Diszkrét matematika II.
2. előadás

Fancsali Szabolcs Levente
nudniq@inf.elte.hu

ELTE IK Komputeralgebra Tanszék

Mérai László diái alapján

Felbonthatatlanok, prímek (múlt heti anyag!)

Emlékeztető: t felbonthatatlan: csak triviális osztói vannak: ε, t, $\varepsilon \cdot t$ típusú osztók (ahol ε egy egység). **Más szavakkal:**

t felbonthatatlan: $t = ab \Rightarrow a$ vagy b egység.

p prím: $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.

p prím $\Rightarrow p$ felbonthatatlan.

Az egész számok körében a fordított irány is igaz:

Tétel

Minden felbonthatatlan szám prímszám.

Bizonyítás

Legyen p felbonthatatlan, és legyen $p \mid ab$. Tfh. $p \nmid b$. Ekkor p és b relatív prímek. A bővített euklideszi algoritmussal kaphatunk x, y egészeket, hogy $px + by = 1$. Innen $pax + aby = a$. Mivel p osztója a baloldalnak, így osztója a jobboldalnak is: $p \mid a$. □

Számelmélet alaptétele (múlt heti anyag!)

Tétel

Minden nem-nulla, nem egység egész szám sorrendtől és asszociáltaktól eltekintve egyértelműen felírható prímszámok szorzataként.

Bizonyítás

Csak nemnegatív számokra.
Létezés: Indukcióval: $n = 2$, $n = 3$ esetén igaz (prímek). Általában ha n prím, akkor készen vagyunk, ha nem, akkor szorzatra bomlik nemtriviális módon. A tényezők már felbonthatók indukció alapján.
Egyértelműség: Indukcióval: $n = 2$, $n = 3$ esetén igaz (prímek). Tfh. $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$, ahol $p_1, p_2 \cdots, p_k, q_1, q_2, \ldots, q_\ell$ prímek. p_1 osztja a bal oldalt $\Rightarrow$ osztja a jobb oldalt, felthehető $p_1 = q_1$.
Egyszerűsítve: $n' = p_2 \cdots p_k = q_2 \cdots q_\ell$. Indukció alapján ez már egyértelmű. $\square$

Számelmélet alaptétele (múlt heti anyag!)

Definíció

Egy n nem-nulla egész szám kanonikus alakja:

$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell} = \pm \prod_{i=1}^{\ell} p_i^{\alpha_i}$, ahol p_1, p_2,..., p_ℓ pozitív prímek, α_1, α_2,..., α_ℓ pozitív egészek.

Következmény (HF)

Legyenek n, $m > 1$ pozitív egészek: $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$, $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_\ell^{\beta_\ell}$, (ahol most α_i, $\beta_i \geq 0$ nemnegatív egészek!).
Ekkor

$(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_\ell^{\min\{\alpha_\ell,\beta_\ell\}}$,

$[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_\ell^{\max\{\alpha_\ell,\beta_\ell\}}$,

$(a, b) \cdot [a, b] = a \cdot b$.

Osztók száma (múlt heti anyag!)

Definíció

Egy $n > 1$ egész esetén legyen $\tau(n)$ az n pozitív osztóinak száma.

Példa

$\tau(6) = 4$: osztók: 1, 2, 3, 6; $\tau(96) = 12$: osztók: 1, 2, 3, 4, 6, 8, ...

Tétel

Legyen $n > 1$ egész, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$ kanonikus alakkal. Ekkor $\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 2) \cdots (\alpha_\ell + 1)$.

Bizonyítás

n lehetséges osztóit úgy kapjuk, hogy a $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_\ell^{\beta_\ell}$ kifejezésben az összes β_i kitevő végigfut a $\{0, 1, \ldots, \alpha_i\}$ halmazon. Így ez a kitevő $\alpha_i + 1$ féleképpen választható. □

Példa

$\tau(2 \cdot 3) = (1 + 1) \cdot (1 + 1)$; $\tau(2^5 \cdot 3) = (5 + 1) \cdot (1 + 1)$.

Prímekről (múlt heti anyag!)

Tétel (Euklidesz)

Végtelen sok prím van.

Bizonyítás

Indirekt tfh csak véges sok prím van. Legyenek ezek $p_1, \ldots, p_k$. Tekintsük az $n = p_1 \cdots p_k + 1$ számot. Ez nem osztható egyetlen $p_1, \ldots, p_k$ prímmel sem, igy n prímtényezős felbontásában kell szerepelnie egy újabb prímszámnak. □

Tétel (Dirichlet, NB)

Ha a, d egész számok, $d > 0$, $(a, d) = 1$, akkor végtelen sok $ak + d$ alakú prím van.

Prímekről (múlt heti anyag!)

Prímszámtétel: x-ig a prímek száma $\sim \frac{x}{\ln x}$. (Sok prím van!)

Prímek száma:

x	prímek száma	$x/\ln x$
10	4	$4,343$
100	25	$21,715$
1000	168	$144,765$
10000	1229	$1085,736$

Erathoszthenész szitája: Keressük meg egy adott n-ig az összes prímet. Soroljuk fel 2-től n-ig az egész számokat. Ekkor 2 prím. A 2 (valódi) többszörösei nem prímek, ezeket huzzuk ki. A következő szám 3 szintén prím. A 3 (valódi) többszörösei nem prímek, ezeket huzzuk ki...
Ismételjük az eljárást $\sqrt{n}$-ig. A ki nem húzott számok mind prímek.

Kongruenciák (múlt heti anyag!)

Oszthatósági kérdésekben sokszor csak a maradékos osztás esetén csak a maradék fontos:

- hét napjai;
- órák száma, ...

Példa

$16 \bmod 3 = 1$ $4 \bmod 3 = 1$: 3-mal való oszthatóság esetén 16 "=" 4.

Definíció

Legyenek a, b, m egészek, akkor $a \equiv b \mod m$ (a és b kongruensek), ha $m \mid a - b$, és $a \not\equiv b \mod m$ (a és b inkongruensek), ha $m \nmid a - b$.

Ekvivalens megfogalmazás: $a \equiv b \mod m \Leftrightarrow a \bmod m = b \bmod m$, azaz m-mel osztva ugyan azt az osztási maradékot adják.

Példa

$16 \equiv 4 \mod 3$ u.i. $3 \mid 16 - 4 \Leftrightarrow 16 \bmod 3 = 1 = 4 \bmod 3$;
$16 \equiv 4 \mod 2$ u.i. $2 \mid 16 - 4 \Leftrightarrow 16 \bmod 2 = 0 = 4 \bmod 2$;
$16 \not\equiv 4 \mod 5$ u.i. $5 \nmid 16 - 4 \Leftrightarrow 16 \bmod 5 = 1 \neq 4 = 4 \bmod 5$.

Kongruencia tulajdonságai (múlt heti anyag!)

Tétel

Minden a, b, c, d és m egész számra igaz

1. $a \equiv a \mod m$; (reflexív)
2. $a \equiv b \mod m$, $m' \mid m \Rightarrow a \equiv b \mod m'$;
3. $a \equiv b \mod m \Rightarrow b \equiv a \mod m$; (szimmetrikus)
4. $a \equiv b \mod m$, $b \equiv c \mod m \Rightarrow a \equiv c \mod m$; (tranzitív)
5. $a \equiv b \mod m$, $c \equiv d \mod m \Rightarrow a + c \equiv b + d \mod m$;
6. $a \equiv b \mod m$, $c \equiv d \mod m \Rightarrow ac \equiv bd \mod m$.

Bizonyítás

1. $m \mid 0 = a - a$;
2. $m' \mid m \mid a - b \Rightarrow m' \mid a - b$;
3. $m \mid a - b \Rightarrow m \mid b - a = -(a - b)$;
4. $m \mid a - b$, $m \mid b - c \Rightarrow m \mid a - c = (a - b) + (b - c)$;
5. $m \mid a - b$, $m \mid c - d \Rightarrow m \mid (a + c) - (b + d) = (a - b) + (c - d)$;
6. $a = q_1 m + b$, $c = q_2 m + d \Rightarrow$
   $ac = (q_1 m + b)(q_2 m + d) = m(q_1 q_2 m + q_1 d + q_2 b) + bd$. □

Kongruencia tulajdonságai (múlt heti anyag!)

Példa

Mi lesz $345 \bmod 7 =?$

$345 = 34 \cdot 10 + 5 \equiv 6 \cdot 3 + 5 = 18 + 5 \equiv 4 + 5 = 9 \equiv 2 \mod 7$.

Emlékeztető: $a \equiv b \mod m$, $c \equiv d \mod m \Rightarrow ac \equiv bd \mod m$

Következmény: $a \equiv b \mod m \Rightarrow ac \equiv bc \mod m$.

Példa

$14 \equiv 6 \mod 8 \Rightarrow 42 \equiv 18 \mod 24$

A másik irány nem igaz!

$2 \cdot 7 \equiv 2 \cdot 3 \mod 8 \not\Rightarrow 7 \equiv 3 \mod 8$.

Kongruencia tulajdonságai (múlt heti anyag!)

Tétel

Legyenek a, b, c, m egész számok. Ekkor
$ac \equiv bc \mod m \Leftrightarrow a \equiv b \mod \frac{m}{(c,m)}$

Következmény: $ac \equiv bc \mod m, (c,m) = 1 \Leftrightarrow a \equiv b \mod m$.

Példa

$2 \cdot 7 \equiv 2 \cdot 3 \mod 8 \Rightarrow 7 \equiv 3 \mod \frac{8}{2}$.

Bizonyítás

Legyen $d = (c,m)$. Ekkor
$m \mid c(a-b) \Leftrightarrow \frac{m}{d} \mid \frac{c}{d}(a-b)$. Mivel $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$,
ezért $\frac{m}{d} \mid (a-b) \Leftrightarrow a \equiv b \mod \frac{m}{d}$. □

Lineáris kongruenciák (itt kezdődik az új anyag)

Oldjuk meg a $2x \equiv 5 \mod 7$ kongruencát.

Ha x egy megoldás és $x \equiv y \mod 7$, akkor y szintén megoldás.

Keressük megoldást a $\{0, 1, \ldots, 6\}$ halmazból!

$x = 0 \Rightarrow 2x = 0 \not\equiv 5 \mod 7$;
$x = 1 \Rightarrow 2x = 2 \not\equiv 5 \mod 7$;
$x = 2 \Rightarrow 2x = 4 \not\equiv 5 \mod 7$;
$x = 3 \Rightarrow 2x = 6 \not\equiv 5 \mod 7$;
$x = 4 \Rightarrow 2x = 8 \equiv 1 \not\equiv 5 \mod 7$;
$x = 5 \Rightarrow 2x = 10 \equiv 3 \not\equiv 5 \mod 7$;
$x = 6 \Rightarrow 2x = 12 \equiv 5 \mod 7$.

A kongruencia megoldása: $\{6 + 7\ell : \ \ell \in \mathbb{Z}\}$.

Van-e jobb módszer?
Oldjuk meg a $23x \equiv 4 \mod 211$ kongruencát! Kell-e 211 próbálkozás?

Lineáris kongruenciák

Tétel

Legyenek a, b, m egész számok, $m > 1$. Ekkor az $ax \equiv b \mod m$ megoldható $\Leftrightarrow (a, m) \mid b$. Ez esetben pontosan (a, m) darab inkongruens megoldás van $\mod m$.

Bizonyítás

$ax \equiv b \mod m \Leftrightarrow ax + my = b$ valamely y egészre.
Mivel $(a, m) \mid a, m \Leftrightarrow (a, m) \mid ax + my = b$.
Ha $d = (a, m) \mid b$ legyen $a' = a/d$, $b' = b/d$, $m' = m/d$: $a'x + m'y = b'$
Mivel $(a', m') = 1$ bővített euklideszi algoritmussal kiszámolható x_0, y_0 együttható, hogy $a'x_0 + m'y_0 = 1 \Rightarrow a'(b'x_0) + m'(b'y_0) = b'$, azaz $x_1 = b'x_0$, $y_1 = b'y_0$ megoldás lesz.
Megoldások száma: legyenek x, ill. y megoldások. Az $a'x + m'y = b'$ és $a'x_1 + m'y_1 = b'$ egyenleteket kivonva egymásból kapjuk:
$a'(x - x_1) = m'(y_1 - y) \Rightarrow m' \mid x - x_1 \Rightarrow x = x_1 + m'k$:
$k = 0, 1, \ldots d - 1$. Ezek megoldások $y = y_1 - ka'$ választással. □

Lineáris kongruenciák

1. $ax \equiv b \mod m \Leftrightarrow ax + my = b$.
2. Oldjuk meg $ax + my = (a, m)$ egyenletet (Bővített euklideszi algoritmus).
2. Ha $(a, m) \mid b \Leftrightarrow$ van megoldás.
4. Megoldások: $x_i = \frac{b}{(a,m)}x + k\frac{m}{(a,m)}$: $k = 0, 1, \ldots, (a, m) - 1$.

Példa Oldjuk meg a $23x \equiv 4 \mod 211$ kongruencát!

i	r_n	q_n	x_i
-1	23	–	1
0	211	–	0
1	23	0	1
2	4	9	-9
3	3	5	46
4	1	1	-55
5	0	3	–

Algoritmus: $r_{i-2} = r_{i-1}q_i + r_i$,
$x_{-1} = 1$, $x_0 = 0$,
$x_i = x_{i-2} - q_i x_{i-1}$

Lnko: $(23, 211) = 1 \mid 4 \Rightarrow$
Egy megoldás: $x = 4(-55) \equiv 202 \mod 211$.

Összes megoldás: $\{202 + 211\ell : \ \ell \in \mathbb{Z}\}$.

Ezek megoldások: $23 \cdot (202 + 211\ell) - 4 = 4642 + 211\ell = (22 + \ell) \cdot 211$

Lineáris kongruenciák

Példa

Oldjuk meg a $10x \equiv 8 \mod 22$ kongruencát!

i	r_n	q_n	x_i
-1	10	–	1
0	22	–	0
1	10	0	1
2	2	2	-2
3	0	5	–

Algoritmus: $r_{i-2} = r_{i-1}q_i + r_i$,
$x_{-1} = 1$, $x_0 = 0$,
$x_i = x_{i-2} - q_i x_{i-1}$

Lnko: $(10, 22) = 2 \mid 8 \Rightarrow$
Egy megoldás pár:
$x_1 = 4(-2) \equiv 14 \mod 22$
$x_2 = 4(-2) + \frac{22}{2} \equiv 14 + 11 \equiv 3 \mod 22$.

Összes megoldás: $\{14 + 22\ell : \ \ell \in \mathbb{Z}\} \bigcup \{3 + 22\ell : \ \ell \in \mathbb{Z}\}$.

Ezek megoldások: $x_1 = 14$: $10 \cdot 14 - 8 = 132 = 6 \cdot 22$
$x_2 = 3$: $10 \cdot 3 - 8 = 22 = 1 \cdot 22$.

Lineáris diofantikus egyenletek

Diofatikus egyenletek: egyenletek egész megoldásait keressük.

Lineáris diofantikus egyenletek: $ax + by = c$, ahol a, b, c egészek.

Ez ekvivalens az $ax \equiv c \mod b$, $by \equiv c \mod a$ kongruenciákkal.

Az $ax + by = c$ pontosan akkor oldható meg, ha $(a, b) \mid c$, és ekkor a megoldások megkaphatók a bővített euklideszi algoritmussal.

További diofantikus egyenletek:
$x^2 + y^2 = -4$: nincs valós megoldás.

$x^2 - 4y^2 = 3$: nincs megoldás, u.i. 4-gyel való osztási maradékok:
$x^2 \equiv 3 \mod 4$. De ez nem lehet, a négyzetszám maradéka 0 vagy 1:

x	$x^2 \bmod 4$
$4k$	0
$4k+1$	1
$4k+2$	0
$4k+3$	1

Szimultán kongruenciák

Szeretnénk olyan x egészet, mely egyszerre elégíti ki a következő kongruenciákat:

$$\left.\begin{array}{l} 2x \equiv 1 \mod 3 \\ 4x \equiv 3 \mod 5 \end{array}\right\}$$

A kongruenciákat külön megoldva:

$$\left.\begin{array}{l} x \equiv 2 \mod 3 \\ x \equiv 2 \mod 5 \end{array}\right\}$$

Látszik, hogy $x = 2$ megoldás lesz!

Vannak-e más megoldások?

- $2, 17, 32, \ldots, 2 + 15\ell$;
- további megoldások?
- hogyan oldjuk meg az általános esetben:

$$\left.\begin{array}{l} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \end{array}\right\}$$

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruencia rendszert:

$$\left.\begin{array}{l} a_1 x \equiv b_1 \mod m_1 \\ a_2 x \equiv b_2 \mod m_2 \\ \quad \vdots \\ a_n x \equiv b_n \mod m_n \end{array}\right\}$$

Az egyes lineáris kongruenciák $a_i x \equiv b_i \mod m_i$ külön megoldhatóak:

$$\left.\begin{array}{l} x \equiv c_1 \mod m_1 \\ x \equiv c_2 \mod m_2 \\ \quad \vdots \\ x \equiv c_n \mod m_n \end{array}\right\}$$

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruencia rendszert:

$$\left.\begin{array}{l} x \equiv c_1 \mod m_1 \\ x \equiv c_2 \mod m_2 \\ \quad \vdots \\ x \equiv c_n \mod m_n \end{array}\right\}$$

Felthető, hogy az $m_1, m_2 \ldots, m_n$ modulusok relatív prímek.
Ha pl. $m_1 = m_1' d$, $m_2 = m_2' d$, akkor az első két sor helyettesíthető (Biz.: később)

$$\begin{array}{l} x \equiv c_1 \mod m_1' \\ x \equiv c_1 \mod d \\ x \equiv c_2 \mod m_2' \\ x \equiv c_2 \mod d \end{array}$$

Ha itt $c_1 \not\equiv c_2 \mod d$, akkor nincs megoldás, különben az egyik sor törölhető.

Kínai maradék tétel

Tétel

Legyenek $1 < m_1, m_2 \ldots, m_n$ relatív prím számok, $c_1, c_2, \ldots, c_n$ egészek. Ekkor a

$$\left.\begin{array}{l} x \equiv c_1 \mod m_1 \\ x \equiv c_2 \mod m_2 \\ \quad \vdots \\ x \equiv c_n \mod m_n \end{array}\right\}$$

kongruencia rendszer megoldható, és bármely két megoldás kongruens egymással modulo $m_1 \cdot m_2 \cdots m_n$.

Kínai maradék tétel

$x \equiv c_1 \mod m_1$, $x \equiv c_2 \mod m_2$, $\ldots$, $x \equiv c_n \mod m_n$. $x = ?$

Bizonyítás

A bizonyítás konstruktív!
Legyen $m = m_1 m_2$. A bővített euklideszi algoritmussal oldjuk meg az $m_1 x_1 + m_2 x_2 = 1$ egyenletet. Legyen $c_{1,2} = m_1 x_1 c_2 + m_2 x_2 c_1$. Ekkor $c_{1,2} \equiv c_j \mod m_j$ $(j = 1, 2)$. Ha $x \equiv c_{1,2} \mod m$, akkor x megoldása az első két kongruenciának. Megfordítva: ha x megoldása az első két kongruenciának, akkor $x - c_{1,2}$ osztható m_1-gyel, m_2-vel, így a szorzatukkal is: $x \equiv c_{1,2} \mod m$. Az eredeti kongruencia rendszer ekvivalens a

$$\left.\begin{array}{l} x \equiv c_{1,2} \mod m_1 m_2 \\ x \equiv c_3 \mod m_3 \\ \quad \vdots \\ x \equiv c_n \mod m_n \end{array}\right\}$$

n szerinti indukcióval adódik az állítás. □

Szimultán kongruenciák

Példa

$$\left.\begin{array}{l} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \end{array}\right\}$$

Oldjuk meg az $3x_1 + 5x_2 = 1$ egyenletet.
Megoldások: $x_1 = -3$, $x_2 = 2$. $\Rightarrow$
$c_{1,2} = 3 \cdot (-3) \cdot 3 + 5 \cdot 2 \cdot 2 = -27 + 20 = -7$.
Összes megoldás: $\{-7 + 15\ell : \ \ell \in \mathbb{Z}\} = \{8 + 15\ell : \ \ell \in \mathbb{Z}\}$.

Példa

$$\left.\begin{array}{l} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 4 \mod 7 \end{array}\right\} \quad \stackrel{c_{1,2}=8}{\Longrightarrow} \quad \left.\begin{array}{l} x \equiv 8 \mod 15 \\ x \equiv 4 \mod 7 \end{array}\right\}$$

Oldjuk meg a $15x_{1,2} + 7x_3 = 1$ egyenletet.
Megoldások: $x_{1,2} = 1$, $x_3 = -2$. $\Rightarrow$
$c_{1,2,3} = 15 \cdot 1 \cdot 4 + 7 \cdot (-2) \cdot 8 = 60 - 112 = -52$.
Összes megoldás: $\{-52 + 105\ell : \ \ell \in \mathbb{Z}\} = \{53 + 105\ell : \ \ell \in \mathbb{Z}\}$.

Maradékosztályok

Sokszor egy adott probléma megoldása nem egy konkrét szám (számok családja), hanem egy egész halmaz (halmazok családja):

- $2x \equiv 5 \mod 7$, megoldások: $\{6 + 7\ell : \ \ell \in \mathbb{Z}\}$
- $10x \equiv 8 \mod 22$, megoldások: $\{14 + 22\ell : \ \ell \in \mathbb{Z}\}$, $\{3 + 22\ell : \ \ell \in \mathbb{Z}\}$.

Definíció

Egy rögzített m modulus és a egész esetén, az a-val kongruens elemek halmazát az a által reprezentált maradékosztálynak nevezzük:
$\overline{a} = \{x \in \mathbb{Z} : x \equiv a \mod m\} = \{a + \ell m : \ \ell \in \mathbb{Z}\}$.

Példa

Az $2x \equiv 5 \mod 7$ megoldása : $\overline{6}$
A $10x \equiv 8 \mod 22$, megoldásai: $\overline{14}$, $\overline{3}$.
$m = 7$ modulussal $\overline{2} = \overline{23} = \{\ldots, -5, 2, 9, 16, 23, 30, \ldots\}$

Általában: $\overline{a} = \overline{b} \Leftrightarrow a \equiv b \mod m$.

Maradékosztályok

Definíció

Egy rögzített m modulus esetén, ha minden maradékosztályból pontosan egy elemet kiveszünk, akkor az így kapott számok teljes maradékrendszert alkotnak modulo m.

Példa

$\{33, -5, 11, -11, -8\}$ teljes maradékrendszer modulo 5.

Gyakori választás teljes maradékrendszerekre

- Legkisebb nemnegatív maradékok: $\{0, 1, \ldots, m-1\}$;
- Legkisebb abszolútértékű maradékok:
  $\left\{0, \pm 1, \ldots, \pm \frac{m-1}{2}\right\}$, ha $2 \nmid m$;
  $\left\{0, \pm 1, \ldots, \pm \frac{m-2}{2}, \frac{m}{2}\right\}$, ha $2 \mid m$.

Maradékosztályok

Megjegyzés: ha egy maradékosztály valamely eleme relatív prím a modulushoz, akkor az összes eleme az: $(a + \ell m, m) = (a, m) = 1$.

Definíció

Egy rögzített m modulus esetén, ha mindazon maradékosztályból, melyek elemei relatív prímek a modulushoz kiveszünk pontosan egy elemet, akkor az így kapott számok redukált maradékrendszert alkotnak modulo m.

Példa

$\{1, 2, 3, 4\}$ redukált maradékrendszer modulo 5.
$\{1, -1\}$ redukált maradékrendszer modulo 3.
$\{1, 19, 29, 7\}$ redukált maradékrendszer modulo 8.
$\{0, 1, 2, 3, 4\}$ nem redukált maradékrendszer modulo 5.

Definíció (kiegészítés)

Egy rögzített m modulus esetén, ha $(a, m) = 1$, akkor az a által reprezentált maradékosztály $\overline{a}$ redukált maradékosztály. A redukált maradékosztályok halmazát $\mathbb{Z}_m^*$-al jelöljuk:
$\mathbb{Z}_m^* = \{\overline{a} : \ 1 \leq 0 < m, \ (a, m) = 1\}$.

Maradékosztályok

A maradékosztályok között természetes módon műveleteket definiálhatunk:

Definíció

Rögzített m modulus, és a, b egészek esetén legyen:

$$\overline{a} + \overline{b} \stackrel{\text{def}}{=} \overline{a+b}; \qquad \overline{a} \cdot \overline{b} \stackrel{\text{def}}{=} \overline{a \cdot b}$$

Állítás

Ez értelme definíció, azaz ,ha $\overline{a} = \overline{a^*}$, $\overline{b} = \overline{b^*}$, akkor $\overline{a} + \overline{b} = \overline{a^*} + \overline{b^*}$, illetve $\overline{a} \cdot \overline{b} = \overline{a^*} \cdot \overline{b^*}$

Bizonyítás

Mivel $\overline{a} = \overline{a^*}$, $\overline{b} = \overline{b^*} \Rightarrow a \equiv a^* \mod m$, $b \equiv b^* \mod m \Rightarrow$
$a + b \equiv a^* + b^* \mod m \Rightarrow \overline{a+b} = \overline{a^* + b^*} \Rightarrow \overline{a} + \overline{b} = \overline{a^*} + \overline{b^*}$.
Szorzás hasonlóan. □

Maradékosztályok

A maradékosztályok között természetes módon műveleteket definiálhatunk: $\overline{a} + \overline{b} = \overline{a+b}$; $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Definíció

Rögzített m modulus, legyen $\mathbb{Z}_m$ a maradékosztályok halmaza. Ekkor a halmaz elemei között definiálhatunk összeadást, illetve szorzást.

Példa

$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Maradékosztályok

Tétel

Legyen $m > 1$ egész. Ha $1 < (a, m) < m$, akkor $\overline{a}$ nullosztó $\mathbb{Z}_m$-ben: $\overline{a}$-hoz van olyan $\overline{b}$, hogy $\overline{a} \cdot \overline{b} = \overline{0}$

Ha $(a, m) = 1$, akkor $\overline{a}$-nak van reciproka (multiplikatív inverze) $\mathbb{Z}_m$-ben: $\overline{a}$-hoz van olyan $\overline{x}$, hogy $\overline{a} \cdot \overline{x} = \overline{1}$.

Speciálisan, ha m prím, minden nem-nulla maradékosztállyal lehet osztani.

Példa

Legyen $m = 9$. $\overline{6} \cdot \overline{3} = \overline{18} = \overline{0}$.
$(2, 9) = 1$, így $\overline{2} \cdot \overline{5} = \overline{10} = \overline{1}$.

Bizonyítás

Legyen $d = (a, m)$. Ekkor $a \cdot \frac{m}{d} = \frac{a}{d} \cdot 0 \equiv 0 \mod m$, ahonnan $b = m/d$ jelöléssel $\overline{a} \cdot \overline{b} = \overline{0}$.
Ha $(a, m) = 1$, akkor a bővített euklideszi algoritmussal megadhatóak x, y egészek, hogy $ax + my = 1$. Ekkor $ax \equiv 1 \mod m$ azaz $\overline{a} \cdot \overline{x} = \overline{1}$. □

Euler-féle φ függvény

Definíció

Egy $m > 0$ egész szám esetén legyen $\varphi(m)$ az m-nél kisebb, hozzá relatív prím egészek száma $\varphi(m) = |\{i : \ 0 < i < m, (m, i) = 1\}|$.

Példa

$\varphi(5) = 4$: 5-höz relatív prím pozitív egészek $1, 2, 3, 4$;
$\varphi(6) = 2$: 6-hoz relatív prím pozitív egészek $1, 5$;
$\varphi(12) = 4$: 12-höz relatív prím pozitív egészek $1, 5, 7, 11$.
$\varphi(15) = 8$: 15-höz relatív prím pozitív egészek $1, 2, 4, 7, 8, 11, 13, 14$.

Megjegyzés: $\varphi(m)$ a redukált maradékosztályok száma modulo m.

Euler-féle φ függvény

$\varphi(m) = |\{i : \ 0 < i < m, (m, i) = 1\}|$

Tétel (NB)

Legyen m prímtényezős felbontása $m = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$. Ekkor
$\varphi(m) = \prod_{i=1}^{\ell} \left(p_i^{e_i} - p_i^{e_i-1}\right) = m \cdot \prod_{i=1}^{\ell} \left(1 - \frac{1}{p_i}\right)$

Ha $a_1, \ldots, a_r$ *páronként* relatív prímek, akkor
$\varphi(a_1 \cdots a_r) = \varphi(a_1) \cdots \varphi(a_r)$.
Ha p prím, akkor $\varphi(p^m) = p^m - p^{m-1}$.

Példa

$\varphi(5) = 5\left(1 - \frac{1}{5}\right) = 4$;
$\varphi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 2$;
$\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$;
$\varphi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8$.

Euler-Fermat tétel

Tétel

Legyen $m > 1$ egész szám, a olyan egész, melyre $(a, m) = 1$. Ekkor

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Következmény (Fermat tétel)

Legyen p prímszám, $p \nmid a$. Ekkor $a^{p-1} \equiv 1 \mod p$,
illetve tetszőleges a esetén $a^p \equiv a \mod p$.

Példa

$\varphi(6) = 2 \Rightarrow 5^2 = 36 \equiv 1 \mod 6$;
$\varphi(12) = 4 \Rightarrow 5^4 = 625 \equiv 1 \mod 12$; $7^4 = 2401 \equiv 1 \mod 12$.

Figyelem! $2^4 = 16 \equiv 2 \not\equiv 1 \mod 12$, mert $(2, 12) = 2 \neq 1$.

Euler-Fermat tétel bizonyítása

Lemma

Legyen $m > 1$ egész, a_1, a_2 $\ldots$, a_m teljes maradékrendszer modulo m. Ekkor minden a, b egészre, melyre $(a, m) = 1$, $a \cdot a_1 + b$, $a \cdot a_2 + b$ $\ldots$, $a \cdot a_m + b$ szintén teljes maradékrendszer. Továbbá, ha a_1, a_2, $\ldots$, $a_{\varphi(m)}$ redukált maradékrendszer modulo m, akkor $a \cdot a_1$, $a \cdot a_2$ $\ldots$, $a \cdot a_{\varphi(m)}$ szintén redukált maradékrendszer.

A fenti lemma bizonyítása

Ha $i \neq j$ esetén $aa_i + b \equiv aa_j + b \mod m \Leftrightarrow aa_i \equiv aa_j \mod m$. Mivel $(a, m) = 1$, egyszerűsíthetünk a-val: $a_i \equiv a_j \mod m$. Tehát $a \cdot a_1 + b$, $a \cdot a_2 + b$ $\ldots$, $a \cdot a_m + b$ páronként inkongruensek. Mivel számuk m, így teljes maradékrendszert alkotnak.

Ha $(a_i, m) = 1$, $(a, m) = 1 \Rightarrow (a \cdot a_i, m) = 1$. Továbbá $a \cdot a_1$, $a \cdot a_2$ $\ldots$, $a \cdot a_{\varphi(m)}$ páronként inkongruensek, számuk $\varphi(m) \Leftrightarrow$ redukált maradékrendszert alkotnak. $\square$

Euler-Fermat tétel bizonyítása

Tétel (Euler-Fermat) $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \mod m$.

A tétel bizonyítása

Legyen $a_1, a_2, \ldots, a_{\varphi(m)}$ egy redukált maradékrendszer modulo m. Mivel $(a, m) = 1 \Rightarrow a \cdot a_1, a \cdot a_2 \ldots, a \cdot a_{\varphi(m)}$ szintén redukált maradékrendszer.

Innen

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} a_j = \prod_{j=1}^{\varphi(m)} a \cdot a_j \equiv \prod_{j=1}^{\varphi(m)} a_j \mod m$$

Mivel $\prod_{j=1}^{\varphi(m)} a_j$ relatív prím m-hez, így egyszerűsíthetünk vele:

$$a^{\varphi(m)} \equiv 1 \mod m$$

□

Euler-Fermat tétel használata

Tétel (Euler-Fermat) $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \mod m$

Példa

Mi lesz a 3^{111} utólos számjegye tizes számrendszerben?
Mi lesz $3^{111} \mod 10$?
$\varphi(10) = 4 \Rightarrow$
$3^{111} = 3^{4 \cdot 27+3} = \left(3^4\right)^{27} \cdot 3^3 \equiv 1^{27} \cdot 3^3 = 3^3 = 27 \equiv 7 \mod 10$

Oldjuk meg a $2x \equiv 5 \mod 7$ kongruencát!
$\varphi(7) = 6$. Szorozzuk be mindkét oldalt 2^5-el. Ekkor
$5 \cdot 2^5 \equiv 2^6 x \equiv x \mod 7$. És itt $5 \cdot 2^5 = 5 \cdot 32 \equiv 5 \cdot 4 = 20 \equiv 6 \mod 7$.

Oldjuk meg a $23x \equiv 4 \mod 211$ kongruencát!
$\varphi(211) = 210$. Szorozzuk be mindkét oldalt 2^{209}-el. Ekkor
$4 \cdot 23^{209} \equiv 23^{210} x \equiv x \mod 211$. És itt $4 \cdot 23^{209} \equiv \ldots \mod 211$.