Nichita Bogdan Valentin

M531

TEMA 2

1. Găsiți numărul minim și maxim de pași pentru algoritmul lui Euclid. Explicați proprietățile.

Numarul mimin de pasi: 1 daca unul dintre numere este divizorul celuilalt sau daca numerele sunt egale

Numarul maxim de pasi: n-1cand numerele sunt doi termini consecutivi din sirul lui Fibonacci (F_{n+1} si F_n)

2. Găsiți numărul de operații elementare pentru algoritmul lui Euclid.

Numarul de pasi pentru algoritmul lui Euclid este ≤ 2($\log_2 a$)

La fiecare pas se executa o impartire si o scadere, deci numarul de operatii elementare este ≤ 4($\log_2 a$) = O($\log_2 a$)

3. Găsiți numărul de operații elementare pentru algoritmul lui Euclid extins.

Numarul de pasi ≤ 2($\log_2 a$)

La fiecare pas se executa o 2 impartiri si 2 scaderi, deci numarul de operatii elementare este ≤ 8($\log_2 a$) = O($\log_2 a$)

4. Demonstrați formula $\sum_{d|n} \boldsymbol{\varphi(d) = n}$

Fie T $= \left(\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}\right) = \left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_{n-1}}{b_{n-1}}, \frac{a_i}{b_i}\right), \qquad (a_i, b_i) = 1, \;\; b_i | \, n$

Fixam d: $d| \, n$

$Daca\ un\ b_i = d, avem\ \ 1 \leq a_i \leq b_i = d\ \ , (a_i, b_i) = (a_i, d) = 1,$

Sunt cel mult $\varphi(d)\ b_i\ pentu\ care\ b_i = d\ (1)$

Fie $a_j\ ai\ \ 1 \leq a_j \leq d,\ \left(a_j, d\right) = 1$

$\frac{a_j}{d} = \frac{a_j \cdot \frac{n}{d}}{d}\ \epsilon$ T

$\frac{a_p}{d} = \frac{a_q}{d} <=> \ a_p = a_q$

Deci sunt cel $putin\ \varphi(d)\ b_i\ pentu\ care\ b_i = d\ (2)$

Din $(1), (2) => sunt\ \varphi(d)\ b_i\ pentu\ care\ b_i = d$

$\sum_{d|n} \varphi(d) = card(T) = n$

6. CMMDC

23. Calculați CMMDC al lui 44556 și 66554 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

66554 = 44556 · 1 + 21998	x_{21998} = (1, 0) – 1 · (0, 1) = (1, -1)
44556 = 21998 · 2 + 560	x_{560} = (0, 1) – 2 · (1, -1) = (-2, 3)
21996 = 560 · 39 + 158	x_{158} = (1, -1) – 39 · (-2, 3) = (79, -118)
560 = 158 · 3 + 86	x_{86} = (-2, 3) – 3 · (79, -118) = (-239, 357)
158 = 86 · 1 + 72	x_{72} = (79, -118) – 1 · (-239, 357) = (318, -475)
86 = 72 · 1 + 14	x_{14} = (-239, 357) – 1 · (318, -475) = (-557, 823)

$72 = 14 \cdot 5 + 2$ $x_2 = (318, -475) - 5 \cdot (-557, 823) = (3103, -4635)$

$14 = 2 \cdot 7 + 0$

CMMDC = 2

$u = -4635$, $v = 3103$

$2 = -4635 \cdot 44556 + 3103 \cdot 66554$

7. Inversul unui număr în $\mathbb{Z}_n$

23. Calculați inversul modular al lui 38 modulo 83.

$83 = 38 \cdot 2 + 7$ $x_7 = (1, 0) - 2 \cdot (0, 1) = (1, -2)$

$38 = 7 \cdot 5 + 3$ $x_3 = (0, 1) - 5 \cdot (1, -2) = (-5, 11)$

$7 = 3 \cdot 2 + 1$ $x_1 = (1, -2) - 2 \cdot (-5, 11) = (11, -24)$

$(83, 38) = 1 \Rightarrow 38$ inversabil in $\mathbb{Z}_{83}$

$1 = 11 \cdot 83 - 24 \cdot 38 \Rightarrow 1 \equiv -24 \cdot 38 \pmod{83} \Rightarrow 38^{-1} \equiv -24 \pmod{83} \equiv 59 \pmod{83}$