Consultatie sesiune 1

Friday, June 4, 2021 5:53 PM

meinsta Today at 17:37
Teoria numerelor: (edited)
- Teorema impartirii cu rest (0<=r< |b|)
- Algoritmul lui Euclid
- algoritmul extins al lui Euclid
- ecuatii diofantice liniare (ax +by = c) (edited)
exemple de exercitii:
- de calculat cmmdc-ul a doua numere folosind Alg. lui Euclid
- de calculat solutii pentru o ecuatie diofantica folosind alg. extins al lui Euclid
- de calculat combinatia liniara a doua numere folosind alg. extins al lui Euclid
alfa*a* + *beta*b = cmmdc(a,b)
- de stiut cum folosim alg. lui Euclid pentru numere negative
----

meinsta Today at 17:44
- Congruente
- ecuatii congruentiale (ax = b mod m)
de stiut cum gasesc o solutie x0
de stiut cum calculez celelalte solutii pornind de la solutia x0
numarul total de solutii cmmdc(a,m)

Teorema chinezeasca a resturilor (CRT/TCR)
de stiut cum se modifica fiecare congruenta
x=b1 mod m1 ------> c1*x1 = b1 mod m1

meinsta Today at 17:47
de stiut cum calculam x1
de stiut cum calculam x-ul final modulo m, unde m = m1*m2*... *mk
solutia este unica modulo m

meinsta Today at 17:47
de stiut cum calculam x1
de stiut cum calculam x-ul final modulo m, unde m = m1*m2*... *mk
solutia este unica modulo m

- cum calculam inversul modular (utilizand alg. extins al lui Euclid)
----

meinsta Today at 17:49
Functia lui Euler:
fi (m) --- numarul de elemente co-prime cu m
fi (m) = |Zm/ *numarul de elemente din Zm*\ (edited)
----
la TCR de stiut cum transformam un sistem in care modulii nu sunt co-primi intr-un sistem in care modulii sunt co-primi (deci in care sa putem aplica si TCR)
-----

meinsta Today at 17:52
Reziduuri patratice
- simbolul Legendre (pentru moduli primi)
- simbolul Jacobi (pentru moduli compusi)
----
ecuatia ax^2 + bx + c = 0 mod p
are 2 radacini in Zp daca delta = y^2 mod p, ... 1 rad cand delta = 0 , 0 radacini altfel (edited)
- ecuatia x^2 = 1 mod p

meinsta Today at 17:56

Ordine de marime
- omega
- teta

meinsta Today at 17:56

Ordine de marime
- omega
- teta
- O mare si o mic

Coduri
- definitia codului

meinsta Today at 17:57
- ce inseamna C^k
- algoritmul Sardinas-Patterson
care ne spune daca o anumita multime este cod sau nu
cum se formeaza multimea C1
cum se formeaza de la C2 in colo
cum stabilim outputul: cand e cod, cand nu e cod

meinsta Today at 17:59
- codificarea Huffman clasic
- codificarea Huffma adaptiv
cum se calculeaza lungimea medie a codificarii
- cum se face decodificarea la Huffman clasic si la Huffman adaptiv (edited)

----

meinsta Today at 18:01
Grupuri
cine este Zm
cine este Zm*
cate elemente are Zm respectiv Zm*

ordinul unui element intr-un grup
- cum il aflam
- proprietatile ordinului unui element intr-un grup
- cum aflam un element de ordin d din grupul Zm*
radacini primitive
- cum aflam o radacina

meinsta Today at 18:06
- cum le aflam pe celelalte pornind de la prima (folosind proprietatea 6 de la ordinul unui element) (edited)
ecuatia x^n = 1 mod m
- cand putem calcula solutii
- cum calculam solutiile folosind o radacina primitiva
- numarul total de solutii (edited)
ecuatia x^n = -1 mod p, unde p numar prim impar

meinsta Today at 18:15
(aceeasi discutie ca mai sus)
Corpuri finite
- adunarea si inmultirea in GF(2^8)
la inmultire calculele se fac modulo un polinom ireductibil de grad 8 (edited)
Si cam atat. 😍

antohir Today at 18:21
Mulțumim mult! Trimit acum și colegilor

meinsta Today at 18:23
O trecere in revista a ceea ce am facut la seminar si avem de pregatit pentru examen 🙂

Teorema împărțirii cu rest: $\forall a,b\in\mathbb{Z},\ b\neq 0,\ \exists!\ q,r;\quad a=b\cdot q+r$

$a:b=q$ rest r

cmmdc $(a_1,a_2)=(a_2, a_1 \bmod a_2)=(a_3, a_2 \bmod a_3)\ \dots = (\text{rest}', 0)$ $\quad 0\le r<|b|$

$a_1>a_2$ $\quad a_1:a_2\to$ restul $=a_3$ $\quad r_m \swarrow$ cmmdc(a_1,a_2)

Algoritmul lui Euclid

$\boxed{(a,b)=r_m}$ $a=r_{-1}$, $b=r_0$

$r_{-1}=r_0\cdot q_1+r_1$

$r_0=r_1\cdot q_2+r_2$

$\vdots$

$r_{m-2}=r_{m-1}\, q_m+\boxed{r_m}$

$r_{m-1}=r_m\cdot q_{m+1}+0$

ex. $a=24,\ b=7$

$24=7\cdot 3+3$

$7=3\cdot 2+\boxed{1}$

$3=1\cdot 3+0$

$V_{(a,b)}=\boxed{V_1}=(\alpha,\beta)$

Algoritmul Extins al lui Euclid

$V_{24}=(1,0)$ $\quad V_7=(0,1)$ $\quad \alpha\cdot a+\beta\cdot b=x$ $\quad V_x=(\alpha',\beta')$

$V_3=V_{24}-3V_7$ $\quad V_3=(1,0)-3\cdot(0,1)=(1-3\cdot 0,\ 0-3\cdot 1)=(1,\ -3)$

$V_1=V_7-2V_3$ $\quad V_1=(0,1)-2\cdot(1,-3)=(-2,7)$

$\alpha\quad\beta$

$\alpha=-2;\ \beta=7$

Vf. $(-2)\cdot 24+7\cdot 7=1=(a,b)$ ✓

Ecuatii liniare diofantice

$ax+by=c$

Ecuatii liniare diofantice

$$ax+by=c$$

$\boxed{!}$ $\exists$ solutie in $\mathbb{Z} \iff (a,b) \mid c$ $\rightarrow$ Algoritmul de calcul pt x si y:

① Alg. Ext. Euclid: $(a,b) = \alpha \cdot a + \beta \cdot b$

② $\boxed{x = \alpha \cdot \frac{c}{(a,b)} \; ; \quad y = \beta \cdot \frac{c}{(a,b)}}$

$1 \mid x \Rightarrow \exists \alpha \in \mathbb{Z},\ x = 1 \cdot \overset{\alpha}{\boxed{x}}$

ex 1 $24x + 7y = 8$

Vf. $24 \cdot (-16) + 7 \cdot 56 \overset{?}{=} 8$ ✓

$x = \alpha \cdot \frac{c}{(a,b)} = (-2) \cdot \frac{8}{1} = -16$

$y = \beta \cdot \frac{c}{(a,b)} = 7 \cdot \frac{8}{1} = 56$

$x = -16$

$y = 56$

ex 2 $-88x + 14y = 8$

$V_a = V_{-88} = (1,0) \qquad V_{14} = (0,1)$

$-88 = 14 \cdot (-7) + 10$ $\qquad V_{10} = V_{-88} - (-7) \cdot V_{14} = (1,0) - (-7)\cdot(0,1) = (1,7)$

$14 = 10 \cdot 1 + 4$ $\qquad V_4 = V_{14} - 1 \cdot V_{10} = (0,1) - 1 \cdot (1,7) = (-1,-6)$

$10 = 4 \cdot 2 + \boxed{2}$ $\qquad \boxed{V_2} = V_{10} - 2 \cdot V_4 = (1,7) - 2(-1,-6) = (\underset{\alpha}{3}, \underset{\beta}{19})$

$4 = 2 \cdot 2 + 0$ $\qquad$ Vf: $3 \cdot (-88) + 19 \cdot 14 = 2$ ✓

$x = \alpha \cdot \frac{c}{(a,b)} = 3 \cdot 4 = 12$

$y = \beta \cdot c/(a,b) = 19 \cdot 4 = 76$

Vf: $(-88) \cdot 12 + 14 \cdot 76 = 8$ ✓

$-88 \cdot 12$: 176, 88, -1056

$76 \cdot 14$: 304, 76, 1064

$1064 - 1056 = 8$

$0 \le r < |b| \qquad V_{35} = (1,0) \qquad V_{-13} = (0,1)$

a) $35 = -13 \cdot (-2) + 9$ $\qquad V_9 = V_{35} - (-2) \cdot V_{-13} = (1,0) - (-2)\cdot(0,1) = (1,2)$

$-13 = 9 \cdot (-2) + 5$ $\qquad V_5 = V_{-13} - (-2) \cdot V_9 = (0,1) - (-2)\cdot(1,2) = (2,5)$

$9 = 5 \cdot 1 + 4$ $\qquad V_4 = V_9 - 1 \cdot V_5 = (1,2) - (2,5) = (-1,-3)$

$5 = 4 \cdot 1 + \boxed{1}$ $\qquad V_1 = V_5 - 1 \cdot V_4 = (2,5) - (-1,-3) = (\underset{\alpha}{3}, \underset{\beta}{8})$

$4 = 1 \cdot 4 + 0$ $\qquad$ Vf. $3 \cdot 35 + 8 \cdot (-13) = 1$ ✓

$a \equiv_m b \overset{def}{\Leftrightarrow} m \mid a-b \overset{def}{\Leftrightarrow} \exists y \in \mathbb{Z},\ a-b = m\cdot y$ $\quad \mathbb{Z}_6^* = \{\cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5\}$ $\quad |\mathbb{Z}_6^*| = \phi(6) = \phi(2)\phi(3) = 1\cdot 2 = 2$ $\quad \mathbb{Z}_7^* = \{\cancel{0}, 1, 2, \dots, 6\}$

$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ $\quad \mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$ $\quad a \in \mathbb{Z}_m^* \Rightarrow \exists! a', \ a\cdot a' \equiv 1 \bmod m$

Inversul modulo: $a\cdot x \equiv 1 \bmod m \Leftrightarrow m \mid ax-1 \Rightarrow \exists y \in \mathbb{Z},\ ax - 1 = my \Leftrightarrow \boxed{ax - my = 1}$ $\exists$ sol în $\mathbb{Z} \Leftrightarrow (a, m) \mid 1$

$4 \cdot \boxed{4} \equiv 1 \bmod 5$ $\quad \boxed{} \cdot x \equiv \boxed{} \bmod m \ / \cdot x^{-1}$ $\quad \boxed{ax + by = c}$ Ec. diofantica

$|\mathbb{Z}_m^*|$ $\quad 2\cdot \boxed{3} \equiv 1 \bmod 6$ $\quad x\cdot x^{-1} \equiv 1 \bmod m$

I Alg. Euclid $\to (a,b)$

Funcția lui Euler $\phi(m) = |\mathbb{Z}_m^*|$

II $(a,b) \mid c \Rightarrow \exists$ sol $\mathbb{Z}$

$\phi(1) = 1$ $\quad \phi(6) = \phi(2)\cdot\phi(3) = 1\cdot 2 = 2.$

III comp. sol. în $\mathbb{Z}$

$\phi(p) = p - 1, \ \forall p$ prim $\quad \phi(36) = \phi(2^2)\,\phi(3^2) = \phi(2^2 - 2^1)\cdot\phi(3^2 - 3^1) = 2\cdot 6 = 12$

Ext. Eucl. $d = (a,b) = \alpha\, a + \beta\, b$ $\quad \forall_1 = (x, \beta)$

$\phi(a\cdot b) = \phi(a)\cdot\phi(b), \ (a,b) = 1$ $\quad \boxed{x_0} = \alpha \cdot \frac{c}{(a,b)}$

$\phi(p^e) = p^e - p^{e-1}$

$\phi(m) = \phi(p_1^{e_1} \cdot \dots \cdot p_k^{e_k}) = (p_1^{e_1} - p_1^{e_1 - 1}) \cdot \dots \cdot (p_k^{e_k} - p_k^{e_k - 1})$ $\quad p_i \neq p_j \ \forall i, j$

Thm. Euler $\quad m \geq 1, \ (a, m) = 1$ atunci $a^{\phi(m)} \equiv 1 \bmod m$

Corolar Fermat $\quad p$ prim, $p \nmid a$ $\quad a^{\phi(p)} \equiv 1 \bmod p$

Ecuații congruențiale $\quad \overset{def}{\Rightarrow} m \mid ax - b \Rightarrow \exists y \in \mathbb{Z},\ ax - b = my$

$\boxed{ax \equiv b \bmod m} \to ax - my = b$, $\exists$ sol în $\mathbb{Z} \Leftrightarrow (a, m) \mid b \to x_0$

$\exists \#(a, m)$ soluții de forma $\left(x_0 + i \cdot \frac{m}{(a,m)}\right) \bmod m$

*

$(4, 5, 16) = 1 \quad (4, 16) = 4 \neq 1$

CRT $\quad k \geq 1, \ m_1, \dots, m_k \geq 1, \ m = m_1 \cdot \dots \cdot m_k$, co-prime 2-2; $\forall b_1, \dots, b_k \in \mathbb{Z}$

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

$c_i = \frac{m}{m_i}$; $\quad c_i x_i \equiv b_i \bmod m_i$ $\quad$ Obs. $(c_i, m_i) = 1 \Rightarrow \exists!$ sol.

$$x = \left(\sum_{i=1}^{k} c_i x_i\right) \bmod m$$

(S) admite sol. unică în $\mathbb{Z}_m$

$c_i x_i - m_i y = b_i$ $\quad \#$ sol?

$\Rightarrow (c_i, m_i) = 1 \quad 1 \mid b_i \Rightarrow \exists!$ în $\mathbb{Z}_{m_i}$

Exerciții:

Ex3 $\quad$ Ec. congr. $\quad$ Toate sol. din $\mathbb{Z}_m$

a) $18x \equiv 12 \bmod 42$ $\quad \left(x_0 + i \cdot \frac{m}{(a, m)}\right) \bmod m$ $\quad i = \overline{1,5}$ $\quad 18x - 42y = 12 \Rightarrow (18, 42) = 6$

b) $14x \equiv 6 \bmod 18$ $\quad i = 1$ $\quad 14x - 18y = 6 \Rightarrow (14, 18) = 2$

Ex3 $\quad$ Ecuații congruențiale:

i) $18x \equiv 12 \bmod 42 \Rightarrow 42 \mid 18x - 12 \Rightarrow \exists y \in \mathbb{Z},\ 18x - 12 = 42y \Rightarrow$

Ex3 Ecuații congruențiale:

i) $18x \equiv 12 \mod 42 \Rightarrow 42 \mid 18x-12 \Rightarrow \exists y \in \mathbb{Z},\ 18x-12=42y \Rightarrow$

$18x - 42y = 12$

(?1) $\exists$ sol în $\mathbb{Z}$? $(18,42) \mid 12$

(?2) # sol în $\mathbb{Z}_m$ $=(18,42)$

Sol în $\mathbb{Z}_{42}$ (6 sol.)

$18 = 42\cdot 0 + 18$ $\qquad V_{18}=(1,0) \quad V_{42}=(0,1)$

$42 = 18\cdot 2 + \boxed{6}$ $\qquad V_6 = V_{42} - 2\cdot V_{18} = (0,1) - 2\cdot(1,0) = (\underset{\alpha}{-2},\underset{\beta}{1})$

$18 = 6\cdot 3 + 0$ $\qquad$ Vf $\alpha\cdot a + \beta\cdot b = (a,b)$

$(-2)\cdot 18 + 1\cdot 42 = 6$ ✓

$x_0 = 38$;

$x_1 = 3 \mod 42 = 3$

$x_2 = -4 + 2\cdot 7 = 10$

$x_3 = -4 + 3\cdot 7 = 17$

$x_4 = 24$; $x_5 = 31$

$x_0 = \alpha \cdot \frac{c}{(a,b)} = (-2)\cdot\frac{12}{6} = \boxed{-4} \mod m$ $\qquad x_i = \left(x_0 + i\cdot\frac{m}{(a,m)}\right) \mod m = -4 + 1\cdot\frac{42}{6} = -4+7 = 3$

$x_0 = 42 - 4 = 38$

$x \in \{3, 10, 17, 24, 31, 38\}$

Ex2 Calc. inversul modular al lui a modulo m

a) $a=18,\ m=23$ $\qquad ax \equiv 1 \mod m \overset{def}{\Rightarrow} m \mid ax-1 \overset{def}{\Rightarrow} \exists y \in \mathbb{Z},\ ax-1 = my \Leftrightarrow \boxed{ax - my = 1}$

b) $a=35,\ m=46$ $\qquad ax+by=c$

$V_d = V_{(a,b)} = (\alpha,\beta) = (-21,-16)$ $\qquad \square\cdot a + \square\cdot b = V_{35}$

b) $\overset{a}{35}x - \overset{b}{46}y = \overset{c}{1}$ $\qquad V_{35}=(1,0) \quad V_{-46}=(0,1)$

$35 = (-46)\cdot 0 + 35$

$-46 = 35\cdot(-2) + 24$ $\qquad V_{24} = V_{-46} - (-2)\cdot V_{35} = (0,1) - (-2)(1,0) = (0,1) - (-2,0) = (2,1)$

$35 = 24\cdot 1 + 11$ $\qquad V_{11} = V_{35} - 1\cdot V_{24} = (1,0) - (2,1) = (-1,-1)$

$24 = 11\cdot 2 + 2$ $\qquad V_2 = V_{24} - 2\cdot V_{11} = (2,1) - 2\cdot(-1,-1) = (2,1) - (-2,-2) = (4,3)$

$11 = 2\cdot 5 + \boxed{1}$ $\qquad V_1 = V_{11} - 5\cdot V_2 = (-1,-1) - 5\cdot(4,3) = (\underset{\alpha}{-21},\underset{\beta}{-16})$

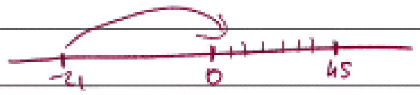
$2 = 1\cdot 2 + 0$ $\qquad$ Vf. $\alpha\cdot 35 + \beta\cdot(-46) = 1$

$0 \le r < |b|$ $\qquad (-21)\cdot 35 + (-16)\cdot(-46) = 1$

$x = \alpha\cdot\frac{c}{(a,b)} = (-21)\cdot\frac{1}{1} = -21 \Rightarrow \boxed{x} = -21 \mod 46 = \boxed{25}$

$\mathbb{Z}_{46} = \{0, 1, \dots, 45\}$

Inversul modular al lui $\boxed{a = \boxed{\alpha \mod m} = a^{-1}}$



TCR Moduli coprimi

$ax \equiv c \mod m$

Ex4 (S) $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 1 \mod 7 \end{cases}$

$c_1 = 5\cdot 7$ $\qquad 35x_1 \equiv 2 \mod 3$ $\qquad x_1 =$

$c_2 = \frac{105}{5} = 3\cdot 7$ $\qquad 21x_2 \equiv 3 \mod 5$ $\qquad x_2 =$

$c_3 = 3\cdot 5$ $\qquad 15x_3 \equiv 1 \mod 7$ $\qquad x_3 =$

CRT $\rightarrow$ Vf: $(3,5)=1$ ✓ $(5,7)=1$ ✓, $(3,7)=1$ ✓

$\Rightarrow \exists!$ sol. în $\mathbb{Z}_{3\cdot 5\cdot 7}$ $\qquad m = 105$

$$ax \equiv c \bmod m$$

Ex 4

$$(S)\ \begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 1 \bmod 7 \end{cases}$$

$c_1 = 5\cdot 7$	$35x_1 \equiv 2 \bmod 3$	$x_1 =$
$c_2 = \frac{105}{5} = 3\cdot 7$	$21x_2 \equiv 3 \bmod 5$	$x_2 =$
$c_3 = 3\cdot 5$	$15x_3 \equiv 1 \bmod 7$	$x_3 =$

CRT $\to$ Vf: $(3,5)=1$ ✓, $(5,7)=1$ ✓, $(3,7)=1$ ✓

$\Rightarrow \exists!$ sol. in $\mathbb{Z}_{3\cdot 5\cdot 7}$ $\quad m = 105$

$$\underline{x} = (c_1 x_1 + c_2 \cdot x_2 + c_3 \cdot x_3) \bmod 105$$

Vf. (S)

TCR Moduli necoprimi

$$\begin{cases} x \equiv 9 \bmod 12 \\ x \equiv 3 \bmod 18 \\ x \equiv 1 \bmod 10 \end{cases} \quad \begin{matrix} 12 = 2^2 \cdot 3 \\ 18 = 2 \cdot 3^2 \\ 10 = 2 \cdot 5 \end{matrix} \quad \to \quad \begin{cases} x \equiv 1 \bmod 4 \\ x \equiv 3 \bmod 9 \\ x \equiv 1 \bmod 5 \end{cases}$$

$(4,9) = (9,5) = (5,4) = 1$ ✓ TCR