{m}{d}t$ megoldások hány maradékosztályba esnek mod m , azaz hány inkongruens megoldás található köztük.

$$\begin{aligned}x_0 + \frac{m}{d}t_1 &\equiv x_0 + \frac{m}{d}t_2 \pmod{m} \iff \frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \pmod{m} \\ &\iff t_1 \equiv t_2 \pmod{d}, \text{ ugyanis } (m, \frac{m}{d}) = \frac{m}{d}, \text{ és } m / (\frac{m}{d}) = d.\end{aligned}$$

P Oldjuk meg a $12x \equiv 15 \pmod{21}$ kongruenciát!

M A kongruencia megoldható, mert $(12, 21) = 3 \mid 15$.

Ekvivalens diofantoszi egyenlet: $12x - 21y = 15$.

Az euklideszi algoritmusból: $3 = 2 \cdot 12 + (-1) \cdot 21 \rightsquigarrow$

$15 = 10 \cdot 12 - 5 \cdot 21$, amiből az összes megoldás:

$x \equiv 10 \pmod{21}$, $x \equiv 10 + 7 \equiv 17 \pmod{21}$, $x \equiv 10 + 2 \cdot 7 \equiv 24 \equiv 3 \pmod{21}$.

D Ha $a \in \mathbb{Z}$ és $(a, m) = 1$, akkor az $ax \equiv 1 \pmod{m}$ kongruencia egy megoldását az **a elem moduláris inverzének** nevezzük modulo m .

P Határozzuk meg az 5 moduláris inverzeit modulo 26.

M $(5, 26) = 1$, tehát az $5x \equiv 1 \pmod{26}$ kongruencia megoldható.

$1 = (-5) \cdot 5 + 26 \rightsquigarrow x \equiv -5$ egy inverz (az összes: $x \equiv -5 \equiv 21 \pmod{26}$), azaz $x = -5 + 26k$.

P Oldjuk meg az $5x \equiv 7 \pmod{26}$ kongruenciát az előző példát használva!

M $(-5) \cdot 5 \equiv 1 \pmod{26} \rightsquigarrow 7 \cdot (-5) \cdot 5 \equiv 7 \pmod{26} \rightsquigarrow x \equiv -35 \equiv 17 \pmod{26}$

- T** Ha p prím, a \mathbb{Z}_p algebrai struktúrában az összeadás kommutatív, asszociatív, invertálható művelet (azaz az $a + x = b$ egyenlet \mathbb{Z}_p -ben megoldható), a szorzás kommutatív, asszociatív, és a $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ halmazon invertálható (azaz az $a \cdot x = b$ egyenlet megoldható \mathbb{Z}_p^* -ban, ha $a, b \in \mathbb{Z}_p^*$), végül a szorzás az összeadásra nézve disztributív.
- m** Ugyanezekkel a tulajdonságokkal rendelkezik \mathbb{R} és \mathbb{Q} is, ezeket a struktúrákat **testeknek** fogjuk nevezni.
- m** \mathbb{Z}_m -ben, ha m nem prím, a szorzás nem invertálható, de kommutatív. Az ilyen algebrai struktúrákat **kommutatív gyűrűknek** nevezzük.
- m** Minden test egyúttal kommutatív gyűrű is.

- F A \mathbb{Z}_m gyűrűben mik az egységek?
- M A \mathbb{Z}_m gyűrű egy modulo n redukált maradékrendszer elemeivel reprezentált elemei.
- F Elem invertálhatósága (additív inverz az ellentett, multiplikatív inverz a reciprok) és művelet (összeadás, szorzás) invertálhatósága két különböző dolog, de szoros kapcsolatban állnak. Mi a kapcsolat?
- F Adjunk definíciót a test és a kommutatív gyűrű fogalmára, melyben művelet invertálhatósága helyett elem invertálhatósága szerepel.
- P Számítsuk ki \mathbb{Z}_{11} -ben a $\frac{7}{3^{89}}$ értékét!
- M Korábban kiszámoltuk: $3^{89} = 4$, és $\frac{7}{4} = 10$, tehát \mathbb{Z}_{11} -ben $\frac{7}{3^{89}} = 10$.

Számolás maradékokkal

Kínai maradéktétel

Tétel (Kínai maradéktétel)

Legyenek m_1, m_2, \dots, m_n pozitív, páronként relatív prím egészek, és legyen $M = m_1 m_2 \dots m_n$. Az

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

\vdots

$$x \equiv a_n \pmod{m_n}$$

kongruenciarendszer egyértelműen megoldható modulo M .

B Legyen $M_k = M/m_k = m_1 \dots m_{k-1} m_{k+1} \dots m_n$. Mivel $(M_k, m_k) = 1$, ezért az $M_k x_k \equiv 1 \pmod{m_k}$ kongruencia minden k -ra egyértelműen megoldható. Tekintsük az

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 + \dots + a_n M_n x_n$$

összeget. Ez egyrészt megoldása mindegyik kongruenciának (mert pl. $a_1 M_1 x_1 \equiv a_1 \cdot 1 \equiv a_1 \pmod{m_1}$, de $a_k M_k x_k \equiv 0 \pmod{m_1}$, ha $k \neq 1$, mert $M_k \equiv 0 \pmod{m_1}$). Másrészt, ha x' egy másik megoldás, akkor $x \equiv x' \pmod{m_k}$, azaz $m_k \mid (x - x')$, következésképp $M \mid (x - x')$, tehát a megoldás egyértelmű mod M .

P Oldjuk meg az

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 4 \pmod{7}$$

kongruenciarendszert!

1M A bizonyítás alapján: $M = 105$, $M_1 = 35$, $M_2 = 21$, $M_3 = 15$,

$$M_1x_1 \equiv 1 \pmod{3} \rightsquigarrow x_1 = 2,$$

$$M_2x_2 \equiv 1 \pmod{5} \rightsquigarrow x_2 = 1,$$

$$M_3x_3 \equiv 1 \pmod{7} \rightsquigarrow x_3 = 1,$$

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 4 \cdot 15 \cdot 1 \pmod{105} = 140 + 63 + 60 \pmod{105} = 53.$$

2M $x \equiv 2 \pmod{3} \rightsquigarrow x = 3k + 2$,

$$3k + 2 \equiv 3 \pmod{5} \rightsquigarrow k = 5l + 2 \rightsquigarrow x = 3(5l + 2) + 2 = 15l + 8,$$

$$15l + 8 \equiv 4 \pmod{7} \rightsquigarrow l \equiv 3 \pmod{7} \rightsquigarrow l = 7n + 3 \rightsquigarrow$$

$$x = 15(7n + 3) + 8 = 105n + 53$$

Számolás maradékokkal

Néhány egyszerű alkalmazás

P 2-nek melyik hatványaival osztható 19753072?

M $2 \mid 2, 4 \mid 72, 8 \mid 72, 16 \mid 3072$, de $32 \nmid 53072$, tehát 2^4 a 2 legnagyobb hatványa, mellyel osztható.

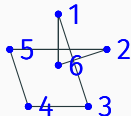
P Igazoljuk, hogy egy pozitív egész 9-cel való osztási maradéka megegyezik számjegyei összegének 9-cel való osztási maradékával!

M $a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0 \equiv$
 $a_n + a_{n-1} + \dots + a_1 10 + a_0 \pmod{9}$

P Mi a 11-gyel való oszthatóság szabálya?

M $a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0 \equiv$
 $a_n (-1)^n + a_{n-1} (-1)^{n-1} + \dots - a_1 + a_0 \pmod{11}$

P Legyen n páros pozitív egész. Bonyolítsunk le egy $n - 1$ -fordulós körmérkőzést n induló esetén.



M A k -adik fordulóban a k -adik játékos az n -edikkel játszik. Az i -edik és j -edik játékos a k -adik fordulóban játszik, ha $i + j \equiv 2k \pmod{n - 1}$, ahol $k = 1, 2, \dots, n - 1$.

E kongruencia minden i, j pár esetén egyértelműen megoldható k -ra, mivel $2 \nmid n - 1$, és egyértelműen megoldható i -re vagy j -re is, ha a másik két szám adva van.

P A magyar személyi szám $1 + 6 + 3 + 1 = 11$ jegyű, és

$$x_{11} \equiv \sum_{i=1}^{10} ix_i \pmod{11}$$

Milyen hibákat jelez ez a módszer, és miért jobb, mint mod 10?

P ISBN-13 és EAN (European Article Number):

$$x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + \dots + 3x_{12} + x_{13} \equiv 0 \pmod{10}$$

F Öröknapár: Jelölje a YYYY-MM-DD formátumban megadott dátum évszámát y , hónapjának sorszámát m , napját d azzal a módosítással, hogy január sorszáma 13, februáré 14 legyen, és ekkor az évszám csökkenjen eggyel. Tehát pl. 2015-01-15 alakja 2014-13-15 legyen, azaz $y = 2014$, $m = 13$, $d = 15$: Hasonlóképp 2000-02-11 esetén $y = 1999$, $m = 14$, $d = 11$. A hét napjainak sorszámát jelölje w , ahol hétfőn $w = 1, \dots$, vasárnap $w = 7$ (a megfelelő ISO-szabványnak megfelelően). Igazoljuk, hogy a következő képlet megadja, hogy egy dátum a Gregorián naptár szerint a hét mely napjára esik:

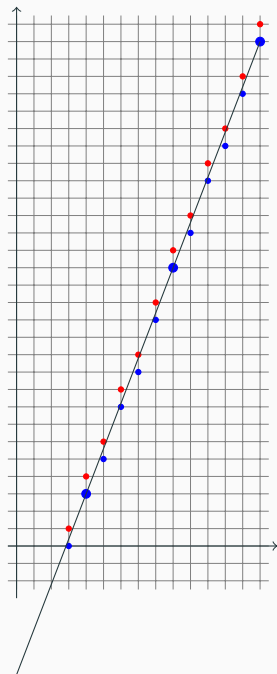
$$w = \left(\left(d + \left\lfloor \frac{13m - 32}{5} \right\rfloor + y + \left\lfloor \frac{y}{4} \right\rfloor - \left\lfloor \frac{y}{100} \right\rfloor + \left\lfloor \frac{y}{400} \right\rfloor \right) \bmod 7 \right) + 1$$

M Egy hónapon belül $w = (d + C_1 \bmod 7) + 1$ (hogy w ne a $[0, 6]$, hanem az $[1, 7]$ intervallumba essen), ahol C_1 egész.

- $365 \equiv 1 \pmod{7}$, ezért minden év egyet ad w -hez: $w = (d + y + C_2 \pmod{7}) + 1$
- A szökőévek még egyet: $w = (d + y + \lfloor \frac{y}{4} \rfloor - \lfloor \frac{y}{100} \rfloor + \lfloor \frac{y}{400} \rfloor + C_3 \pmod{7}) + 1$
- A hónapok változó hozzájárulása:

M	Á	M	J	J	A	S	O	N	D	J	F
3	4	5	6	7	8	9	10	11	12	13	14
31	30	31	30	31	31	30	31	30	31	31	28
3	2	3	2	3	3	2	3	2	3	3	
0	3	5	8	10	13	16	18	21	23	26	29

- Innen jön még $\frac{13}{5}m - \frac{37}{5}$,
- Végül egy konkrét dátummal meghatározzuk C értékét ($= 1$). Ezt az előző tört konstans tagjához adva $-\frac{32}{5}$ -öt kapunk.



P 2016-09-23

M $y = 2015, m = 9, d = 18,$

$$\begin{aligned}w &= \left(\left(18 + \left\lfloor \frac{13 \cdot 9 - 32}{5} \right\rfloor + 2015 + \left\lfloor \frac{2015}{4} \right\rfloor - \left\lfloor \frac{2015}{100} \right\rfloor + \left\lfloor \frac{2015}{400} \right\rfloor \right) \bmod 7 \right) + 1 \\ &= (4 + 3 + 6 + 6 - 6 + 5) \bmod 7 + 1 = 5 = \text{péntek}\end{aligned}$$