# Diszkrét matematika II.
# 3. előadás

Fancsali Szabolcs Levente
nudniq@inf.elte.hu

ELTE IK Komputeralgebra Tanszék

Mérai László diái alapján

# Kínai maradék tétel (múlt heti anyag!)

## 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 (múlt heti anyag!)

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

## 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 (múlt heti anyag!)

## 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 (múlt heti anyag!)

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 (múlt heti anyag!)

## 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 (múlt heti anyag!)

**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 (múlt heti anyag!)

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 (múlt heti anyag!)

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 (múlt heti anyag!)

## 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 $\varphi$ függvény (múlt heti anyag!)

## 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 $\varphi$ függvény (múlt heti anyag!)

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

## 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 (múlt heti anyag!)

## 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 (múlt heti anyag!)

## 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.

## Bizonyítás

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 (múlt heti anyag!)

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

## Bizonyítás

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 (múlt heti anyag!)

**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 $4 \cdot 23^{209} \equiv \ldots \mod 211$.

# Gyors hatványozás (ezzel kezdődik az új anyag)

Legyenek $m, a, n$ pozitív egészek, $m > 1$. Szeretnénk kiszámolni $a^n \bmod m$ maradékot hatékonyan.

Ábrázoljuk $n$-et 2-es számrendszerben:

$$n = \sum_{i=0}^{k} \varepsilon_i 2^i = (\varepsilon_k \varepsilon_{k-1} \dots \varepsilon_1 \varepsilon_0)_{(2)}, \text{ ahol } \varepsilon_0, \varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}.$$

Legyen $n_j$ $(0 \le j \le k)$ az első $j+1$ jegy által meghatározott szám:

$n_j = \lfloor n/2^{k-j} \rfloor = (\varepsilon_k \varepsilon_{k-1} \dots \varepsilon_{k-j+1})_{(2)}$

Ekkor meghatározzuk minden $j$-re az $x_j \equiv a^{n_j} \mod m$ maradékot:

$n_0 = \varepsilon_0 = 1$, $x_0 = a$.

$n_j = 2 \cdot n_{j-1} + \varepsilon_j \Rightarrow$

$$x_j = a^{\varepsilon_j} x_{j-1}^2 \bmod m = \begin{cases} 1 \cdot x_{j-1}^2 \bmod m, & \text{ha } \varepsilon_j = 0 \\ a \cdot x_{j-1}^2 \bmod m, & \text{ha } \varepsilon_j = 1 \end{cases} \Rightarrow$$

$x_k = a^n \bmod m$.

Az algoritmus helyessége az alábbi formulából következik (Biz.: HF):

$$a^n = a^{\sum_{i=0}^{k} \varepsilon_i 2^i} = \prod_{i=0}^{k} \left(a^{2^i}\right)^{\varepsilon_i}$$

# Gyors hatványozás

## Példa

Mi lesz $3^{111} \bmod 10$? (Euler-Fermat $\Rightarrow 7$)

$111_{(10)} = 1101111_{(2)}$ itt $k = 6$, $a = 3$.

| $j$ | $n_j$ | $x_j = a^{\varepsilon_j} \cdot x_{j-1}^2$ | $x_j \bmod 10$ |
|---|---|---|---|
| 0 | 1 | – | 3 |
| 1 | 1 | $x_1 = 3 \cdot 3^2$ | 7 |
| 2 | 0 | $x_2 = 7^2$ | 9 |
| 3 | 1 | $x_3 = 3 \cdot 9^2$ | 3 |
| 4 | 1 | $x_4 = 3 \cdot 3^2$ | 7 |
| 5 | 1 | $x_5 = 3 \cdot 7^2$ | 7 |
| 6 | 1 | $x_6 = 3 \cdot 7^2$ | 7 |

$3^{111} = 3^{64+32+8+4+2+1} = 3^{64} \cdot 3^{32} \cdot 3^8 \cdot 3^4 \cdot 3^2 \cdot 3 =$

$((((((3)^2 \cdot 3)^2 \cdot 1)^2 \cdot 3)^2 \cdot 3)^2 \cdot 3)^2 \cdot 3$

# Gyors hatványozás

## Példa

Oldjuk meg a $23x \equiv 4 \mod 211$ kongruencát!
Euler-Fermat $\Rightarrow x \equiv 4 \cdot 23^{209} \equiv \ldots \mod 211$.

Mi lesz $23^{209} \mod 211$?
$209_{(10)} = 11010001_{(2)}$ itt $k = 7$, $a = 23$.

| $j$ | $n_j$ | $x_j = a^{\varepsilon_j} \cdot x_{j-1}^2$ | $x_j \mod 211$ |
|---|---|---|---|
| 0 | 1 | – | 23 |
| 1 | 1 | $x_1 = 23 \cdot 23^2$ | 140 |
| 2 | 0 | $x_2 = 140^2$ | 188 |
| 3 | 1 | $x_3 = 23 \cdot 188^2$ | 140 |
| 4 | 0 | $x_4 = 140^2$ | 188 |
| 5 | 0 | $x_5 = 188^2$ | 107 |
| 6 | 0 | $x_6 = 107^2$ | 55 |
| 7 | 1 | $x_6 = 23 \cdot 55^2$ | 156 |

$x \equiv 4 \cdot 23^{209} \equiv 4 \cdot 156 \equiv 202 \mod 211$.

# Generátor

## Tétel (NB)

Legyen $p$ prímszám. Ekkor $\mathbb{Z}_p^*$-ban van generátor (primitív gyök), azaz van olyan $1 < g < p$ egész, mely hatványaiként előáll minden redukált maradékosztály: $\{\overline{g^0} = \overline{1}, \overline{g}, \overline{g^2}, \ldots, \overline{g^{p-1}}\} = \mathbb{Z}_p^*$, azaz $\{1 = g^0, g \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p\} = \{1, 2, \ldots, p-1\}$.

## Példa

3 generátor modulo 7

$$
\begin{aligned}
3^1 &= 3 = 3^0 \cdot 3 \equiv 1 \cdot 3 = 3 \equiv 3 \mod 7 \\
3^2 &= 9 = 3^1 \cdot 3 \equiv 3 \cdot 3 = 9 \equiv 2 \mod 7 \\
3^3 &= 27 = 3^2 \cdot 3 \equiv 2 \cdot 3 = 6 \equiv 6 \mod 7 \\
3^4 &= 81 = 3^3 \cdot 3 \equiv 6 \cdot 3 = 18 \equiv 4 \mod 7 \\
3^5 &= 243 = 3^4 \cdot 3 \equiv 4 \cdot 3 = 12 \equiv 5 \mod 7 \\
3^6 &= 729 = 3^5 \cdot 3 \equiv 5 \cdot 3 = 15 \equiv 1 \mod 7
\end{aligned}
$$

# Generátor

## Példa

2 generátor modulo 11

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $2^n \bmod 11$ | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |

2 nem generátor modulo 7

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $2^n \bmod 7$ | 2 | 4 | 1 | 2 | 4 | 1 |

# Diszkrét logaritmus

## Definíció

Legyen $p$ prímszám, $g$ generátor modulo $p$. Ekkor az $a \in \mathbb{Z}$: $(p \nmid a)$ $g$ alapú diszkrét logaritmusa (indexe):

$$\log_g a = n: \quad a \equiv g^n \bmod p, \quad 0 \leq n < p-1.$$

## Példa

3 generátor modulo 7:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $3^n$ | 3 | 2 | 6 | 4 | 5 | 1 |

$\longrightarrow$

| $3^n$ | 3 | 2 | 6 | 4 | 5 | 1 |
|---|---|---|---|---|---|---|
| $n$ | 1 | 2 | 3 | 4 | 5 | 6 |

azaz

| $a$ | 3 | 2 | 6 | 4 | 5 | 1 |
|---|---|---|---|---|---|---|
| $\log_3 a$ | 1 | 2 | 3 | 4 | 5 | 6 |

$\longrightarrow$

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $\log_3 a$ | 6 | 2 | 1 | 4 | 5 | 3 |

# Diszkrét logaritmus

## Példa

2 generátor modulo 11

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $2^n \bmod 11$ | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |

Logaritmus-táblázat:

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\log_2 a$ | 10 | 1 | 8 | 2 | 4 | 9 | 7 | 3 | 6 | 2 |

## Tétel (HF)

Legyen $p$ prímszám, $g$ generátor modulo $p$, $1 \leq a, b < p$, $n \in \mathbb{Z}$ . Ekkor

$$\log_g(a \cdot b) \equiv \log_g a + \log_g b \mod p-1$$
$$\log_g(a^n) \equiv n \cdot \log_g a \mod p-1$$

# Alkalmazások

Számelmélet alkalmazási területei:

- Kriptográfia
  - üzenetek titkosítása;
  - digitális aláírás;
  - azonosítás, . . .
- Kódelmélet
- . . .

# Caesar kód

Julius Caesar katonáival a következő módon kommunikált:

Feleltessük meg az (angol) ábécé betüit a $\{0, 1, \ldots, 25\}$ halamznak:

$$\begin{aligned} \mathtt{a} &\mapsto 0 \\ \mathtt{b} &\mapsto 1 \\ \mathtt{c} &\mapsto 2 \\ &\vdots \\ \mathtt{z} &\mapsto 25 \end{aligned}$$

**Titkos kulcs** $s \in \{0, 1, \ldots, 25\}$.

**Titkosítás** adott $a \in \{0, 1, \ldots, 25\}$ esetén $a$ titkosítása $a \mapsto a + s \bmod 26$. Üzenet titkosítás betünként.

**Kititkosítás** adott $b \in \{0, 1, \ldots, 25\}$ esetén $b$ kititkosítása $b \mapsto a - s \bmod 26$. Üzenet kititkosítás betünként.

## Példa

`hello` titkosítása az $s = 13$ kulcscsal:

$\mathtt{hello} \to 7\ 4\ 11\ 11\ 14 \overset{\text{titkosítás}}{\to} 20\ 17\ 24\ 24\ 1 \to \mathtt{uryyb}$

`urzzc` kititkosítása az $s = 13$ kulcscsal:

$\mathtt{uryyb} \to 20\ 17\ 24\ 24\ 1 \overset{\text{kititkosítás}}{\to} 7\ 4\ 11\ 11\ 14 \to \mathtt{hello}$

# Caesar kód

Ha $s = 13$ kulcsot választjuk: Rot13.
Titkosítás és kititkosítás ugyan azzal a kulcscsal: $-13 \equiv 13 \mod 26$.

A titkosítás nem biztonságos: betűgyakoriság vizsgálattal törhető
(al-Kindi i.sz 9 sz.)

Ha a különböző pozíciókban különböző kulcsokat választhatunk
(véletlenszerűen) $\Rightarrow$ bizonyítottan biztonságos

**Gyakorlatban:** One Time Pad – OTP

**Üzenetek:** bináris formában: $\mathtt{m}=100100101$
**Kulcs:** bináris sorozat: $\mathtt{s}=010110110$
**Titkosítás:** bitenkénti XOR (mod2 összeadás):

$$\begin{array}{rr} & \mathtt{m}=100100101 \\ \text{XOR} & \mathtt{s}=010110110 \\ \hline & \mathtt{c}=110010011 \end{array}$$

Kritikus pont: az $s$ titkos kulcs átadása.

# RSA

Ron **Rivest**, Adi **Shamir** és Leonard **Adleman** 1977-ben a következő eljárást javasolták:

**Kulcskenerálás** Legyen $p$, $q$ két (nagy, 1024 bites) prím, $n = p \cdot q$.
Legyen $e \in \{1, \ldots, \varphi(n)\}$, hogy $(e, \varphi(n)) = 1$.
Legyen $d$ az $ex \equiv 1 \mod \varphi(n)$ kongruencia megoldása.
Kulcsok: nyilvános kulcs $(n, e)$.
titkos kulcs $d$.

**Titkosítás** Adott $0 \leq m < n$ üzenet titkosítása:
$c = m^e \mod n$.

**Kititkosítás** Adott $0 \leq c < n$ titkosított üzenet kititkosítása:
$m = c^d \mod n$.

**Algoritmus helyessége**

$$c^d \equiv (m^e)^d = m^{e \cdot d} = m^{k \cdot \varphi(n)+1} \overset{\text{E-F}}{\equiv} m \mod n$$

# RSA

Valóságban az $m$ üzenet egy titkos kulcs további titkosításhoz.

Az eljárás biztonsága azon múlik, hogy nem tudjuk hatékonyan faktorizálni az $n = p \cdot q$ szorzatot.

## Feladat

Találjuk meg a következő szám osztóit.
RSA-100 =
522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139

RSA-2048=
251959084756578934940271832400483985714292821262040320277771378360436620207075955562640185258807844069182906412495150821892985591491761845028084891200728449926873928072877767359714183472702618963750149718246911650776133798590957000973304597488084284017974291006424586918171951187461215151726546322822168699875491824224336372590851418654620435767984233871847744479207399342365848238242811981638150106748104516603773060562016196762561338441436038339044149526344321901146575444541784240209246165157233507787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103971228221207203 57

# RSA

RSA-2048 faktorizálása:

Próbaosztás (Erathoszthenész szitája): $n$ számot esetén $\sim \sqrt{n}$ osztást kell végezni:

RSA-2048 $\sim 2^{2048}$, $\sim 2^{1024}$ próbaosztás.

Ha $1$ másodperc alatt $\sim 10^9 \approx 2^{30}$ osztás $\Rightarrow 2^{1024}/2^{30} = 2^{994}$ másodperc kell a faktorizáláshoz.

$2^{994}$ másodperc $=2^{969}$ év.

Ugyan ezt 2 db géppel: $2^{968}$ év.

Ugyan ezt a legjobb (ismert) algoritmussal:
$25000000000000000000000000000000$ év $(= 2,5 \cdot 10^{30})$

Univerzum életkora: $1,38 \cdot 10^{10}$ év.

# RSA

## Példa

**Kulcsgenerálás**

Legyen $p = 61$, $q = 53$ és $n = 61 \cdot 53 = 3233$, $\varphi(3233) = 3120$.

Legyen $e = 17$. Bővített euklidészi algoritmussal: $d = 2753$

Nyilvános kulcs: $(n = 3233, e = 17)$;

Titkos kulcs: $d = 2753$.

**Titkosítás** Legyen $m = 65$.

$c = 2790 \equiv 65^{17} \mod 3233$

**Kititkosítás** Ha $c = 2790$:

$2790^{2753} \equiv 65 \mod 3233$

**Digitális aláírásit** is lehet generálni: $e$ és $d$ felcserélésével:
(Ekkor külön $n'$, $e'$, $d'$ kell a titkosításhoz!)

**Aláírás** Legyen $s = m^d \mod n$, ekkor az aláírt üzenet: $(m, s)$.

**Ellenőrzés** $m \stackrel{?}{\equiv} s^e \mod n$.

# Diffie-Hellman kulcscsere protokoll

Az első nyilvános kulcsú kriptográfiai rendszert Whitfield **Diffie** és Martin **Hellman** 1976-ban publikálta.

| Alice | | Bob |
|---|---|---|
| | nem megbízható csatorna | |
| választ $a \in_R \{0, 1, \ldots, p-2\}$ | | választ $b \in_R \{0, 1, \ldots, p-2\}$ |
| | $\xrightarrow{g^a}$ | |
| | $\xleftarrow{g^b}$ | |
| kiszámolja $\left(g^b\right)^a$ | | kiszámolja $\left(g^a\right)^b$ |
| | közös titkos kulcs: $g^{ab}$ | |

**Nyilvános paraméterek** $p$ (nagy) pírm, $g$ generátor $\bmod p$.
**Kulcsok** Alice titkos kulcsa $a$: $1 \leq a < p-1$, nyilvános kulcsa $g^a \bmod p$
Bob titkos kulcsa $b$: $1 \leq a < p-1$, nyilvános kulcsa $g^b \bmod p$
**Közös kulcs** $g^{ab} \bmod p$.

# Diffie-Hellman kulcscsere protokoll

A protokoll biztonsága azon múlik, hogy a diszkrét logaritmus kiszámítás nehéz.

Ha $p \sim 2^{2048}$ (2048 bites), diszkrét logaritmus számolása $\sim 10^{30}$ év.

## Példa

**Nyilvános paraméterek** Legyen $p = 11$, $g = 2$.

**Kulcsok** Alice titkos kulcsa $a = 4$, nyilvános kulcsa $2^4 \bmod p = 5$

Bob titkos kulcsa $b = 8$, nyilvános kulcsa $2^8 \bmod p = 3$

**Közös kulcs** $\left(g^b\right)^a = 3^4 \bmod p = 4$, $\left(g^a\right)^b = 5^8 \mathrm{mod} = 4$.

# Műveletek

## Definíció (Művelet)

Egy $X$ halmazon értelmezett ($r$-változós, "$r$-ér") művelet alatt egy $* : X^r \to X$ függvényt értünk.
Egy $X$ halmazon értelmezett binér (kétváltozós) művelet egy $* : X \times X \to X$ függvény. Gyakran $*(x, y)$ helyett $x * y$-t írunk.
Egy $X$ halmazon értelmezett unér (egyváltozós) művelet egy $* : X \to X$ függvény.

## Példa

- $\mathbb{C}$ halmazon az $+$ is, és $\cdot$ is binér műveletek.
- $\mathbb{C}$ halmazon az $\div$ (osztás) nem művelet, mert $\mathrm{dmn}(\div) \neq \mathbb{C} \times \mathbb{C}$.
- $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ halmazon az $\div$ binér művelet.
- $\mathbb{C}$ halmazon a $0$ illetve $1$ konstans kijelölése nullér művelet.
- $\mathbb{R}^n$ ($n > 1$) vektortéren a vektorok skaláris szorzása nem művelet, mert $\mathrm{rng}(\langle , \rangle) = \mathbb{R} \neq \mathbb{R}^n$ (a szorzás eredménye nem vektor)
- $\mathbb{R}^n$ vektortéren egy adott $\lambda \in \mathbb{R}$ skalárral való szorzás unér művelet

# Műveleti tulajdonságok

## Definíció

A $* : X \times X \to X$ művelet:
- asszociatív, ha $\forall a, b, c \in X : (a * b) * c = a * (b * c)$;
- kommutatív, ha $\forall a, b \in X : a * b = b * a$.

## Példa

- $\mathbb{C}$-n az $+$ ill. a $\cdot$ műveletek asszociatívak, kommutatívak.
- A függvények halmazán a kompozíció művelete asszociatív: $(f \circ g) \circ h = f \circ (g \circ h)$.
- A függvények halmazán a kompozíció művelete nem kommutatív: $f(x) = x + 1$, $g(x) = x^2$: $x^2 + 1 = (f \circ g)(x) \neq (g \circ f)(x) = (x + 1)^2$.
- A kivonás az egész számok halmazán nem asszociatív: $-1 = (1 - 1) - 1 \neq 1 - (1 - 1) = 1$.

# Művelettartó leképezések

## Definíció

Legyen $X$ halmaz a $*$ művelettel, $Y$ a $\circ$ művelettel. Az $f : X \to Y$ függvény művelettartó, ha $\forall x, y \in X$ esetén

$$f(x * y) = f(x) \circ f(y).$$

## Példa

- Legyen $X = \mathbb{R}$ az $+$ művelettel, $Y = \mathbb{R}^+$ a $\cdot$ művelettel.
  Ekkor az $x \mapsto a^x$ művelettartó: $a^{x+y} = a^x \cdot a^y$.
- Legyen $X = Y = \mathbb{C}$ az $+$ művelettel.
  Ekkor a $z \mapsto \overline{z}$ művelettartó: $\overline{z + w} = \overline{z} + \overline{w}$.
- Legyen $X = \mathbb{Z}$ a $+$ művelettel, $Y = \mathbb{Z}_m$ a $+_m$ (összeadás modulo $m$) művelettel.
  Ekkor a $n \mapsto n \bmod m$ művelettartó:
  $(k + n) \bmod m = (k \bmod m) +_m (n \bmod m)$.
- Legyen $X = \{\mathrm{I}, \mathrm{H}\}$ a XOR/$\wedge$ művelettel, $\mathbb{Z}_2$ a $+/\cdot$ művelettel. Ekkor a $\mathrm{H} \mapsto 0$, $\mathrm{I} \mapsto 1$ hozzárendelés művelettartó (XOR-nak $+$).

# Algebrai struktúrák

## Definíció (Algebrai struktúra)

A $(H; M)$ pár algebrai struktúra, ha $H$ egy halmaz, $M$ pedig $H$-n értelmezett műveletek halmaza.

A $(H; \{*, +, \circ\})$ jelölés helyett a $(H; *, +, \circ)$ jelölést is használhatjuk.

## Definíció (Grupoid)

Ha az $M$ művelethalmaz egyetlen műveletet tartalmaz, és az egy binér művelet, akkor a $(H; M)$ struktúrát grupoidnak nevezzük.

- $(\mathbb{N}; +)$ algebrai struktúra, mert természetes számok összege természetes szám (ld. Diszkrét matematika 1.), és grupoid is.
- $(\mathbb{N}; -)$ nem algebrai struktúra, mert például $0 - 1 = -1 \notin \mathbb{N}$.
- $(\mathbb{Z}; +, \cdot)$ algebrai struktúra, mert egész számok összege és szorzata egész szám (ld. Diszkrét matematika 1.), de nem grupoid.
- $(\mathbb{Z}_m; +, \cdot)$ algebrai struktúra (ld. Diszkrét matematika 1.), de nem grupoid, mert két művelet van.

# Félcsoportok

## Definíció (Félcsoport)

A $(G; *)$ grupoid félcsoport, ha $*$ asszociatív $G$-n.

## Definíció (egységelem, semleges elem)

Ha létezik olyan $s \in G$ elem, amire $\forall g \in G : s * g = g * s = g$, akkor az $s$ elemet semleges elemnek (más néven egységelemnek) nevezzük.

## Definíció (Monoid)

Ha $(G; *)$ félcsoportban létezik $s$ semleges elem, akkor $G$-t semleges elemes félcsoportnak, egységelemes félcsoportnak, más néven monoidnak nevezzük.

- $\mathbb{N}$ az $+$ művelettel egységelemes félcsoport $n = 0$ egységelemmel.
- $\mathbb{Q}$ a $\cdot$ művelettel egységelemes félcsoport $n = 1$ egységelemmel.
- $\mathbb{C}^{k \times k}$ a mátrixszorzással egységelemes félcsoport az egységmátrixszal mint egységelemmel.