FAI

Materiale **Recapitulative**

Cateva elemente de teorie si exercitii rezolvate pentru materia Fundamente Algebrice ale Informaticii

Teoria Numerelor

Algoritmul Extins al lui Euclid

$Fie\ a, b > 0$

$r_{-1} = a;\ r_0 = b$

$r_{-1} = r_0 * q_1 + r_1$

$r_0 = r_1 * q_2 + r_2$

...

$r_{n-2} = r_{n-1} * q_n + r_n\ ,\ unde\ r_n\ este\ ultimul\ rest\ nenul$

$r_{n-1} = r_n * q_{n+1} + r_{n+1}\ ,\ unde\ r_{n+1}\ este\ nul$

$(a, b) = (r_{-1}, r_0) = \ldots = r_n$

Teorema: Numarul de impartiri ale calculului nu depasteste 5 * numarul de cifre al lui b

Ecuatii de tipul ax+by=c = Ecuatii liniare diofantice

Pentru a rezolva ecuatii de tipul: $ax + by = c$

Pasul 1: Calculam (a,b)

Pasul 2: Daca (a,b) nu divide c => se poate afirma ca ecuatia nu are solutie

Pasul 3: Daca (a,b) divide c atunci calculam d, unde d*(a,b)=c

Pasul 4: Folosind algoritmul extins al lui Euclid calculam (a,b) = α a + β b

Pasul 5: Solutia este reprezentata de: x = α d si y = β d

Exemplu de ecuatie rezolvata pas cu pas:

Pentru a = 27, b = 21 si c =12 avem ecuatia: 27x+21y=12

Pasul 1: Calculam (a,b)

(a,b) = (27,21) = 3

Pasul 2: Daca (a,b) nu divide c => se poate afirma ca ecuatia nu are solutie

3 divide 12 => ecuatia are solutie

Pasul 3: Daca (a,b) divide c atunci calculam d, unde d*(a,b)=c

Calculam d: d * 3 = 12 => d = $\frac{12}{3}$ = 4

Pasul 4: Folosind algoritmul extins al lui Euclid calculam (a,b) = α a + β b

Algoritmul lui Euclid	Algoritmul lui Euclid extins

27 = 21*1 + 6
21 = 6 * 3 + 3
6 = 3* 2 + 0
	V_{27} = (1,0) //intotdeauna V_a = (1,0)
	V_{21} = (0,1) // intotdeauna V_b =(0,1)
	V_{r1} = V_6 = V_{27} - V_{21} * 1 =(1 , 0) - (0, 1) =(1 , -1)
	V_{r2} = V_3 = V_{21} - 3* V_6 = (0, 1) - 3*(1, -1) = (-3,4), ultimul rest nenul

Avem: (a,b) = α a + β b $\Leftrightarrow$ 3 = α * 27 + β * 21 si cunoastem V_{r2} = (-3, 4). De aici se poate afirma ca α = -3 si β = 4

Pasul 5: Solutia este reprezentata de: x = α d si y = β d

x = -12 si y = 16

Calculul inversului modular

Z_m = clasa de resturi ale impartirii la m

$Z_m^* = Z_m \setminus \{0\}$

a $\in Z_m^*$ este inversabil ddaca (a,m) = 1

Pentru a calcula inversul unui numar a (cand acesta exista):

Pasul 1: Folosind algoritmul extins al lui Euclid determinam α si β a.i. a α + m β =(a,m)= 1

Pasul 2: Daca a>m atunci inversul lui a, notat a^{-1} = α mod m

Pasul 3: Daca a<m atunci inversul lui a, notat a^{-1} = β mod m

Exemplu: Z_6^* ={1, 2, 3, 4, 5 }. Pentru a=5 inversul va fi calculat astfel:

Pasul 1: Folosind algoritmul extins al lui Euclid determinam α si β a.i. a α + m β =(a,m)= 1

Algoritmul lui Euclid	Algoritmul extins al lui Euclid
6 = 5*1 + 1 5 = 5*1 + 0	V_6 = (1, 0) V_5 = (0, 1) $V_1 = V_6 - V_5$ =(1, -1)

α = 1 si β = -1

Pasul 2: Daca a>m atunci inversul lui a, notat a^{-1} = α mod m

a=5 si m=6 => a nu este mai mare decat b

Pasul 3: Daca a<m atunci inversul lui a, notat a^{-1} = β mod m

a=5 si m=6 => a<m => 5^{-1} = β mod m = -1 mod 6 = 5

Functia lui Euler

$\phi(m) = card\ Z_m^*$ unde $card\ Z_m^* \Leftrightarrow |Z_m^*|$

$\phi(m)$ = functia lui Euler

Proprietati:

1. $\phi(1) = 1$
2. $\phi(p) = p - 1 \, \forall p \, prim$
3. $\phi(a * b) = \phi(a) * \phi(b), \; \forall a, b, \; (a, b) = 1$
4. $\phi(p^e) = p^e - p^{e-1} \; \forall p \, prim, \; e \geq 1$
5. $\phi(n) = (p_1^{e_1} - p_1^{e_1 - 1}) * ... * (p_k^{e_k} - p_k^{e_k - 1})$ unde $n = p_1^{e_1} * ... * p_k^{e_k}$ este descompunerea in factori primi a lui n

Teorema: $a^{\phi(m)} = 1 \; mod \; m \; \forall a \; cu \; (a, m) = 1$

Ecuatii congruentiale ax ≡ b mod m

Pot fi transformate in ecuatii diofantice:

ax ≡ b mod m

ax - b ≡ 0 mod m

$\exists y \in Z \; a.i$ ax - b = ym

ax-my=b => Trebuie aflat x si y folosind aceeasi pasi de mai sus

Altfel, daca o ecuatie de acest fel are solutie (i.e. daca (a,m) divide b) solutiile sunt de forma:

$x_i = (x_0 + i \frac{m}{(a,m)}) \; mod \; m$ cu $0 \leq i < (a, m)$ si x_0 este o solutie particulara.

Exemplu: 6x ≡ 36 mod 15.

(6,15) = 3 iar 3 divide 36 => ecuatia are o solutie

36 mod 15 = 6 => $x_0 = \; solutie \; particulara \; = 1$

$x_1 = (1 + 1 \frac{15}{3}) \; mod \; 15$ = 6 mod 15

$x_2 = (1 + 2 \frac{15}{3}) \; mod \; 15$ = (1 + 2*5) mod 15 = 11 mod 15

Ecuatii congruentiale $x^n \equiv 1 \; mod \; p$

Ecuatia are (n, $\phi(m)$) solutii de forma $\alpha^i mod\ m$ unde α este radacina primitiva mod m si i este solutia ecuatiei $im \equiv 0\ mod\ \phi(m)$. Pentru ecuatiile $im \equiv 0\ mod\ \phi(m)$ se gasesc solutii de forma $i \in k * \frac{\phi(m)}{(n,\phi(m))}$, 0 ≤ k < (n, $\phi(m)$). Exista $\phi(\phi(m))$ radacini primitive mod m.

Un numar a este radacina primitiva mod n daca $ord_n(a) = \phi(n)$. $ord_n(a)$ = cel mai mic k pentru care $a^k \equiv 1$ (mod n)

Exemplu: $x^6 \equiv 1\ mod\ 38$

Solutiile sunt de forma : $\alpha^i mod\ m$ cu i ∈ $k\frac{\phi(m)}{(n,\phi(m))}$, 0 ≤ k < (n, $\phi(m)$) si α radacina primitiva mod 38

$\phi(38) = 18$

(6, $\phi(38)$) = (6,18) = 6 => i ∈ $k\frac{18}{6}$ =3k, 0 ≤ k < 6

Sunt $\phi(\phi(38))$ = 6 radacini primitive: {3, 5, 7, 11, 17, 23}

Teorema Chineza a resturilor

Consideram un sistem de forma:

$$x \equiv b_1 mod\ m_1$$

$$x \equiv b_2 mod\ m_2$$

...

$$x \equiv b_k mod\ m_k$$

Cu $m_1, \dots m_k$ coprime intre ele

Un astfel de sistem se rezolva prin urmatorii pasi:

Pasul 1: Calculam m= $m_1 * \dots * m_k$

Pasul 2: Calculam $c_i = \frac{m}{m_i}$

Pasul 3: Rezolvam ecuatiile $c_i\, x \equiv b_i\ mod\ m_i$ **cu solutii unice notate** x_i

Pasul 4: Calculam solutia finala: $x_0 = (c_1 * x_1 + \dots + c_k * m_k)\ mod\ m$

Exemplu: Pentru sistemul

$x \equiv 5\ mod\ 7$

$x \equiv 1 \ mod \ 2$

$x \equiv 6 \ mod \ 3$

Pasul 1: Calculam m= $m_1 * \ ... \ * m_k$

m = 7*2*3 =42

Pasul 2: Calculam $c_i = \frac{m}{m_i}$

$c_1 = \frac{42}{7} = 6 ; \ c_2 = \frac{42}{2} = 21 ; \ c_3 = \frac{42}{3} = 14$

Pasul 3: Rezolvam ecuatiile $c_i \ x \equiv b_i \ mod \ m_i$ **cu solutii unice notate** x_i

$c_1 \ x \equiv b_1 \ mod \ m_1 \Leftrightarrow 6 \ x \equiv 5 \ mod \ 7 \Leftrightarrow x_1 = 2$

$c_2 \ x \equiv b_2 \ mod \ m_2 \Leftrightarrow 21 \ x \equiv 1 \ mod \ 2 \Leftrightarrow x_1 = 1$

$c_3 \ x \equiv b_3 \ mod \ m_3 \Leftrightarrow 14 \ x \equiv 6 \ mod \ 3 \Leftrightarrow x_3 = 0$

Pasul 4: Calculam solutia finala: $x_0 = (c_1 * x_1 + ... + c_k * m_k) \ mod \ m$

$x_0 = (c_1 * x_1 + ... + c_k * m_k) \ mod \ m$ = 6*2 + 21*1 + 14*0 = 33

Consecinta: ax = b mod p*q poate fi scrisa ca sistemul:

ax = b mod p

ax = b mod q

Din moment ce ambele ecuatii au o solutie unica si conduc la o solutie finala unica => ecuatia initiala are solutie unica

Teorema: Fie f(x) polinomiala cu $m_1, \ ... \ m_k$ coeficienti coprimi. O solutie pentru f(x)=0 mod $m_1 * \ ... \ * m_k$ exista daca si numai daca exista cate o solutie pentru orice ecuatie f(x) = 0 mod m_i

Simbolul Legendre

Pentru a $\in Z$, p>2, p = un numar prim

Simbolul Legendre notat:

$(\frac{a}{p})$ = 0 daca p divide a;

1 daca p nu divide a si a rest patratic mod p

-1 daca p nu divide a si a nu este rest patratic mod p

a = rest patratic mod p ⇔ ecuatia $x^2 \equiv a \ mod \ p$ are solutie

Proprietati:

1. $(\frac{a}{p}) = (\frac{b}{p})$ daca $a \equiv b \ mod \ p$
2. $(\frac{a}{p}) = (\frac{a \ mod \ p}{p})$
3. $(\frac{a*b}{p}) = (\frac{a}{p})*(\frac{b}{p})$, a,b prime
4. $(\frac{a}{p}) = a^{\frac{p-1}{2}} mod \ p$
5. $(\frac{1}{p}) = 1$
6. $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}, \ p, q \ prime$

Exemplu: $(\frac{201}{17}) = (\frac{201 \ mod \ 17}{17}) = (\frac{14}{17}) = (\frac{2}{17})(\frac{7}{17})$ = 1 * (-1) = -1

Simbolul Jacobi

Pentru a $\in Z$ si n $\in$ N

Simbolul Jacobi notat:

$(\frac{a}{n})$ = 1, n=1

$(\frac{a}{p_1})^{e_1} * ... * (\frac{a}{p_k})^{e_k}$ unde n= $p_1^{e_1} * ... * p_k^{e_k}$, altfel

Exemplu:

$(\frac{5}{81}) = (\frac{5}{3})^4 = (-1)^4 = 1$