Diszkrét matematika 1. középszint

10. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼ nagy
Mérai László diái alapján

Komputeralgebra Tanszék

2017. ősz

Számelmélet alaptétele

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 (felbonthatatlanok). Tfh. $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$, ahol $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_\ell$ prímek, és n a legkisebb olyan szám, aminek két lényegesen különböző előállítása van. p_1 osztja a bal oldalt, ezért osztja a jobb oldalt, így a prímtulajdonság miatt osztja annak valamelyik tényezőjét; feltehető $p_1 | q_1$. Mivel q_1 felbonthatatlan (hiszen prím), ezért $p_1 = q_1$. Egyszerűsítve: $n' = p_2 \cdots p_k = q_2 \cdots q_\ell$. Indukció alapján ez már egyértelmű. □

Számelmélet alaptétele

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 különböző pozitív prímek, α_1, α_2,..., α_ℓ pozitív egészek.

Következmény

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

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

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

$(n, m) \cdot [n, m] = n \cdot m$.

Osztók száma

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 $\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_\ell + 1)$.

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

$\tau(2 \cdot 3) = (1 + 1) \cdot (1 + 1) = 4$; $\tau(2^5 \cdot 3) = (5 + 1) \cdot (1 + 1) = 12$.

Prímekről

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 (Miért?), így 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 ($k \in \mathbb{Z}$) prím van.

Prímekről

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, 33
100	25	21, 71
1000	168	144, 76
10000	1229	1085, 73

Eratoszthenész 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 húzzuk ki. A következő (ki nem húzott) szám a 3, ez szintén prím. A 3 (valódi) többszörösei nem prímek, ezeket húzzuk ki...

Ismételjük az eljárást $\sqrt{n}$-ig. A ki nem húzott számok mind prímek.

Kongruenciák

Oszthatósági kérdésekben sokszor csak a maradékos osztás esetén kapott 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, ekkor $a \equiv b \pmod{m}$ (a és b kongruensek modulo m), ha $m \mid a - b$, és $a \not\equiv b \pmod{m}$ (a és b inkongruensek), ha $m \nmid a - b$.

Ekvivalens megfogalmazás: $a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$, azaz m-mel osztva ugyanazt az osztási maradékot adják.

Példa

$16 \equiv 4 \pmod{3}$ ui. $3 \mid 16 - 4 \Leftrightarrow 16 \bmod 3 = 1 = 4 \bmod 3$;
$16 \equiv 4 \pmod{2}$ ui. $2 \mid 16 - 4 \Leftrightarrow 16 \bmod 2 = 0 = 4 \bmod 2$;
$16 \not\equiv 4 \pmod{5}$ ui. $5 \nmid 16 - 4 \Leftrightarrow 16 \bmod 5 = 1 \neq 4 = 4 \bmod 5$.

Kongruencia tulajdonságai

Tétel

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

1. $a \equiv a \pmod{m}$;
2. $a \equiv b \pmod{m}$, $m' \mid m \Rightarrow a \equiv b \pmod{m'}$;
3. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$;
4. $a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$;
5. $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$;
6. $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.

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. $a = q_1 m + b$, $c = q_2 m + d \Rightarrow$
   $\Rightarrow ac = (q_1 m + b)(q_2 m + d) = m(q_1 q_2 m + q_1 d + q_2 b) + bd$. □

Kongruencia tulajdonságai

Példa

Mi lesz $345 \bmod 7 = ?$

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

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

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

Példa

$14 \equiv 6 \pmod 8 \Rightarrow 42 \equiv 18 \pmod 8$

A másik irány nem igaz!

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

Kongruencia tulajdonságai

Tétel

Legyenek a, b, c, m egész számok. Ekkor

$ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{(c,m)}}$

Következmény: $(c, m) = 1$ esetén $ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$.

Példa

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

Bizonyítás

Legyen $d = (c, m)$. Ekkor

$ac \equiv bc \pmod{m} \Leftrightarrow m \mid c(a-b) \Leftrightarrow \frac{m}{d} \mid \frac{c}{d}(a-b)$. Mivel $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$,

ezért $\frac{m}{d} \mid \frac{c}{d}(a-b) \Leftrightarrow \frac{m}{d} \mid (a-b) \Leftrightarrow a \equiv b \pmod{\frac{m}{d}}$. □

Lineáris kongruenciák

Oldjuk meg a $2x \equiv 5 \pmod 7$ kongruenciát!

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

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

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

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

Van-e jobb módszer?
Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruenciát! Kell-e 211 próbálkozás?

Lineáris kongruenciák

Tétel

Legyenek a, b, m egész számok, $m > 1$. Ekkor az $ax \equiv b \pmod{m}$ kongruencia pontosan akkor oldható meg, ha $(a, m) \mid b$. Ez esetben pontosan (a, m) darab páronként inkongruens megoldás van $\bmod m$.

Bizonyítás

$ax \equiv b \pmod{m} \Leftrightarrow m | ax - b \Leftrightarrow ax + my = b$ valamely y egészre.
Ez egy kétváltozós, lineáris, diofantikus egyenlet, ami pontosan akkor oldató meg, ha $(a, m) \mid b$. Ha ennek x_0 megoldása, akkor az összes megoldás felírható $x_t = x_0 + \frac{m}{(a,m)} \cdot t$ alakban, ahol $t \in \mathbb{Z}$ tetszőleges.
Ebből $x_t - x_0 = \frac{m}{(a,m)} \cdot t$, így $\frac{m}{(a,m)} | x_t - x_0$, vagyis x pontosan akkor megoldás, ha $x \equiv x_0 \left(\bmod \frac{m}{(a,m)}\right)$.
Tekintsük a következő (a, m) db megoldást:
$x_k = x_0 + k\frac{m}{(a,m)}$: $k = 0, 1, \ldots, (a, m) - 1$.
Ezek páronként inkongruensek $\bmod m$ (Miért?), és bármely x megoldás esetén van köztük x-szel kongruens $\bmod m$ (Miért?).

Lineáris kongruenciák

1. $ax \equiv b \pmod{m} \Leftrightarrow ax + my = b$.
2. Pontosan akkor van megoldás, ha $(a, m) \mid b$.
3. Oldjuk meg az $ax' + my' = (a, m)$ egyenletet (bővített euklideszi algoritmus)!
4. Megoldások: $x_k = \frac{b}{(a,m)}x' + k\frac{m}{(a,m)}$: $k = 0, 1, \ldots, (a, m) - 1$.

Példa Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruencát!

i	r_i	q_i	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: $x_0 = 4(-55) \equiv 202 \pmod{211}$.

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 $10x \equiv 8 \pmod{22}$ kongruenciát!

i	r_i	q_i	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: $(10, 22) = 2 \mid 8 \Rightarrow$
Két inkongruens megoldás:
$x_0 = 4(-2) \equiv 14 \pmod{22}$
$x_1 = 4(-2) + 1 \cdot \frac{22}{2} \equiv 14 + 11 \equiv 3 \pmod{22}$.

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

Ezek megoldások: $x_0 = 14$: $10 \cdot 14 - 8 = 132 = 6 \cdot 22$,
$x_1 = 3$: $10 \cdot 3 - 8 = 22 = 1 \cdot 22$.

Diofantikus egyenletek

Diofantikus egyenletek: egyenletek egész megoldásait keressük.

Kétváltozós lineáris diofantikus egyenletek: $ax + by = c$, ahol a, b, c egészek adottak.

Ez ekvivalens az $ax \equiv c \pmod{b}$, $by \equiv c \pmod{a}$ 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, ui. 4-gyel való osztási maradékok:
$x^2 \equiv 3 \pmod{4}$. 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:

$$\left.\begin{aligned} 2x &\equiv 1 \pmod 3 \\ 4x &\equiv 3 \pmod 5 \end{aligned}\right\}$$

A kongruenciákat külön megoldva:

$$\left.\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 2 \pmod 5 \end{aligned}\right\}$$

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:

$$\left.\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}\right\}$$

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruenciarendszert:

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_n x &\equiv b_n \pmod{m_n} \end{aligned}\right\}$$

Az egyes $a_i x \equiv b_i \pmod{m_i}$ lineáris kongruenciák külön megoldhatóak:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_n \pmod{m_n} \end{aligned}\right\}$$

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruenciarendszert:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_n \pmod{m_n} \end{aligned}\right\}$$

Feltehető, 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:

$$\begin{aligned} x &\equiv c_1 \pmod{m_1'} \\ x &\equiv c_1 \pmod{d} \\ x &\equiv c_2 \pmod{m_2'} \\ x &\equiv c_2 \pmod{d} \end{aligned}$$

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

Kínai maradéktétel

Tétel

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

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_n \pmod{m_n} \end{aligned}\right\}$$

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

Kínai maradéktétel

$x \equiv c_1 \pmod{m_1}$, $x \equiv c_2 \pmod{m_2}$, $\ldots$, $x \equiv c_n \pmod{m_n}$. $x = ?$

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 $c_{1,2} \equiv c_j \pmod{m_j}$ $(j = 1, 2)$. Ha $x \equiv c_{1,2} \pmod{m}$, 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: $x \equiv c_{1,2} \pmod{m}$. Az eredeti kongruenciarendszer ekvivalens az

$$\left.\begin{aligned} x &\equiv c_{1,2} \pmod{m_1 m_2} \\ x &\equiv c_3 \pmod{m_3} \\ &\vdots \\ x &\equiv c_n \pmod{m_n} \end{aligned}\right\}$$

kongruenciarendszerrel. n szerinti indukcióval adódik az állítás. □

Szimultán kongruenciák

Példa

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

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

Példa

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

Oldjuk meg a $15x_{1,2} + 7x_3 = 1$ egyenletet!
Megoldások: $x_{1,2} = 1$, $x_3 = -2$. $\Rightarrow$
$\Rightarrow c_{1,2,3} = 15 \cdot 1 \cdot 4 + 7 \cdot (-2) \cdot 8 = 60 - 112 = -52$.
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):

- $2x \equiv 5 \pmod 7$, megoldások: $\{6 + 7\ell : \ \ell \in \mathbb{Z}\}$
- $10x \equiv 8 \pmod{22}$, 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:
$\overline{a} = \{x \in \mathbb{Z} : x \equiv a \pmod m\} = \{a + \ell m : \ \ell \in \mathbb{Z}\}$.