Teorie - Test 1 (FAI)

✓ 1) Teorema chineză a resturilor; (sisteme de ecuații)

✓ 2) Rezolvarea unei ecuații congruențiale;

✓ 3) Calcul de invers modulor multiplicativ;

✓ 4) Rezolvarea unei ecuații în $\mathbb{Z}n$;

calculi lucru

✓ 5) Euclid; (AEE)

✓ 6) Ecuații diofantică;

✓ 7) Discriminant, verificare dacă ecuațiile admit soluții în $\mathbb{Z}n$; (ecuații de grad II) < Δ, RCR

✓ 8) Simbolul Legendre; (criteriul lui Gauss)

✓ 9) Reziduu pătratic;

✓ 10) Simbolul Legendre (reguli de bază). - nr. prime

✓ 11) Simbolul Jacobi - nr. impare

(reducerea de la Jacobi la Legendre - indicat prin metoda cu reguli)

1. Teoria chineză a resturilor

Considerăm un sistem de ecuații

$$(S) = \begin{cases} x \equiv b_1 \bmod m_1 \\ \dots\dots\dots \\ x \equiv b_k \bmod m_k \end{cases}$$

$\boxed{\text{Condiție: } (m_1, m_2, \dots, m_k) = 1}$

Demonstrație + pași pe exemplu:

$$(S) = \begin{cases} x \equiv \overset{a}{2} \bmod \overset{b}{3} \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases} \Rightarrow \begin{cases} m_1 = 3 \\ m_2 = 5 \\ m_3 = 7 \end{cases}$$

Pas I: aflăm c_1, c_2, c_3;

Avem:
Pas I
$$\begin{cases} c_1 = m_2 \cdot m_3 \\ c_2 = m_1 \cdot m_3 \\ c_3 = m_2 \cdot m_3 \end{cases}$$

$\Pi m = m_1 \cdot \dots \cdot m_k$
$\Rightarrow$ fără $\boxed{m_n}$

$$\begin{cases} c_1 = 35 \\ c_2 = 21 \\ c_3 = 15 \end{cases}$$

Pas II: aflăm x_1, x_2, x_3.

Formal: $c_1 \cdot x \equiv a \bmod b$

ex: $35 x_1 \equiv 2 \boxed{\bmod 3} \Leftrightarrow (35 \bmod 3) x_1 = 2 \bmod 3$

$2 x_1 = 2 \bmod 3 \Rightarrow \boxed{x_1 = 1}$

ș.a.m.d.

$$\Rightarrow \begin{cases} x_1 = 1;\ x_2 = 3 \\ x_3 = 2 \end{cases}$$

Pas III: soluție finală $\Rightarrow (c_1 \cdot x_1 + c_2 \cdot x_2 + c_3 \cdot x_3) \% (m_1 \cdot m_2 \cdot m_3)$

3. Inversul modular / multiplicativ.

Formulare: inversul modular a lui $a \bmod m$.

Pas I: Rezolv ecuația $a \cdot x \equiv 1 \bmod m$.

Pas II: Verificăm dacă ~~soluția / ecuația are~~ ecuația are soluții: condiție $(a, m) = 1$.

Pas III: Aplicăm AEE;

Pas IV: La final vom avea $\alpha \cdot a + \beta \cdot m = (a, m)$

Inversul multiplicativ $= \alpha$

2+4. Rezolvarea ecuațiilor congruențiale în $\mathbb{Z}_m$.

Formal: $ax \equiv b \bmod m$

Condiții: $m \geq 1$; $a, b, m \in \mathbb{Z}$

Condiție importantă: (ec. este rezolvabilă dacă) $\{ (a, m) \mid b$;

Soluțiile le aflăm: $\left\{ \left(x_0 + i \frac{m}{(a, m)}\right) \bmod m \right.$

x_0 - soluție întreagă arbitrară;

1) Aflăm x_0 cu AEE;

2) $0 \leq i < (a, m)$

$, m_3) = x$

HINT: $ax \equiv b \bmod m \Rightarrow \exists y$ a.î. $ax - b = my$

$ax - my = b$

5. AEE- euclid : $(ax + my = b)$

Teorie : $V_k = (\alpha, \beta)$ a.î. $\alpha \cdot a + \beta \cdot b = (a, m)$

Condiție : $(a, m) = 1$

Exemplu : $\overset{D}{12}x + \overset{Î}{7}y = 3$
$(12, 7) = 1$ (A)
$\Rightarrow V_n = (\alpha, \beta)$ a.î. $\alpha \cdot 12 + \beta \cdot 7 = (12, 7) = 1$

Împărțiri

D Î R

$12 = 1 \cdot 7 + 5$

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

($R = 0 \Rightarrow$ ne oprim)

AEE

$V12 = (1, 0)$

$V7 = (0, 1)$

$V5 = V12 - V7 = (1, -1)$

$V2 = V7 - V5 = (-1, 2)$

$\boxed{V1 = V5 - 2 \cdot V2 = (3, -5)}$

ultimul obținut
a înlocuiește în
ecuație

$\Rightarrow \alpha \cdot 12 + \beta \cdot 7 = 1$

$3 \cdot 12 + (-5) \cdot 7 = 1$ (A)

!! obs $\Rightarrow$ la noi $12x + 7y = 3 \Rightarrow$

$12(3) + 7 \cdot (-5) = 1 / 3$

$12 \cdot 9 + 7 \cdot (-15) = 3$

$\Rightarrow \begin{cases} x = 9 \\ y = -15 \end{cases}$

6. Ecuația diofantică

Fie $ax+by=c$ (formal)

Condiții: $\exists$ sol. $\in \mathbb{Z} \Leftrightarrow (a,b) \mid c$

Pasul I: Algoritmul lui Euclid; $(a,b)=\alpha a+\beta b=d$

Pasul II: $c'=\frac{c}{(a,b)}$;

Pasul III: $x=\alpha\cdot c'$;

$y=\beta\cdot c'$;

ecuațiile de gradul II – opțiunea I

7. Discriminantul, verificare dacă ecuațiile admit soluții în $\mathbb{Z}_n$

Formal: Se dau două ecuații de gradul 2 și se verifică dacă admit soluții în $\mathbb{Z}_k$ și $\mathbb{Z}_l$ (k și $l \in \mathbb{Z}$)

$\Delta=(b^2-4ac)^{\frac{y^2}{}}$ mod p $(ax^2+bx+c=0)$ mod m

Condiții: $(a,m)=1$.

Soluții: $x_{1,2}=\frac{-b+\sqrt{\Delta}\ \%\ p}{2a}$

//nu facem împărțirea propriu-zisă, ci aflăm $2a^{-1}$;

1. $\Delta\equiv y^2$ mod p (două soluții)

2. $\Delta\equiv 0$ mod p

p de la $\mathbb{Z}_p$ (dat)

Cum aflăm inversul $2a^{-1}$?

Exemplu: $4^{-1} = ?$

$4x \equiv 1 \bmod 7$ (7 dat în problemă: $\mathbb{Z}/7$)

$x = 2$

ș.a.m.d

Ecuații de grad II - Oarecare II

Folosim TCR

Formal: $(ax^2 + bx + c = 0) \bmod m$

Condiție: $(a, m) = 1$

Condiție: dacă m poate fi descompus ca produs de factori primi $\Rightarrow$ obținem 2 ecuații

$$ax^2 + bx + c \equiv 0 \bmod m_1$$
$$ax^2 + bx + c \equiv 0 \bmod m_2$$
$$(m_1, m_2) = 1$$

Exemplu: Dacă știm soluțiile aflate cu Δ,

avem $\begin{cases} x_1 = 4 \\ x_2 = 5 \\ (\%7) \end{cases}$ $\quad x_1' = 1$, $x_2' = 2$ $(\%3)$ $\quad m = 21 \begin{cases} m_1 = 3 \\ m_2 = 7 \end{cases}$

Formăm sistemul:

$$(S) = \begin{cases} x \equiv x_1 \bmod 7 \\ x \equiv x_1' \bmod 3 \end{cases} \Leftrightarrow \begin{cases} x \equiv 4 \bmod 7 \\ x \equiv 1 \bmod 3 \end{cases} (1)$$

sau

$$\begin{cases} x \equiv 4 \bmod 7 \\ x \equiv 2 \bmod 3 \end{cases} (2)$$

Utilizăm TCR pt (1) sau (2) sau (3) sau (4)

// oricare.

sau

$$\begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 1 \bmod 3 \end{cases} (3)$$

Aflăm soluția;

sau

$$\begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 2 \bmod 3 \end{cases} (4)$$

8. Simbolul Legendre (Gauss)

Formal: calculați simbolul Legendre al lui $a \% p$, notat (a/p), utilizând criteriul lui Gauss.

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ dacă } p \mid a; \\ 1, \text{ dacă } p \nmid a \text{ și } a \text{ este reziduu p. } \% p; \\ -1, \text{ dacă } p \nmid a \text{ și } a \text{ nu este r. p } \% p; \end{cases}$$

Gauss: $\left(\frac{a}{p}\right) = (-1)^r$

card. mult. $= r = |\{i \in \{1, \dots, (p-1)/2\} \mid (i \cdot a) \% p > p/2\}|$

9. Reziduu pătratic $\% p$

1) Dacă am făcut Gauss $\begin{cases} 1 - r \cdot p \\ -1 \Rightarrow ! \, r \cdot p \end{cases}$;

2) Dacă aplicăm: $a \equiv x^2 \bmod p$

// $a - r \cdot p \Leftrightarrow$ poate fi scris ca $x^2 \bmod p$)

10. Simbolul Legendre - reguli de bază — q, p - nr. prime distincte!!

1. $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$;

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;

3. $\left(\frac{1}{p}\right) = 1$;

4. $\left(\frac{-1}{p}\right) = \begin{cases} 1, \text{ if } p \equiv 1 \% 4 \\ -1, \text{ if } p \equiv 3 \bmod 4 \end{cases}$

5. $\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ if } \equiv \pm 1 \% 8 \\ -1, \text{ if } p \equiv \pm 3 \bmod 8 \end{cases}$

R6: ℓ, p nr. prime distincte

6. $\left(\frac{\ell}{p}\right) = \begin{cases} \left(\frac{p}{\ell}\right), \text{ if } p \equiv 1 \% 4 \text{ or } \ell \equiv 1 \% 4 \\ -\left(\frac{p}{\ell}\right), \text{ if } p \equiv \ell \equiv 3 \% 4 \end{cases}$ / dacă nr sunt impare

11. Simbolul Jacobi

Caz I: Reducerea de la Jacobi la Legendre

$$\left(\frac{a}{n}\right)=\begin{cases}1, & \text{dacă } n=1\\ \left(\frac{a}{p_1}\right)^{c_1}\cdots\left(\frac{a}{p_k}\right)^{c_k}, & \text{altfel}\end{cases}$$

Condiții: $\begin{cases}\left(\frac{a}{n}\right)\neq 0\\ (a,n)=1\end{cases}$

Pas I: Descompunem n în factori primi.

Pas II: Aplicăm regulile lui Legendre.

Caz II: Aplicăm direct regulile lui Jacobi.

Obs: Regula 6 o aplicăm $\Leftrightarrow$ (a,n) - impare distincte!!

Reguli

1. $\left(\frac{a}{p}\right)=\left(\frac{a\,\%\,p}{p}\right)$;
2. $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\cdot\left(\frac{b}{n}\right)$;
3. $\left(\frac{1}{n}\right)=1$;
4. $\left(\frac{-1}{n}\right)=\begin{cases}1, & n\equiv 1\ \%\ 4\\ -1, & n\equiv 3\ \%\ 4\end{cases}$
5. $\left(\frac{2}{n}\right)=\begin{cases}1, & n\equiv \pm 1\ \%\ 8\\ -1, & n\equiv \pm 3\ \%\ 8\end{cases}$

$$6.\ \left(\frac{m}{n}\right)=\begin{cases}\left(\frac{n}{m}\right), & n\equiv 1\ \%\ 4 \ \|\ m\equiv 1\ \%\ 4\\ -\left(\frac{n}{m}\right), & n\equiv m\equiv 3\ \%\ 4\end{cases}$$

n, m nr. prime distincte >0