Diszkrét matematika 1. középszint

11. előadás

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

Komputeralgebra Tanszék

2017. ősz

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 maradékosztályokból, 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 $\overline{b} \neq \overline{0}$, 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 $\overline{a} \cdot \overline{x} = \overline{1}$. □

Maradékosztályok

Megjegyzés

Könnyen látható, hogy tetszőleges $1 < m \in \mathbb{Z}$ esetén $\mathbb{Z}_m$-en a maradékosztály-összeadás asszociatív, kommutatív, $\overline{0}$ semleges elem, minden elemnek van additív inverze; a maradékosztály-szorzás asszociatív és teljesül a maradékosztály-összeadásra vonatkozó disztributivitása, így $(\mathbb{Z}_m; +, \cdot)$ gyűrű (ráadásul kommutatív és egységelemes ($\overline{1}$) is).
Ha a modulus egy p prím, akkor ráadásul az előző tétel alapján minden nem-nulla elemnek van multiplikatív inverze is, így $(\mathbb{Z}_p; +, \cdot)$ test.

Euler-féle φ függvény

Definíció

Egy $m > 0$ egész szám esetén legyen $\varphi(m)$ az m-nél kisebb, hozzá relatív prím természetes számok száma $\varphi(m) = |\{j : \ 0 \leq j < m, (m, j) = 1\}|$.

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 φ függvény

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

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 tízes 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 $4 \cdot 23^{209} \equiv \ldots \pmod{211}$.

RSA

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

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

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

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

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

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 =
1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139

RSA-2048=
2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440691829064124951508218929855914917618450280848912007284499268739280728777673597141834727026189637501497182469116507761337985909570009733045974880842840179742910064245869181719511874612151517265463228221686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067481045166037730605620161967625613384414360383390441495263443219011465754445417842402092461651572335077870774981712577246796292638635637328991215483143816789988504044536402352738195137863656439121201039712282212072035 7

RSA

RSA-2048 faktorizálása:

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

RSA-2048 $n \sim 2^{2048}$, $\sqrt{n} \sim 2^{1024}$ 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 $\approx 2^{969}$ év.

Ugyanezt 2 db géppel: 2^{968} év.

Ugyanezt 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 euklideszi algoritmussal: $d = 2753$.

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

Titkos kulcs: $d = 2753$.

Titkosítás: Legyen $m = 65$.

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

Kititkosítás: Ha $c = 2790$:

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

Digitális aláírást is lehet generálni: e és d felcserélésével:

(Ekkor külön n', e', d' kell a titkosításhoz!)

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

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