# Diszkrét matematika I. középszint

10. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

# Felhívás

Szakirányválasztó fórum december 4-én.
Jelentkezés november 26-ig:
http://goo.gl/forms/dYIHA8SQOZ

Bővebb információ:
http://compalg.inf.elte.hu/∼nagy

# Lineáris diofantikus egyenletek

Diofantikus egyenletek: egyenletek egész megoldásait keressük.

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

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, u.i. 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 (biz.: később)

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

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

# Kínai maradéktétel

## Tétel

Legyenek $1 < m_1, m_2, \ldots, m_n$ 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:
$\overline{a} = \{x \in \mathbb{Z} : x \equiv a \pmod m\} = \{a + \ell m : \ \ell \in \mathbb{Z}\}$.

## Példa

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

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

# 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 abszolút értékű 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: $(a + \ell m, m) = (a, m) = 1$. Ezeket a maradékosztályokat redukált maradékosztályoknak nevezzük.

## 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.

# 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 értelmes 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 $\overline{a} = \overline{a^*}$, $\overline{b} = \overline{b^*} \Rightarrow a \equiv a^* \pmod{m}$, $b \equiv b^* \pmod{m} \Rightarrow$
$\Rightarrow a + b \equiv a^* + b^* \pmod{m} \Rightarrow \overline{a+b} = \overline{a^* + b^*} \Rightarrow \overline{a} + \overline{b} = \overline{a^*} + \overline{b^*}$.
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 esetén legyen $\mathbb{Z}_m$ a maradékosztályok halmaza. Ekkor a halmaz elemei között definiálhatunk összeadást, illetve szorzást.

## Példa

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

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

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

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

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

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

# 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 $a \cdot \frac{m}{d} = \frac{a}{d} \cdot m \equiv 0 \pmod{m}$, 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 $ax \equiv 1 \pmod{m}$ azaz $\overline{a} \cdot \overline{x} = \overline{1}$. □

# Euler-féle $\varphi$ függvény

## Definíció

Egy $m > 0$ egész szám esetén legyen $\varphi(m)$ az $m$-nél kisebb, hozzá relatív prím pozitív 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

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

## Tétel (NB)

Legyen $m$ kanonikus alakja $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$. Ekkor
$\varphi(m) = m \cdot \prod_{i=1}^{\ell} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{\ell} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$.

## Példa

$\varphi(5) = 5\left(1 - \frac{1}{5}\right) = 5^1 - 5^0 = 4$;
$\varphi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = (2^1 - 2^0)(3^1 - 3^0) = 2$;
$\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = (2^2 - 2^1)(3^1 - 3^0) = 4$;
$\varphi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = (3^1 - 3^0)(5^1 - 5^0) = 8$.

# Euler-Fermat tétel

## Tétel

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

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

## Következmény (Fermat tétel)

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

## Példa

$\varphi(6) = 2 \Rightarrow 5^2 = 25 \equiv 1 \pmod{6}$;
$\varphi(12) = 4 \Rightarrow 5^4 = 625 \equiv 1 \pmod{12}$; $7^4 = 2401 \equiv 1 \pmod{12}$.

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

# Euler-Fermat tétel bizonyítása

## Lemma

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

## Bizonyítás

Tudjuk, hogy $aa_i + b \equiv aa_j + b \pmod{m} \Leftrightarrow aa_i \equiv aa_j \pmod{m}$. Mivel $(a, m) = 1$, egyszerűsíthetünk $a$-val: $a_i \equiv a_j \pmod{m}$. Tehát $a \cdot a_1 + b$, $a \cdot a_2 + b$,..., $a \cdot a_m + b$ páronként inkongruensek. Mivel számuk $m$, így teljes maradékrendszert alkotnak.

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

# Euler-Fermat tétel bizonyítása

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

## 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

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

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

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

□

# Euler-Fermat tétel

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

## Példa

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

Oldjuk meg a $2x \equiv 5 \pmod{7}$ kongruenciát!
$\varphi(7) = 6$. Szorozzuk be mindkét oldalt $2^5$-nel. Ekkor
$5 \cdot 2^5 \equiv 2^6 x \equiv x \pmod{7}$. És itt $5 \cdot 2^5 = 5 \cdot 32 \equiv 5 \cdot 4 = 20 \equiv 6 \pmod{7}$.

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

# Gyors hatványozás

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:

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

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

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

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

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

$x_k = a^n \bmod m$.

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 $k = 6$, $a = 3$, $m = 10$.

| $j$ | $n_j$ | $x_j = a^{\varepsilon_{k-j}} \cdot x_{j-1}^2$ | $x_j \bmod 10$ |
|---|---|---|---|
| 0 | 1 | – | 3 |
| 1 | 11 | $x_1 = 3 \cdot 3^2$ | 7 |
| 2 | 110 | $x_2 = 7^2$ | 9 |
| 3 | 1101 | $x_3 = 3 \cdot 9^2$ | 3 |
| 4 | 11011 | $x_4 = 3 \cdot 3^2$ | 7 |
| 5 | 110111 | $x_5 = 3 \cdot 7^2$ | 7 |
| 6 | 1101111 | $x_6 = 3 \cdot 7^2$ | 7 |

# Gyors hatványozás

## Példa

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

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

| $j$ | $n_j$ | $x_j = a^{\varepsilon_{k-j}} \cdot x_{j-1}^2$ | $x_j \bmod 211$ |
|---|---|---|---|
| 0 | 1 | – | 23 |
| 1 | 11 | $x_1 = 23 \cdot 23^2$ | 140 |
| 2 | 110 | $x_2 = 140^2$ | 188 |
| 3 | 1101 | $x_3 = 23 \cdot 188^2$ | 140 |
| 4 | 11010 | $x_4 = 140^2$ | 188 |
| 5 | 110100 | $x_5 = 188^2$ | 107 |
| 6 | 1101000 | $x_6 = 107^2$ | 55 |
| 7 | 11010001 | $x_6 = 23 \cdot 55^2$ | 156 |

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