Diszkrét matematika 2

4. előadás
Számelmélet

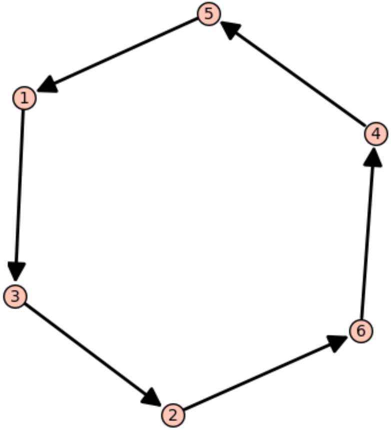
Mérai László
merai@inf.elte.hu
https://sites.google.com/view/laszlomerai

Komputeralgebra Tanszék

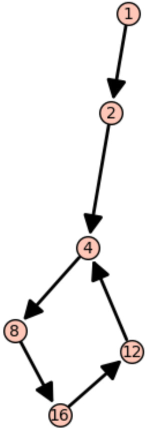
2023 ősz

Hatványmaradékok

Az $a^i \bmod n$ hatványok:



$10^i \bmod 7$



$2^i \bmod 20$

Euler-Fermat tétel

Tétel (Euler-Fermat)

Legyenek $a, n \in \mathbb{Z}$, $(a, n) = 1$. Ekkor

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

ahol φ az Euler-féle függvény.

Bizonyítás: később

Példa

- $2^6 \equiv 1 \mod 7$, mert $\varphi(7) = 6$.
- $3^6 \equiv 1 \mod 7$, mert $\varphi(7) = 6$.
- $9^8 \equiv 1 \mod 20$, mert $\varphi(20) = 8$.

Figyelem, kisebb hatvány is lehet 1:

- $1^6 = 1 \equiv 1 \mod 7$,
- $2^3 = 8 \equiv 1 \mod 7$,
- $9^2 = 81 \equiv 1 \mod 20$.

Maradékosztályok

Jelölés: Legyen $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ a nemnegatív maradékok halmaza, és tekintsük a $+, \cdot$ műveleteket modulo n

Példa

$\mathbb{Z}_3 = \{0, 1, 2\}$ $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Emlékeztető: ha $(a, n) = 1$, akkor $ax \equiv b \mod n$ kongruenciának mindig létezik egyértelmű megoldása modulo n.

Legyen $\mathbb{Z}_n^* = \{1 \leq a < n : (a, n) = 1\}$. Speciálisan $\#\mathbb{Z}_n^* = \varphi(n)$.

Példa

$\mathbb{Z}_3^* = \{1, 2\}$, $\mathbb{Z}_4^* = \{1, 3\}$, $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

Euler-Fermat tétel – bizonyítás

Legyenek $a, n \in \mathbb{Z}$, $(a, n) = 1$. Ekkor $a^{\varphi(n)} \equiv 1 \mod n$.

Bizonyítás. A bizonyítás lineáris kongruenciákkal!

Tekintsük az $ax \equiv b \mod n$ lineáris kongruenciát. Mivel $(a, n) = 1$, minden b-hez létezik egyértelmű x megoldás. Azaz az $x \mapsto ax \bmod n$, $\mathbb{Z}_n^*$ egy bijekciója. Így a

$$\mathbb{Z}_n^* \quad \text{és} \quad \{ax \bmod n : x \in \mathbb{Z}_n^*\}$$

halmazok azonosak. Ekkor a halmazok elemeinek szorzata is megegyezik:

$$\prod_{x \in \mathbb{Z}_n^*} x \equiv \prod_{x \in \mathbb{Z}_n^*} ax \equiv a^{\varphi(n)} \prod_{x \in \mathbb{Z}_n^*} x \mod n.$$

Mivel

$$\left(n, \prod_{x \in \mathbb{Z}_n^*} x\right) = 1$$

így a szorzattal egyszerűsíthetünk: $1 \equiv a^{\varphi(n)} \mod n$. $\square$

Euler-Fermat tétel – példák

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

Példa

Mi lesz a 3^{111} utolsó számjegye tízes számrendszerben? Mi lesz $3^{111} \mod 10$?

$\varphi(10) = 4 \Rightarrow$

$3^{111} = 3^{4\cdot 27+3} = \left(3^4\right)^{27} \cdot 3^3 \equiv 1^{27} \cdot 3^3 = 3^3 = 27 \equiv 7 \mod 10$

Példa

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

$\varphi(7) = 6$. Szorozzuk be mindkét oldalt 2^5-el. Ekkor

$5 \cdot 2^5 \equiv 2^6 x \equiv x \mod 7$. És itt $5 \cdot 2^5 = 5 \cdot 32 \equiv 5 \cdot 4 = 20 \equiv 6 \mod 7$.

Példa

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

$\varphi(211) = 210$. Szorozzuk be mindkét oldalt 23^{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

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

Ötlet:

Ábrázoljuk k-t 2-es számrendszerben:

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

$$a^k \equiv a^{\sum_{i=0}^{\ell} \varepsilon_i 2^i} \equiv \prod_{i=0}^{\ell} (a^{\varepsilon_i})^{2^i}$$

$$\equiv \left(\left(\ldots \left((a^{2\varepsilon_\ell} \mod n) \cdot a^{\varepsilon_{\ell-1}} \mod n \right)^2 \ldots \right)^2 \cdot a^{\varepsilon_1} \mod n \right)^2 \cdot a^{\varepsilon_0} \mod n$$

Példa $3^{11} \equiv ? \mod 5$. $11 = 2^3 + 2^1 + 2^0 = (1011)_2$. Így

$$3^{11} \equiv \left(\left((3^{2\cdot 1} \mod 5) \cdot 3^0 \mod 5 \right)^2 \cdot 3^1 \mod 5 \right)^2 \cdot 3^1 \mod 5$$

Gyors hatványozás

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

Általában: $k = (\varepsilon_\ell \varepsilon_{\ell-1} \ldots \varepsilon_1 \varepsilon_0)_{(2)}$.
Legyen k_j ($0 \leq j \leq \ell$) az első $j+1$ jegy által meghatározott szám:
$k_j = \lfloor k/2^{\ell-j} \rfloor = (\varepsilon_\ell \varepsilon_{\ell-1} \ldots \varepsilon_{\ell-j+1})_{(2)}$

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

$k_0 = \varepsilon_\ell = 1$, $x_0 = a$.

$$k_j = 2 \cdot k_{j-1} + \varepsilon_{\ell-j} \Rightarrow x_j = x_{j-1}^2 \cdot a^{\varepsilon_{\ell-j}} \mod n = \begin{cases} x_{j-1}^2 \mod n, & \text{ha } \varepsilon_{\ell-j} = 0 \\ x_{j-1}^2 \cdot a \mod n, & \text{ha } \varepsilon_{\ell-j} = 1 \end{cases} \Rightarrow$$

$x_\ell = a^k \mod n$.

- Az algoritmus helyessége HF
- Számítási igény: $\approx \log k$ művelet n méretű számokon.

Gyors hatványozás – példa

Példa

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

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

j	k_j	$x_j = a^{\varepsilon_j} \cdot x_{j-1}^2$	$x_j \bmod 10$
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

Példa

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

Euler-Fermat $\Rightarrow x \equiv 4 \cdot 23^{209} \equiv \dots \mod 211$.

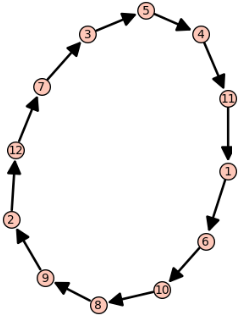
Mi lesz $23^{209} \mod 211$? $209_{(10)} = 11010001_{(2)}$ itt $\ell = 7$, $a = 23$.

j	k_j	$x_j = a^{\varepsilon_j} \cdot x_{j-1}^2$	$x_j \mod 211$
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

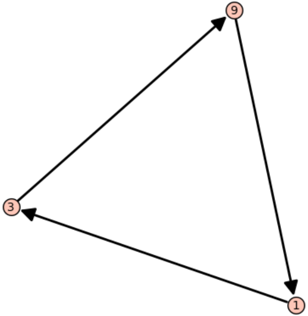
$x \equiv 4 \cdot 23^{209} \equiv 4 \cdot 156 \equiv 202 \mod 211$.

Hatványok maradékai még egyszer

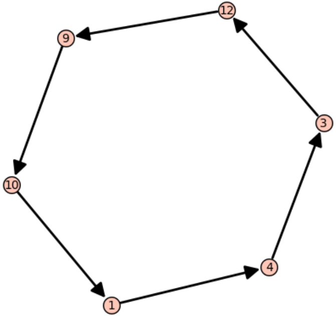
Legyen p egy prímszám és $p \nmid a$. Ekkor az Euler-Fermat tétel szerint $a^{p-1} \equiv 1 \mod p$. ($\varphi(p) = p - 1$)



$6^i \mod 13$



$3^i \mod 13$



$4^i \mod 13$

Vannak jó a alapok, melyekenk $p - 1$ különböző hatványa van modulo p.

Generátorok

Tétel (NB)

Legyen p prímszám. Ekkor $\mathbb{Z}_p^*$-ban van generátor (primitív gyök): van olyan $1 < g < p$ egész, melyre,
$\{1 = g^0, g \bmod p, g^2 \bmod p, \ldots, g^{p-2} \bmod p\} = \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$.

Példa

3 generátor modulo 7

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

Generátor – példa

Példa

2 generátor modulo 11

n	0	1	2	3	4	5	6	7	8	9
$2^n \bmod 11$	1	2	4	8	5	10	9	7	3	6

Példa

2 nem generátor modulo 7

n	0	1	2	3	4	5
$2^n \bmod 7$	1	2	4	1	2	4

Diszkrét logaritmus

Definíció

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

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

Példa

3 generátor modulo 7:

n	0	1	2	3	4	5
3^n	1	3	2	6	4	5

$\longrightarrow$

3^n	3	2	6	4	5	1
n	1	2	3	4	5	0

azaz

a	3	2	6	4	5	1
$\log_3 a$	1	2	3	4	5	0

Diszkrét logaritmus

Példa

2 generátor modulo 11

n	0	1	2	3	4	5	6	7	8	9
$2^n \bmod 11$	1	2	4	8	5	10	9	7	3	6

Logaritmus-táblázat:

a	1	2	3	4	5	6	7	8	9	10
$\log_2 a$	0	1	8	2	4	9	7	3	6	5

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 betűit a $\{0, 1, \ldots, 25\} = \mathbb{Z}_{26}$ halmaznak:

$$\begin{array}{lcl} \texttt{a} & \mapsto & 0 \\ \texttt{b} & \mapsto & 1 \\ \texttt{c} & \mapsto & 2 \\ & & \vdots \\ \texttt{z} & \mapsto & 25 \end{array}$$

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 betűnként.

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

Példa

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

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

`uryyc` kititkosítása az $s = 13$ kulccsal:

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

Caesar kód

Ha $s = 13$ kulcsot választjuk: Rot13.
Titkosítás és kititkosítás ugyanazzal a kulccsal: $-13 \equiv 13 \mod 26$.

A titkosítás nem biztonságos: betűgyakoriság vizsgálattal törhető.

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

Gyakorlatban: One Time Pad – OTP

Üzenetek: bináris formában: m=100100101
Kulcs: bináris sorozat: s=010110110
Titkosítás: bitenkénti XOR ($\mathrm{mod}\ 2$ összeadás):

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

Kritikus pont: az s titkos kulcs átadása.