Informatikai biztonság alapjai 1. gyakorlat

Oláh Norbert

2022.

Tartalom

RSA titkosítás alapjai

- Prímszámok szorzata
  ”amilyen egyszerű két prímszámot összeszorozni,ugyanolyan nehézségekbe ütközik a faktorizáció, azaz a szorzat alapján megállapítani, hogy mely számokat is szoroztuk össze”
- Nehéz matematikai problémák
  Nincs rá polinomiális idejű algoritmus.
  Diszkrét logaritmus probléma
  Elliptikus Görbe diszkrét logaritmus probléma
  Faktorizáció

Oszthatóság

Definition

A b egész számot az a egész szám osztójának nevezzük, ha létezik olyan q egész szám, amelyre $a = bq$.
Jelölés: $b|a$.

- a az osztandó
- b az osztó
  Osztó: azokat a számokat, amelyekkel egy A szám osztható, az A szám osztóinak nevezzük. Minden számnak legalább két osztója van, 1 és önmaga.
- q hányados

Alapok

- **Prímszám (törzsszám)**: csak két osztója van, 1 és önmaga, pl. 2, 3, 5, 7.
- **Összetett szám**: 1-en és önmagán kívül más osztója is van, pl. 4, 6, 10.
  Minden összetett szám felbontható prímszámok szorzatára, pl. $60 = 2 * 2 * 3 * 5$
- **Legnagyobb közös osztó**

Definition

Az a és b számok legnagyobb közös osztója d, ha

- $d|a$ és $d|b$; és
- ha egy c-re $c|a$, $c|b$ teljesül akkor $|c| \leq |d|$

$(80, 50)$ legnagyobb közös osztója?

Maradék osztás tétele

Definition

Tetszőleges a és $b \neq 0$ számokhoz egyértelműen léteznek olyan q és r számok, melyekre $a = b * q + r$, ahol $0 \leq r < |b|$. Ilyenkor azt mondjuk, hogy b megvan a-ban q-szor és maradék az r.

Euklideszi algoritmus

80	50	30	20	**10**	0
-	1	1	1	2	

(845,68) LNKO?

Euklideszi algoritmus

845	68	29	10	9	**1**	0
-	12	2	2	1	9	

Így a két szám relatív prím, azaz:$(845, 68) = 1$

Euklideszi algoritmus pszeudó kód

- Euklidesz(a, b, d)
- $d \leftarrow a$
- If($b \neq 0$)
- Then Euklidesz($b, a \ mod \ b, d$)
- Return (d)

Kibővített Euklideszi algoritmus

Az a és b két egész szám legnagyobb közös osztója $x, y \in Z$ számokkal kifejezhető a következő alakban:

$(a, b) = a * x + b * y$

Mindig!

$x_0 = 1 \; x_1 = 0$

$y_0 = 0 \; y_1 = 1$

Képlet:

$x_{i+1} = x_i * q_i + x_{i-1}$

$y_{i+1} = y_i * q_i + y_{i-1}$

$x = (-1)^n * x_n$

$y = (-1)^{n+1} * y_n$

Kibővített Euklideszi algoritmus 1 példa

k	0	1	2	-
r_k	280	3	1	0
q_k	-	93	3	
x_k	1	0	1	
y_k	0	1	93	

$(-1)^2$ és $(-1)^{2+1}$

1=280*1+3*-93

Kibővített Euklideszi algoritmus 2 példa

k	0	1	2	3	4	
r_k	544	119	68	51	17	0
q_k	-	4	1	1	3	
x_k	1	0	1	1	2	
y_k	0	1	4	5	9	

$(-1)^4$ és $(-1)^{4+1}$

17=544*2+119*-9

Kibővített Euklideszi algoritmus pszeudó kód

- KibővítettEuklidesz(a, b, d, x, y)
- $x_0 \leftarrow 1$, $x_1 \leftarrow 0$, $y_0 \leftarrow 0$, $y_1 \leftarrow 1$, $s \leftarrow 1$
- While ($b \neq 0$)
- $r \leftarrow a \ mod \ b$, $q \leftarrow a \ div \ b$
- $a \leftarrow b$, $b \leftarrow r$
- $x \leftarrow x_1$, $y \leftarrow y_1$
- $x_1 \leftarrow q * x_1 + x_0$, $y_1 \leftarrow q * y_1 + y_0$
- $x_0 \leftarrow x$, $y_0 \leftarrow y$
- $s \leftarrow -s$
- End While
- $x \leftarrow s * x_0$, $y \leftarrow -y_0$
- $(d, x, y) \leftarrow (a, x, y)$
- Return (d, x, y)

Kongruencia

Legyenek a és b egész számok és m pozitív egész. Aztmondjuk, hogy a **kongurens** b-vel modulo m, ha $m||a - b$.
Jelölés: $a \equiv b \pmod{m}$

- m modulusnak nevezzük.
- Két szám pontosan akkor kongruens modulo m, ha m-mel osztva ugyanazt a maradékot adják.
- ha nem ugyanazt a maradékot adják akkor inkongruensek

Példák: $13 \equiv 8 \pmod{5}$, $25 \equiv -10 \pmod{7}$, $25 \not\equiv 10 \pmod{7}$

Kongruencia tulajdonságai

- szimmetrikus:
  ha $a \equiv b \pmod m$ akkor $b \equiv a \pmod m$
- reflexív:
  $a \equiv a \pmod m$
- tranzítiv:
  ha $a \equiv b \pmod m$ és ha $b \equiv c \pmod m$ akkor ha $a \equiv c \pmod m$
  Példa: $18 \equiv 13 \pmod 5$ és ha $13 \equiv 8 \pmod 5$ akkor $18 \equiv 8 \pmod 5$

Maradékosztályok

Ha $a \in Z$, akkor az a-val kongruens (mod m) egész számok halmazát az a által reprezentált (mod m) maradékosztálynak nevezzük.
Jelölés $(a)_m$
Z_n olyan halmaz melynek elemei maradékosztályok
Z_6=$(0)_6, (1)_6, (2)_6, (3)_6, (4)_6, (5)_6,$

Maradékosztályok tulajdonságok

- $(a)_m + (b)_m = (a + b)_m$
- $(a)_m * (b)_m = (ab)_m$
- Példák:
  $(2)_6 + (5)_6 = (2 + 5)_6 = ?$
  $(3)_6 + (3)_6 = ?$
  $(4)_6 + (5)_6 = ?$
  $(2)_6 * (5)_6 = ?$
- Algebrai struktúrát alkotnak.

Köszönöm a figyelmet!