

Bevezetés a Számításelméletbe II. 9. előadás

Sali Attila

Budapest Műszaki és Gazdaságtudományi Egyetem

Számítástudományi Tsz.

I. B. 137/b

`sali@cs.bme.hu`

2002 április 9.

Maradékosztályok

1. Definíció. Legyen $a, b \in \mathbb{Z}$. Ekkor a **kongruens** b -vel az m modulusra vonatkozólag (jelölve $a \equiv b \pmod{m}$), ha $m \mid a - b$.

1. \equiv **reflexív**: $a \equiv a \pmod{m}$

2. \equiv **szimmetrikus**: $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$

3. \equiv **transzitiv**: $a \equiv b \pmod{m}$ és $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$

Ezzel ekvivalencia osztályokba soroljuk az egész számok halmazát.

Egy–egy ilyen osztályt hívunk **maradékosztálynak**.

Példa: $A \pmod{2}$ maradékosztályok a páros, illetve páratlan számok.

$A \pmod{17}$ maradékosztályok: $\{\dots, -34, -17, 0, 17, 34, \dots\}$,
 $\{\dots, -33, -16, 1, 18, 35, \dots\}$, $\{\dots, -32, -15, 2, 19, 36, \dots\}, \dots$,
 $\{\dots, -18, -1, 16, 33, 50, \dots\}$.

Műveletek maradékosztályokkal

Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor

$$a + c \equiv b + d, \quad a - c \equiv b - d, \quad ac \equiv bd \pmod{m}.$$

Az utóbbihoz

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$$

azonos átalakítást alkalmazzuk. Ha $a - b$ és $c - d$ is osztható m -mel, akkor $ac - bd$ is.

2. Definíció. Két \pmod{m} maradékosztály összege (különbsége, szorzata) egy-egy reprezentánsuk összegének (különbségének, szorzatának) maradékosztálya.

Példa

$$\mathbb{Z}$$

\vdots	\vdots	\vdots	\vdots
-8	-7	-6	-5
-4	-3	-2	-1
0	1	2	3
4	5	6	7
8	9	10	11
\vdots	\vdots	\vdots	\vdots
0	1	2	3

Osztás

Lehet-e?

$$20 \equiv 80 \pmod{15} \text{ és } \frac{20}{4} = 5 \equiv 20 = \frac{80}{4} \pmod{15}.$$

$$\text{Viszont } \frac{20}{5} = 4 \not\equiv 16 = \frac{80}{5} \pmod{15}$$

Legyen $ac \equiv bc \pmod{m}$ és $d(c, m) = 1$. $ac - bc = c(a - b)$ osztható m -mel, $\implies m \mid a - b$, azaz $a \equiv b \pmod{m}$. Ha viszont c és m nem relatív prímek, akkor a c -vel való osztáskor megváltozik a modulus:

3. Tétel. *Legyen $ac \equiv bc \pmod{m}$ és $d(c, m) = t$. Ekkor $a \equiv b \pmod{\frac{m}{t}}$ teljesül.*

BIZONYÍTÁS Legyen $c = tc'$ és $m = tm'$. Ekkor a c' és m' már relatív prímek. $ac - bc = c(a - b) = tc'(a - b)$ osztható $m = tm'$ -vel, $\implies c'(a - b)$ osztható m' -vel. Mivel $d(c', m') = 1$, így $a - b$ osztható $m' = \frac{m}{t}$ -vel.

Teljes maradékrendszer

Ha a $\text{mod } m$ maradékosztályok mindegyikéből kiválasztunk egy tetszőleges elemet, a keletkező számhalmazt **$\text{mod } m$ teljes maradékrendszernek** nevezzük.

4. Állítás. Az $\{b_1, b_2, \dots, b_n\}$ számhalmaz akkor és csak akkor alkot $\text{mod } m$ teljes maradékrendszert, ha

$$(1) \quad n = m$$

$$(2) \quad \text{bármely } i \neq j \text{ indexpárra } b_i \not\equiv b_j \pmod{m}$$

5. Tétel. Legyen $d(a, m) = 1$. Ha egy $\text{mod } m$ teljes maradékrendszer minden elemét a -val megszorozzuk, ismét egy $\text{mod } m$ teljes maradékrendszert kapunk.

Redukált maradérendszer

Ha két szám ugyanabba a $\text{mod } m$ maradékosztályba tartozik, akkor vagy mindkettő relatív prím m -hez, vagy egyik sem :

$$a \equiv b \pmod{m} \implies m \mid a - b \iff a - b = t \cdot m \implies a = t \cdot m + b \implies (a, m) = (b, m).$$

6. Definíció. A $\text{mod } m$ maradékosztályok közül azokból, melyek minden eleme relatív prím m -hez kiveszünk egyet–egyet, a keletkező számhalmazt **mod m redukált maradérendszernek** nevezzük.

Redukált maradérendszer elemeinek száma annyi, ahány szám a $\{0, 1, 2, \dots, m - 1\}$ halmazból relatív prím m -hez. Ezt a számot **$\varphi(m)$** -mel jelöljük.

7. Állítás. Egy $\{c_1, c_2, \dots, c_k\}$ számhalmaz akkor és csak akkor alkot mod m redukált maradékrendszert, ha

(1) $k = \varphi(m)$

(2) bármely $i \neq j$ indexpárra $c_i \not\equiv c_j \pmod{m}$

(3) bármely i indexre $d(c_i, m) = 1$

8. Tétel. Legyen $d(a, m) = 1$. Ha egy mod m redukált maradékrendszer minden elemét a -val megszorozzuk, ismét egy mod m redukált maradékrendszert kapunk.

BIZONYÍTÁS A maradékrendszer elemeinek számát az a -val való szorzás nem befolyásolja. Ha $x \not\equiv y \pmod{m}$ és $d(a, m) = 1$, akkor $ax \not\equiv ay \pmod{m}$. Ugyanis azt már láttuk, hogy ha $ax \equiv ay \pmod{m}$, akkor $x \equiv y \pmod{m}$.¹ Végül redukált maradékrendszer esetén(3) is teljesül: az m -hez relatív prím a és c_i számok szorzata is relatív prím m -hez.

¹Itt végeztünk a teljes maradékrendszerre vonatkozó állítás bizonyításával.

Euler-Fermat tétel

9. Tétel (Euler-Fermat tétel). *Ha $m > 1$ tetszőleges egész szám és a tetszőleges olyan szám, melyre $d(a, m) = 1$, akkor*

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

10. Tétel („kis” Fermat tétel). *Tetszőleges p prímszámmra és tetszőleges a egész számmra $a^p \equiv a \pmod{p}$.*

BIZONYÍTÁS $\varphi(p) = p - 1$. $a^p - a = a(a^{\varphi(p)} - 1)$. Mivel p prím, vagy $p \mid a$, vagy $(a, p) = 1$

Euler-Fermat bizonyítása

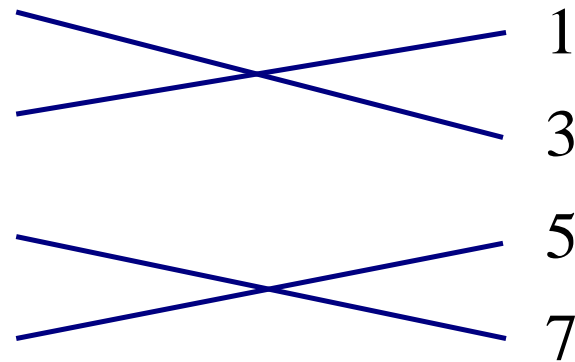
Legyen $\{c_1, c_2, \dots, c_{\varphi(m)}\}$ egy mod m redukált maradékrendszer. Az $\{ac_1, ac_2, \dots, ac_{\varphi(m)}\}$ számhalmaz is egy mod m redukált maradékrendszer lesz, tehát az $ac_1, ac_2, \dots, ac_{\varphi(m)}$ szorzatok valamilyen sorrendben kongruensek a $c_1, c_2, \dots, c_{\varphi(m)}$ számokkal. Például $m = 8$ és $a = 3$:

$$3 \cdot 1 = 3$$

$$3 \cdot 3 = 9 \equiv 1$$

$$3 \cdot 5 = 15 \equiv 7$$

$$3 \cdot 7 = 21 \equiv 5$$



Így

$$(ac_1)(ac_2) \dots (ac_{\varphi(m)}) \equiv (c_1)(c_2) \dots (c_{\varphi(m)}) \pmod{m}$$

teljesül, vagyis

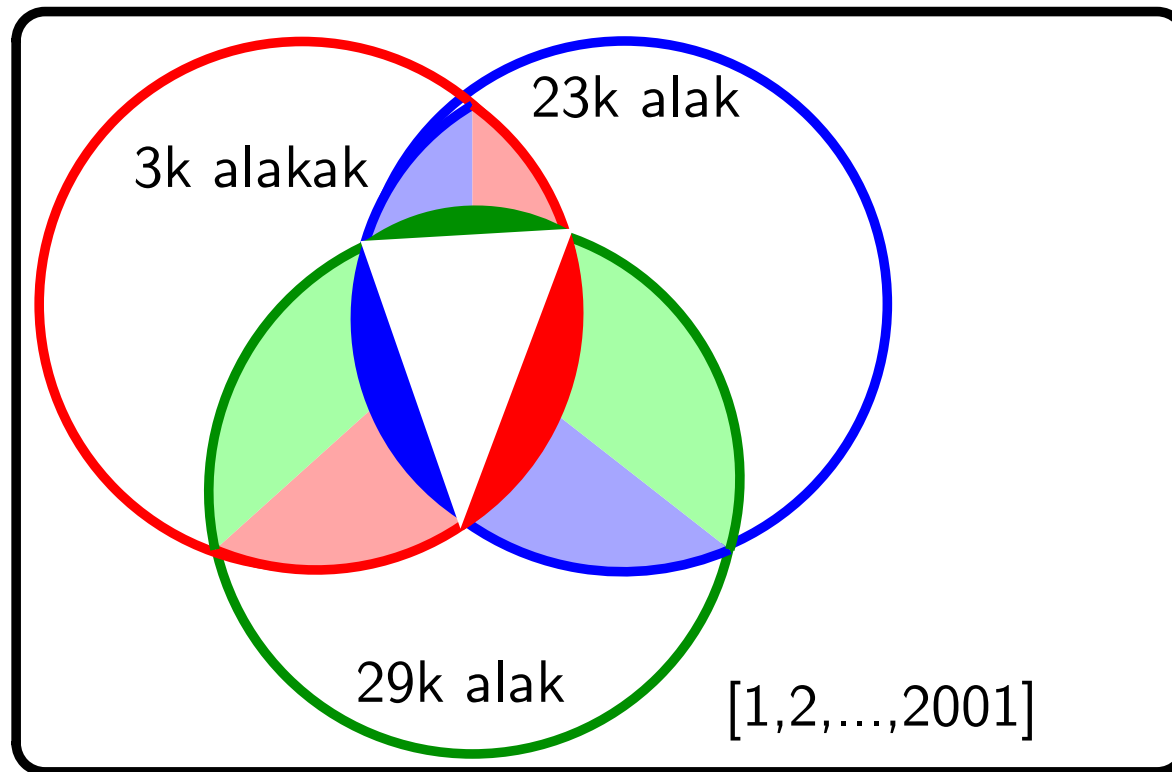
$$\left(a^{\varphi(m)} - 1\right) \prod_{i=1}^{\varphi(m)} (c_i) \equiv 0 \pmod{m}.^2$$

Mivel a c_i számok m -hez relatív prímek voltak, szükségképp $a^{\varphi(m)} - 1$ osztható m -mel.

²Sajtóhiba a könyvben!

$\varphi(2001)$ kiszámítása

$n = 2001 = 3 \cdot 23 \cdot 29 \implies (a, n) = 1 \iff 3, 23, 29$ egyikével sem osztható.



Szita formula

11. Tétel (Szita formula). Legyenek $A_1, A_2, \dots, A_n \subseteq S$, ahol S egy véges halmaz és legyenek $A_I = \bigcap_{i \in I} A_i$ $I \subseteq \{1, 2, \dots, n\}$ -re ($A_\emptyset = S$). Ekkor

$$|S - (A_1 \cup A_2 \cup \dots \cup A_n)| = \sum_{I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|} |A_I|.$$

BIZONYÍTÁS Ha $x \in S - (A_1 \cup A_2 \cup \dots \cup A_n)$, akkor egyszer számoltuk.

Ha x pontosan k darab A_i eleme, akkor $\binom{k}{0} - \binom{k}{1} + \binom{k}{2} - \dots + (-1)^k \binom{k}{k} = (1 - 1)^k = 0$ -szor számoltuk.

$\varphi(n)$ kiszámítása

Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. $(a, n) = 1 \iff p_1, p_2, \dots, p_k$ egyikével sem osztható. Alkalmazzuk a szita formulát: $S = \{1, 2, \dots, n\}$, $A_i = p_i$ -vel osztható számok n -ig. $\implies \varphi(n) = |S - (A_1 \cup A_2 \cup \dots \cup A_k)|$.

Ha $I = \{i_1, i_2, \dots, i_r\}$, akkor $|A_I| = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_r}}$. Behelyettesítve a formulába:

$$\begin{aligned} \varphi(n) = n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \dots + \frac{n}{p_k} \right) + \left(\frac{n}{p_1 p_2} + \dots + \frac{n}{p_{k-1} p_k} \right) + \\ \dots + (-1)^k \frac{n}{p_1 \cdots p_k} = n \prod_{i=1}^k \left(1 - \frac{1}{p_i} \right) \end{aligned}$$

Másképp: $\varphi(n) = \prod \left(p_i^{\alpha_i} - p_i^{\alpha_i-1} \right)$.

$\varphi(n)$ tulajdonságai

1. Ha m prím, akkor $\varphi(m) = m - 1$.
2. Ha m egy p^α alakú prímhatalvány, akkor $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, hisz az $1, 2, \dots, p^\alpha$ számok közül épp a p -vel osztható $p^{\alpha-1}$ darab szám **nem** relatív prím p^α -hoz.
3. Ha a és b relatív prímelek, akkor $\varphi(ab) = \varphi(a) \cdot \varphi(b)$ is teljesül, a $\varphi(n)$ -re kapott formula alapján.

1.-3. a $\varphi(n)$ formulája nélkül is bizonyítható (3. bizonyítása nem egyszerű). Ezzel a $\varphi(n) = \prod (p_i^{\alpha_i} - p_i^{\alpha_i-1})$ egy újabb bizonyítását kapjuk.

3. tulajdonság azt mondja, hogy $\varphi(n)$ *multiplikatív* számelméleti függvény. Ilyen még $\sigma(n)$ (osztók összege), $d(n)$ (osztók száma).

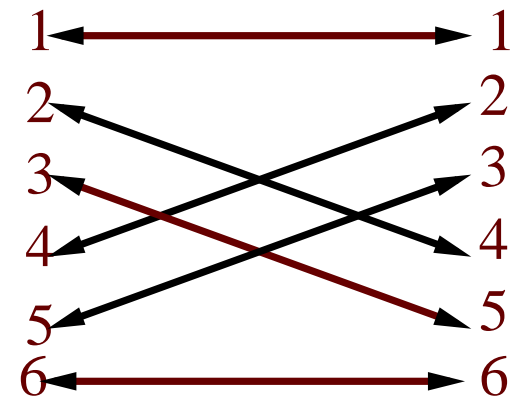
Prím modulus

$\varphi(p) = p - 1$. $\{c_1, c_2, \dots, c_{p-1}\}$ egy redukált maradékrendszer. (Az összes nemnulla maradék.) Ha $a \neq 0$, akkor $\{ac_1, ac_2, \dots, ac_{p-1}\}$ egy redukált maradékrendszer. Speciálisan, $\exists i: ac_i \equiv 1 \pmod{p}$. c_i az a **multiplikatív inverze**. („ $c_i = 1/a \pmod{p}$ ”)

Minden c_i -nek van $c_{i'}$ párja, hogy $c_i \cdot c_{i'} \equiv 1 \pmod{p}$.

Ha $i = i'$, akkor $c_i^2 \equiv 1 \pmod{p} \implies c_i^2 - 1 = (c_i - 1)(c_i + 1) \equiv 0 \pmod{p}$. p prím, így a szorzat valamelyik tényezőjét osztja $\implies c_i = \pm 1$. Tehát csak a ± 1 maradékok párja önmaguk.

$p = 7$ esetben



Wilson tétel

12. Tétel (Wilson-tétel). *Legyen $k \geq 2$ tetszőleges pozitív szám. Ekkor*

$$(k-1)! \equiv \begin{cases} -1 \pmod{k}, & \text{ha } k \text{ prím,} \\ 2 \pmod{k}, & \text{ha } k = 4, \\ 0 \pmod{k}, & \text{ha } k \geq 6 \text{ összetett szám.} \end{cases}$$

BIZONYÍTÁS $k = 4\sqrt{}$. Ha $k > 4$ és összetett, akkor van $1 < a < b < k$, melyekre $ab = k, \implies 1 \cdot 2 \cdot 3 \cdot \dots \cdot (k-1) = a \cdot b \cdot c \equiv 0 \pmod{k}$.

Legyen végül k prím $\implies 1$ és $k-1$ kivételével a szorzótényezők párbaállíthatóak, hogy a szorzatuk 1 legyen.

Például $k = 7$ -re

$$(k-1)! = 1 \cdot 6 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \equiv 6 \equiv -1 \pmod{k}$$

mert $2 \cdot 4 \equiv 3 \cdot 5 \equiv 1 \pmod{7}$.

$n!$ prímtényezős felbontása

Legyen $2 \leq p \leq n$ prím. Mekkora a hatványkitevője $n!$ felbontásában?

p	\dots	$2p$	\dots	$(p-1)p$	p^2	\dots	p^3	\dots	p^s	n	
p		p	\dots	p	p	\dots	p	\dots	p		minden p -ik
					p	\dots	p	\dots	p		minden p^2 -ik
							p	\dots	p		minden p^3 -ik
									\vdots		\vdots
									p		minden p^s -ik

Tehát p kitevője:

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

Lineáris kongruenciák

13. Tétel. Az $ax \equiv b \pmod{m}$ kongruencia akkor és csak akkor oldható meg, ha $d = d(a, m)$ osztója b -nek. Ilyenkor a megoldások száma d darab maradékosztály \pmod{m} .

BIZONYÍTÁS Ha megoldható, akkor $m \mid ax - b, \implies ax - b = ym \implies ax + ym = b \implies (a, m) \mid b$.

Ha $d = (a, m) \mid b$, akkor

$$ax \equiv b \pmod{m} \implies \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}},$$

ahol $\frac{a}{d}$ és $\frac{m}{d}$ már relatív prímek.

Ha a $\text{mod } \frac{m}{d}$ teljes maradékrendszer minden elemét végigszorozzuk a modulushoz relatív prím $\frac{a}{d}$ számmal, akkor ismét teljes maradékrendszerhez jutunk, \implies pontosan egy $\text{mod } \frac{m}{d}$ maradékosztály elemeire teljesül a kongruencia. Ha $x \equiv x_0 \pmod{\frac{m}{d}}$ megoldása, akkor

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d}$$

számok által meghatározott d darab $\text{mod } m$ maradékosztály lesz az eredeti megoldása.

Megoldás előállítása–elméleti út

1. Leosztunk (a, m) -el. $\implies ax \equiv b \pmod{m}$ -ben feltehető, hogy $d(a, m) = 1$.

$a^{\varphi(m)} \equiv 1 \pmod{m} \implies ax \equiv b \pmod{m}$ mindkét oldalát $a^{\varphi(m)-1}$ -el szorozva:

$$x \equiv b \cdot a^{\varphi(m)-1} \pmod{m},$$

hisz a kongruencia mindkét oldalát a -val szorozva $ax \equiv b \cdot a^{\varphi(m)} \equiv b \pmod{m}$ adódik.

m prímtényezős felbontásának ismeretében ez működik. Csak túl sok számolás.

Megoldás előállítás–gyakorlati út

$ax \equiv b \pmod{m}$: először is a és b értékét a velük $\text{mod } m$ kongruens legkisebb pozitív értékkel helyettesítjük: $a_1x \equiv b_1 \pmod{m}$

Most $a_1x - b_1 = x_1m \implies \frac{x_1m + b_1}{a_1}$ egész, azaz ha m maradéka $\text{mod } a_1$ az a_2 és b_1 maradéka $\text{mod } a_1$ az b_2 , akkor $x_1a_2 + b_2 = a_1x_2$. Ezt a gondolatot folytatva az x_i együtthatója (gyorsan) csökken.

Amikor 1, akkor onnan az eredeti kongruencia megoldása visszafejthető.

$$523x \equiv 39 \pmod{23}$$

$$17x \equiv 16 \pmod{23} \implies 23x_1 = 17x - 16$$

$$23x_1 \equiv -16 \pmod{17} \implies 6x_1 \equiv 1 \pmod{17}$$

$$6x_1 - 1 = 17x_2 \implies 5x_2 \equiv -1 \pmod{6}$$

$$5x_2 + 1 = 6x_3 \implies x_3 \equiv 1 \pmod{5}$$

$$\text{Visszafejtve: } x_3 = 5t + 1 \implies x = 23t + 5, \text{ azaz a megoldás:}$$

$$x \equiv 5 \pmod{23}$$