Seminar V. Cornaciu

19/04/2022

Seminar 10

Elemente de teoria numerelor aplicate în criptografie

↳ Teorema împărțirii cu rest, divizibilitate, numere prime.

• Fie $m, n \in \mathbb{Z}$, $n \neq 0$. Atunci există și sunt unice nr. $q, r \in \mathbb{Z}$ a.î.

$$\boxed{m = n \cdot q + r}, \quad 0 \leq r \leq |n| - 1$$

• Spunem că un număr n divide m $(n \mid m)$ dacă există un alt număr $q \in \mathbb{Z}$ a.î.:

$$\boxed{m = n \cdot q}$$

Ex. $2 \mid 4$

Proprietăți:

1) $n \mid n$

2) $n \mid m$ și $m \mid p \rightarrow n \mid p$

3) $n \mid m$ și $m \mid n \rightarrow n = \pm m$

4) $n \mid m \Rightarrow |n| \leq |m|$

• Un număr $\mathbb{Z}$ p se numește număr prim dacă $p \neq 1, -1, 0$ și nu are divizori proprii.

• Se numește cel mai mare divizor comun al numerelor $a, b \in \mathbb{Z}$, notăm cu cmmdc(a, b) sau (a, b), număr pozitiv d cu proprietățile

a) $d \mid a$, $d \mid b$

b) $c \mid a$, $c \mid b \Rightarrow c \mid d$

• Se numește cel mai mic multiplu comun lui $a, b \in \mathbb{Z}$ notat cu cmmmc(a, b) sau $[a, b]$, un număr pozitiv m cu proprietățile:

a) $a \mid m$, $b \mid m$

b) $a \mid n$, $b \mid n \Rightarrow m \mid n$

$$\boxed{a \cdot b = (a, b) \cdot [a, b]}$$

Exp. $a = 189$ $b = 154$

$189 = 3^3 \cdot 7$

$154 = 2 \cdot 7 \cdot 11$

$(189, 154) = 7$

$[189, 154] = 2 \cdot 3^3 \cdot 7 \cdot 11 = 4.158$

Algoritmul lui Euclid pentru cmmdc

$(\forall) a,b \in \mathbb{Z}$ a.î. $\exists!\ d=(a,b)$ și $\exists\ u,v \in \mathbb{Z}$ a.î.

$$d = a\cdot u + b\cdot v$$

Algoritm

$$a = b\cdot q_1 + r_1$$
$$\downarrow$$
$$b = r_1\cdot q_2 + r_2$$
$$\downarrow$$
$$r_1 = r_2\cdot q_3 + r_3$$
$$\vdots$$
$$r_{n-3} = r_{n-2}\cdot q_{n-1} + r_{n-1} = d$$
$$r_{n-2} = r_{n-1}\cdot q_n$$

Ex: Să se arate că dacă n este un număr natural impar, atunci există o corespondență biunivocă între divizorii lui n care sunt mai mari ca $\sqrt{n}$ și modurile de scriere ale lui n sub forma $n = u^2 - v^2$.

Sol:

$n = a\cdot b$, $a > \sqrt{n}$, n = impar, a,b = impare

$n = u^2 - v^2 = (u-v)(u+v)$

$\Rightarrow a\cdot b = (u-v)(u+v)$

$\rightarrow a = (u+v)$ $\quad b = (u-v)$ $\rightarrow$ $a + b = 2u \rightarrow u = \frac{a+b}{2}$

$a - b = +2v \rightarrow v = \frac{a-b}{2}$

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

Ex 2: Să se afle toate scrierile de forma u^2-v^2 ale lui 35 și 1575

I $n = 35 \rightarrow \underset{a}{7}\cdot\underset{b}{5}$

$\hookrightarrow 35 = \left(\frac{7+5}{2}\right)^2 - \left(\frac{7-5}{2}\right)^2 = 6^2 - 1^2$

II $n = 35 \rightarrow \underset{a}{35}\cdot\underset{b}{1}$

$\hookrightarrow 35 = \left(\frac{35+1}{2}\right)^2 - \left(\frac{35-1}{2}\right)^2 = 18^2 - 17^2$

$1575 = 5^2 \cdot 3^2 \cdot 7$

I $n = 1575 = 1575 \cdot 1$

$$1575 = \left(\frac{1575+1}{2}\right)^2 - \left(\frac{1575-1}{2}\right)^2 = 788^2 - 787^2$$

II $n = 1575 = 525 \cdot 3$

$$1575 = \left(\frac{525+3}{2}\right)^2 - \left(\frac{525-3}{2}\right)^2 = 264^2 - 261^2$$

III $n = 1575 = 315 \cdot 5$

$$1575 = \left(\frac{315+5}{2}\right)^2 - \left(\frac{315-5}{2}\right)^2 = 160^2 - 155^2$$

III $n = 1575 = 225 \cdot 7$

$$1575 = \left(\frac{225+7}{2}\right)^2 - \left(\frac{225-7}{2}\right)^2 = 116^2 - 109^2$$

III $n = 1575 = 175 \cdot 9$

$$1575 = \left(\frac{175+9}{2}\right)^2 - \left(\frac{175-9}{2}\right)^2 = 92^2 - 83^2$$

IV $n = 1575 = 105 \cdot 15$

$$1575 = \left(\frac{105+15}{2}\right)^2 - \left(\frac{105-15}{2}\right)^2 = 60^2 - 45^2$$

V $n = 1575 = 75 \cdot 21$

$$1575 = \left(\frac{75+21}{2}\right)^2 - \left(\frac{75-21}{2}\right)^2 = 48^2 - 27^2$$

VII $n = 1575 = 45 \cdot 35$

VI $n = 1575 = 63 \cdot 25$

$$1575 = \left(\frac{63+25}{2}\right)^2 - \left(\frac{63-25}{2}\right)^2 = 44^2 - 19^2$$

$$1575 = \left(\frac{45+35}{2}\right)^2 - \left(\frac{45-35}{2}\right)^2 = 40^2 - 5^2$$

Ex. Să se afle cel mai mare divizor comun

$a = 189$ $b = 154$ și să se scrie d sub forma

$d = a \cdot u + b \cdot v$, $u, v \in \mathbb{Z}$

$$\begin{cases} 189 = 154 \cdot 1 + 35 \\ 154 = 35 \cdot 4 + 14 \\ 35 = 14 \cdot 2 + 7 \rightarrow 7 = (189, 154) \\ 14 = 7 \cdot 2 + 0 \end{cases}$$

$7 = 35 - 14 \cdot 2 \rightarrow 35 - (154 - 35 \cdot 4) \cdot 2 = -154 \cdot 2 + 9 \cdot 35$

$= 154 \cdot (-2) + 9 \cdot (189 - 154 \cdot 1) = 154 \cdot (-11) + 9 \cdot 189 =$

$= \underset{u}{9} \cdot \underset{a}{189} - \underset{v}{11} \cdot \underset{b}{154}$ $u = 9$

$v = -11$

Ex Să se calculeze c.m.m.d.c. $n_1 = 63775075$

$n_2 = 48769175$

$63775075 = 48769175 \cdot 1 + 15005900$

$48769175 = 15005900 \cdot 3 + 3.751.475$

$15005900 = 3.751.475 \cdot 4 + 0$

$d = 3751475$

Grupuri, Inele, Corpuri

- $G \neq \emptyset$, $(G, \circ)$ grup
  1) asociativă $(x \circ y) \circ z = x \circ (y \circ z)$
  2) element neutru $\exists e \in G$ a.î. $\forall x \in G$ avem $(x \circ e) = (e \circ x) = x$
  3) elemente simetrizabile $\forall x \in G, \exists x' \in G$ a.î. $x \circ x' = x' \circ x = e$

Dacă am și

4) Comutativitate $x \circ y = y \circ x$ Grup comutativ

• $(A, +, \cdot)$ $A \neq 0$, $+, \cdot$ operatori interni

1) $(A,+)$ grup abelian
2) $(A,\cdot)$ grup monoid
3) „·" este distributivă față de adunare „+"

$$x \cdot (y+z) = (x+y)\cdot(x+z) \quad \forall\ x,y,z \in A$$

Noțiunea de congruență modulo n

$$x \equiv y \ (\text{modulo } n) \Leftrightarrow \boxed{n \mid x-y}$$

Exp $9 \equiv 4 \ (\text{mod } 5)$

$9-4=5 \ \vdots\ 5$

$\mathbb{Z}_n = \{0,1,2,3,\dots,n-1\}$

Exp $\mathbb{Z}_6 = \{0,\dots,6\}$

$\mathbb{Z}_7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$(\mathbb{Z}_n, +)$ grup comutativ

$\mathbb{Z}_7$:
$1^{-1} = 1$
$2^{-1} = 4$
$3^{-1} = 5$
$4^{-1} = 2$
$5^{-1} = 3$
$6^{-1} = 6$

$\mathbb{Z}_6$: $1^{-1} = 1$
$5^{-1} = 5$

$\mathbb{Z}_6$

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$(\mathbb{Z}_n, \cdot)$ monoid

$\Rightarrow (\mathbb{Z}_n, +, \cdot)$ inel clase de resturi mod n

$(\mathbb{Z}_p^*, +, \cdot)$ corp.
$\hookrightarrow$ n prim

$U(\mathbb{Z}_n)$ = elementele inversabile lui $\mathbb{Z}_n$ în raport cu $\cdot$

$= \{ a \in \mathbb{Z}_n \mid \exists a^{-1} \in \mathbb{Z}_n \}$

$= \{ a \in \mathbb{Z}_n \mid (a, n) = 1 \}$