Algebră 3/4 27.10.2017

Principiul includerii și excluderii

$A_1, A_2, \ldots, A_n$ mulțimi finite

Atunci $\left|\bigcup_{i\in I} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| +$

$+ \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| \ldots + (-1)^{n+1} |A_1 \cap A_2 \ldots \cap A_n|$

Dem

- inducție după n

Verificare $n=1$ $|A| = |A|$ evident

$n=2$ $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

$A_1 \cap A_2 = \{a_1, \ldots, a_k\}$

$A_1 \setminus A_2 = \{b_1, \ldots, b_t\}$

$A_2 \setminus A_1 = \{c_1, \ldots, c_s\}$

$t+k+s = |A_1 \cup A_2|$

$|A_1| + |A_2| - |A_1 \cap A_2| = (t+k) + (s+k) - \cancel{(t+s+k)}$

$= \cancel{k}\ t+s+k = |A_1 \cup A_2|$

- pp Adev pt n

dem pt $n+1$

$A_1, A_2, \ldots, A_n$ mulțimi finite

$\left|\bigcup_{j=1}^{n+1} A_j\right| = |X \cup A_{n+1}| \underset{\substack{\downarrow \\ \text{cazul } n=2}}{=} |X| + |A_{n+1}| - |X \cap A_{n+1}| \underset{\downarrow}{=}$

aplic ipoteza de inducție pt a calcula $|X|$

$X = A_1 \cup A_2 \ldots \cup A_n$

A_{n+1}

$\rightarrow = |A_{n+1}| + \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| + \dots$

$+ (-1)^{n+1} |A_1 \cap A_2 \dots \cap A_n|$

$A_{n+1} \cap X = A_{n+1} \cap (A_1 \cup A_2 \cup \dots \cup A_n) = (A_{n+1} \cap A_1) \cup ($

$(A_{n+1} \cap A_2) \cup \dots \cup (A_{n+1} \cap A_n)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$|A_{n+1} \cap X| = |A_{n+1} \cap A_1| + |A_{n+1} \cap A_2| + \dots + |A_{n+1} \cap$

ipoteza
ind

$\cap A_n| - |A_1 \cap A_2 \cap A_{n+1}| - |A_1 \cap A_3 \cap A_{n+1}| - \dots (-1)^{n+1} |A_1 \cap$

$\cap A_2 \dots \cap A_n \cap A_{n+1}|$

$(A_{n+1} \cap A_1) \cap (A_{n+1} \cap A_2) = A_1 \cap A_2 \cap A_{n+1}$

$(U(\mathbb{Z}_n), \cdot)$ grup comutativ cu $\varphi(n)$ elemente

$n \in \mathbb{N}, n \ge 2$

$a, b \in \mathbb{Z}$

$\bar{a} = \bar{b} \overset{def}{\Leftrightarrow} n \mid a - b$

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

$\bar{a} + \bar{b} = \overline{a+b}$

$a \in \mathbb{Z}_1, (a, n) = 1$ $\quad$ $\bar{a} \in U(\mathbb{Z}_n)$

$b \in \mathbb{Z}_1, (b, n) = 1$

$\bar{a} \cdot \bar{b} \overset{def}{=} \overline{a \cdot b}$

$\varphi(n) = |\{a \in \mathbb{Z} \mid 0 \le a \le n-1, (a, n) = 1\}|$

$\varphi(n) = n \cdot \prod_{\substack{p \text{ prim} \\ p \mid n}} (1 - \frac{1}{p})$

$n = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$ $p_1 < p_2 < \ldots < p_r$

p_j prim, $a_j \in \mathbb{N}^*$

$\forall j = \overline{1,r}$

$\varphi(n) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}$

Teorema lui Lagrange:

$(G, \cdot)$ grup comutativ finit

e - elem. neutru

$g \in G$

$|G|$

$\Rightarrow g = e$

Aplic Lagrange pentru $(G, \cdot) = (U(\mathbb{Z}_n), \cdot)$

$a \in \mathbb{Z}, (a, n) = 1 \Rightarrow \bar{a}^{|U(\mathbb{Z}_n)|} = \bar{1}$

Teoremă (Euler)

$$\left.\begin{array}{l} a \in \mathbb{Z} \ \ (a, n) = 1 \\ n \in \mathbb{N}, n \geq 2 \end{array}\right| \Rightarrow \bar{a}^{\varphi(n)} = \bar{1}$$

$n \mid a^{\varphi(n)} - 1$

Caz particular al teoremei lui Euler

n prim $\Rightarrow \varphi(n) = n - 1$ $\left.\begin{array}{l} a \in \mathbb{Z} \\ (a, n) = 1 \end{array}\right\} \Rightarrow \bar{a}^{n-1} = \bar{1}$

$n \mid a^{n-1} - 1$

n prim $r = 1$

$a_1 = 1$

$n = p_1$

$\varphi(n) = p_1 - p_1^{2} = p_1 - 1 = n - 1$

Mica teoremă a lui Fermat

Ex: p prim $\Rightarrow 7p + 3^p - 4$ nu este pătrat perfect

$x_2 = 14 + 9 - 4 = 19$ nu e pp

$x_3 = 21 + 27 - 4 = 44$ nu e pp

$x_5 = 35 + 243 - 4 = 274$ nu e pp

șapte

Dem

$p = 4k+1$

$\mathbb{Z}_4$ $\hat{7}p = \hat{7}\hat{p} + \hat{3}^{\hat{p}} - \hat{4}$ $\quad \hat{p} = \hat{1}$ $\quad \hat{3}^{p} = (\hat{-1})^{p} = \hat{-1} = \hat{3}$

$= \hat{7} + \hat{3} = \hat{2}$

$4t+2 = u^2$

Dacă $4t+2 = u^2 \Rightarrow u$ par

$u = 2v$

$4t+2 = 4v^2$

$\Rightarrow 4 \mid 2$

$\hat{2} = \hat{0}$ $\mathbb{Z}_4$ $\cancel{o}$

$\left.\begin{array}{l} p \text{ prim} \\ p \neq 2 \end{array}\right\} \Rightarrow \left\langle \begin{array}{l} p = 4k+1 \\ p = 4k+3 \end{array}\right.$

$p = 4k+3$, $k \in \mathbb{N}$, p prim

Pp. că $7p + 3^p - 4 = u^2$ $\quad u \in \mathbb{Z}$

$\boxed{\mathbb{Z}_p}$

$\hat{3} - \hat{4} = \overline{7p + 3^p - 4} = \hat{u}^2$

$p \nmid 3 \Rightarrow 3^{p-1} = \hat{1} \Rightarrow \hat{3}^p = \hat{3}$

Mica T. Fermat

$p \mid u^2 - 1$

$p \nmid u$

$\hat{u}^{p-1} = \hat{1}$

$\hat{-1} = (\hat{-1})^{\frac{p-1}{2}} = (\hat{u}^2)^{\frac{p-1}{2}} = \hat{u}^{p-1} = \hat{1}$

$\Rightarrow p \mid 2$

$p = 2$ $\cancel{o}$

$\frac{p-1}{2} = 2k+1$

$(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$

Algoritmul de criptare RSA
(Rivest, Shamir, Adleman)

1 CESAR

A B C D ... X Y Z
0 1 2 3 ... 23 24 25

ZARURILE AU FOST ARUNCATE
→ CDU...

$(n, e) \to$ publice

$n = p \cdot q$ p, q prime distincte „mari"

p, q secrete $\varphi(p \cdot q) = (p-1)(q-1)$

$e \in \mathbb{N}$ $(e, \varphi(n)) = 1$

„Alfabet" $26^k < n < 26^{k+1}$

26 - lungimea alfabetului

STEAUA ≠ CSB   o secvență de k simboluri se transformă într-una de k+1 simboluri

$\overline{a_{k-1}, a_{k-2} \dots a_1, a_0}$

$a_j \leftrightarrow n$

$P = a_{k-1} \cdot 26^{k-1} + a_{k-2} 26^{k-2} + \dots + a_1 \cdot 26 + a_0$

mesajul criptat este $\hat{P}^e = \hat{Q}$

$\mathbb{Z}_n$ $0 \le Q \le n-1$

$Q = b_k \cdot 26^k + \dots + b_1 \cdot 26 + b_0$

Ex

$n = 713$ $e = 89$ $26^2 = 676$

$26^3 > 713$

N U → 13 · 26 + 20 = 358
13 20

NU $\to \overline{358}^{89}$ $\qquad 713 = 27^2 - 4^2 = 23 \cdot 31$

$\mathbb{Z}_{23}$ $\quad 358 : 23 = 13 \cdot 15$

$\overline{13}^{22} = \overline{1}$

Mica t Fermat

$\overline{358}^{89} = \overline{13}^{89} = (\overline{13}^{22})^4 \cdot \overline{13} = \overline{13}$

$\mathbb{Z}_{31}$ $\quad \overline{358}^{89} = \overline{17}^{89} = \overline{17}^{29}$

$\overline{17} \cdot \overline{x} = \overline{17}^{30} = \overline{1} \mid \overline{2}$

$\overline{3}x = \overline{34}\, x = \overline{2} = \overline{33} \qquad x = \overline{11}$

$x = 23u + 13$

$x = 31v + 11$

$\mathbb{Z}_{23}$ $\quad \overline{31v + 11} = \overline{23u + 13} = \overline{13}$

$\overline{8v} = \overline{13 - 11} = \overline{2}$

$\overline{8v} = \overline{2} = \overline{24}$

$v = \overline{6}$

$= 713t + 31 \cdot 6 + 11 = 197$

NU $\to \overline{358}^{89} = \overline{197} = 26 \cdot 7 + 15 = 0 \cdot 26^2 + 7 \cdot 26 + 15$

NU $\to$ 0, 7, 15

A H P

Decriptare (cazul general

1) Găsesc p, q

2) $\overline{e} \cdot \overline{f} = \overline{1} \quad U(\mathbb{Z}_n)$

3) $\overline{a}^f \in \mathbb{Z}_n$