Subiecte abordate azi: Alg. lui Euclid, Ecuatii Diofantice, TCR

Algoritmul lui Euclid

Avand a, b cu a>b avem urmatorul algoritm de aflare al CMMDC-ului:

Exemplu: a = 46, b = 12

12 = 46 * 0 + 12 * 1

46 = 12 * 3 + 10

12 = 10 * 1 + 2 → CMMDC

10 = 2 * 5 + 0

CMMDC-ul lui a si b = ultimul rest nenul => 2

Algoritmul lui Euclid extins

Avand a, b cu a>b avem urmatorul algoritm: vom afla CMMDC-ul conform algoritmului de mai sus

Exemplu: a = 46, b = 12 V12 = (0, 1)

12 = 46 * 0 + 12 * 1 V46 = (1,0)

46 = 12 * 3 + 10 → V10 = V46 - 3* V12 = (1,0) - (0, 3) = (1, -3)

12 = 10 * 1 + 2 → V2 = V12 - V10 = (0,1) - (1, -3) = (-1, 4) => alfa = -1, beta = 4

10 = 2 * 5 + 0

Dupa aflarea algoritmului avem urmatoarea ecuatie: **a * alfa + b * beta = CMMDC**

Exemplu: 46 * alfa + 12 * beta = 2

Scriem in felul urmator : V12 = (0, 1) 46* alfa + 12 * beta = 12 => V12 = (0, 1)

V46 = (1, 0) 46* alfa + 12 * beta = 46 => V46 = (1, 0)

Pentru fiecare rest al operatiilor din algoritmul lui Euclid, calculam V.

V-ul corespunzator CMMDC ului va contine valorile parametrilor alfa si beta.

Verificare: 46* (-1) + 4 * 12 = 2 "Adevarat"

Ecuatii diofantice: ax + by = c

Pasul 1: Verificam daca ecuatia are solutii: (a,b)/c - verificam daca CMMDC dintre a si b, divide c

Pasul 2: Daca ecuatia are solutii, solutiile o sa fie de forma: x= (alfa * c)/CMMDC(a,b)

y = (beta * c)/CMMDC(a,b)

Exemplu: 4x + 11y = 17

a= 4, b= 11, c=17

Pasul 1: Verificam ca ecuatia are solutii/nu

Calculam CMMDC(a, b) adica CMMDC(4, 11) folosind alg. lui Euclid

4 = 11* 0 + 4*1

11 = 4*2 + 3

4 = 3*1 + 1

3 = 1*3 + 0

Verificam ca 1/17 "Adevarat" => Ecuatia are solutii

Pasul 2: Calculam alfa si beta folosind algortimul lui Euclid extins : 4 * alfa + 11 * beta = 1

V4 = (1, 0)

V11 = (0,1)

V3 = V11 - V4*2 = (0,1) - (2, 0) = (-2, 1)

V1 = V4 - V3* 1 = (1, 0) - (-2, 1) = (3,-1) => alfa = 3, beta = -1

x= (alfa * c)/CMMDC(a, b) => x = (3 * 17)/ 1 = 51 => x= 51

y = (beta * c)/CMMDC(a,b) => y = (-1 * 17)/1 = -17 => y = -17

Verificare: 4 * 51 + 11 * (-17) = 17

4*51 - 11*17 = 17

204 - 187 = 17

17 = 17 "Adevarat"

Ecuatii congruentiale: ecuatii de forma: *ax = b mod c*

Pasul 1: Verificam daca ecuatia are solutii: (a, c) / b

Pasul 2: Daca ecuatia are solutii calculam:

x0 = (alfa* b)/ CMMDC(a,c)

xi = [x0 + i* c/CMMDC(a,c)] mod c

Ecuatia o sa aibe CMMDC solutii

a = b mod m=> m\(a-b) <=> Exista un c apartine lui Z astfel incat (a-b) = m*c

Exemplu: x = 3 mod 5

a = 1, b = 3, c = 5

Pasul 1: Verificam existenta solutiilor: (1, 5)/3 => 1/3 "Adevarat" => ecuatia are solutii

a=1 c =5

1 = 5*0 + 1

5 = 1* 5 + 0

V1 = (1, 0) => alfa = 1, beta = 0

Pasul 2: Calculam solutia arbitrara x0 = (1* 3)/1 mod c = 3 mod 5 = 3

Ecuatia are CMMDC solutii <=> ecuatia are o solutie = > solutia ecuatiei este x= 3

Exemplul 2: **18x = 12 mod 42**

a = 18, b= 12, c= 42

Pasul 1: Verificam daca ecuatia are solutii: (a, c)/b => 6/12 "A" => ecuatia are 6 solutii

Pasul 2: Calculam alfa si beta

18 * alfa + 42 * beta = 6

V18 = (1,0)

V42 = (0,1)

V6 = V42 - 2*V18 = (0,1) - 2 * (1,0) = (-2, 1) => alfa = -2

Calculam solutia arbitrara x0 = (alfa* b)/(a,c) = (-2*12)/6 = -4 mod 42 = 38

-a = (m-a) mod m

Calculam celelalte solutii:

x1 = (-4 + 1 * 42/6) mod 42 = 3

x2 = (-4 + 2* 42/6) mod 42 = 10

x3 = (-4 + 3* 42/6) mod 42 = 17

x4= (-4 + 4* 42/6) mod 42 = 24

x5= (-4 + 5* 42/6) mod 42 = 31

Verificare: 17 * 18 mod 42 = 12 mod 42 "A"

Relatia a = b mod m se mai poate scrie ca a mod m = b mod m

Solutiile ecuatiei sunt = {2, 10, 38.....}

Teorema Chineza a resturilor

Teorema Chineza a resturilor se foloseste pentru rezolvarea sistemelor de tipul:

$$\begin{cases} x = b1 \bmod m1 \\ x = b2 \bmod m2 \\ x = b3 \bmod m3 \\ \dots\dots\dots \\ x = bk \bmod mk \end{cases}$$

Pasi de rezolvare:

1) Calculam $ci = m/mi$, unde $m = m1 * m2 * \dots * m$, $i = \overline{1,k}$
2) Rezolvam ecuatiile $ci * x = bi \bmod mi$, $i = \overline{1,k}$
3) Dupa ce am aflat solutiile "partiale" de la toate ecuatiile anterioare ($x1$, $x2, \dots xk$), solutia finala a sistemului va fi egala cu:

$$x = (c1x1 + c2x2 + \dots ck*xk) \bmod m$$

Sistemul de mai sus are solutii daca $(mi, mj) = 1, \forall\, i,j \in \overline{1,k}$, practic sistemul are solutii daca m-urile sunt prime intre ele doua cate doua.

Exemplu: Calculati solutia sistemului daca exista

$$\begin{cases} x = 3 \bmod 5 \\ x = 2 \bmod 3 \\ x = 1 \bmod 7 \end{cases} \qquad m1 = 5,\ m2 = 3,\ m3 = 7$$

Pasul 1: $m = 5 * 3 * 7 = 105$

$c1 = 105/5 = 21$

$c2 = 105/3 = 35$

$c3 = 105/7 = 15$

Pasul 2: Avem urmatoarele ecuatii pe care trebuie sa le rezolvam

$21x = 3 \bmod 5 \quad \Rightarrow x1 = 2$

$35x = 2 \bmod 3 \quad \Rightarrow x2 = 1$

$15x = 1 \bmod 7 \quad \Rightarrow x3 = 1$

Obs! Rezolvam sistemele de mai sus urmand pasii de la ecuatii congruentiale

Pasul 3: Calculam solutia finala => $x = (c1 * x1 + c2*x2 + c3*x3) \bmod m$

$x = (3*21 + 35*1 + 15*1) \bmod 105 = 8$