Tema 2

Teme Portofoliu:

1. Numărul minim de pași pentru algoritmul lui Euclid este unul. Acesta se realizează când unul dintre numere este multiplul celuilalt număr.

de exemplu: cmmdc (34, 17) returnează 17 și se oprește după un singur pas.

Numărul maxim de pași pentru algoritmul lui Euclid se atinge când ale două numere fac parte din șirul lui Fibonacci. În acest caz, numărul de pași este cu unul mai puțin decât poziția din șir a numărului mai mic.

de exemplu: cmmdc (13, 21) returnează 1, iar pași sunt:

1. $21 = 1 \cdot 13 + 8$

2. $13 = 1 \cdot 8 + 5$

3. $8 = 1 \cdot 5 + 3$

4. $5 = 1 \cdot 3 + 2$

5. $3 = 1 \cdot 2 + 1$

6. $2 = 1 \cdot 1 + 1$

Poziția în șir a numărului 13 este 7, iar algoritmul lui Euclid în acest caz a avut $7-1=6$ pași.

Proprietățile algoritmului lui Euclid:

1. Algoritmul este eficient, având o complexitate logaritmică $O(\log n)$

2. Algoritmul poate fi aplicat pe oricare două numere naturale

2. Operațiile elementare sunt: a mod b și actualizarea valorilor a și b.

În cazul cel mai favorabil are loc o singură împărțire cu rest și o singură actualizare a valorilor, deci 2 operații.

În cazul cel mai nefavorabil am văzut că avem n-1 pași (n este poziția în șirul Fibonacci a numărului mai mic), ceea ce înseamnă că vom avea n-1 împărțiri cu rest și de două ori n-1 atribuiri, deci 3(n-1) operații.

3. În cazul algoritmului lui Euclid extins avem patru operații elementare: împărțirea cu rest, atribuirea, înmulțirea și scăderea.

per iterație vom avea:

- 4 atribuiri: r=n, a=n, n=x1, x0=r
- 2 împărțiri: a/n, a%n
- o înmulțire: q*x1
- o scădere: x0 - q*x1

* 3 atribuiri: $q = a / n$, $n = a \% n$, $x1 = x0 - q * x1$

→ 11 operații per iterație

4. $\sum_{d/n} f(d) = n$ #

Fie $S = \{1, 2, \dots, n\}$.
Pentru fiecare divizor $d$ al lui $n$ fie:

$A(d) = \{k \in S \mid (k, n) = d\}$.

Deci, $A(d)$ conține elementele lui $S$ care au cel mai mare divizor comun al lui $d$ și $n$. Astfel, $A(d)$ este o colecție disjunctă care, reunită formează $S$.

Deci, dacă $f(d)$ numără numărul numerelor prime cu numărul mai mic decât acesta atunci:

$$\sum_{d/n} f(d) = n.$$

6.2) cmmdc dintre 23456 și 65432 folosind alg lui Euclid extins pentru a găsi coef. Bezout.

$X_{65432} = (1,0)$

$X_{23456} = (0,1)$

$65432 = 23456 \cdot 2 + 18520$

$X_{18520} = X_{65432} - 2 \cdot X_{23456} = (1,0) + (0,-2) = (1,-2)$

$23456 = 18520 \cdot 1 + 4936$

$X_{4936} = X_{23456} - X_{18520} = (0,1) + (-1,2) = (-1,3)$

$18520 = 4936 \cdot 3 + 3712$

$X_{3712} = X_{18520} - 3 \cdot X_{4936} = (1,-2) + (3,-9) = (4,-11)$

$4936 = 3712 \cdot 1 + 1224$

$X_{1224} = X_{4936} - X_{3712} = (-1,3) + (-4,11) = (-5,14)$

$3712 = 1224 \cdot 3 + 40$

$X_{40} = X_{3712} - 3X_{1224} = (4,-11) + (15,-42) =$

$= (19,-53)$

$1224 = 40 \cdot 30 + 24$

$X_{24} = X_{1224} - 30X_{40} = (-5, 14) + (-570, 1590)$

$= (-575, 1604)$

$40 = 24 \cdot 1 + 16$

$X_{16} = X_{40} - X_{24} = (19, -53) + (575, -1604)$

$= (594, -1657)$

$24 = 16 \cdot 1 + 8$

$X_8 = X_{24} - X_{16} = (-575, 1604) + (-594, 1657)$

$= (-1169, 3261)$

$16 = 8 \cdot 2 + 0$

$\Rightarrow 8 = 65432 \cdot (-1169) + 23456 \cdot 3261$

7. 2) Inversul modular al lui 15 modulo 26.

$15X \equiv 1 \pmod{26}$

$26 = 15 \cdot 1 + 11$

$15 = 11 \cdot 1 + 4$

$11 = 4 \cdot 2 + 3$

$4 = 3 \cdot 1 + 1$

$3 = 1 \cdot 3 + 0$

$\Rightarrow (15, 26) = 1 \Rightarrow \exists$ soluție unică

$\Rightarrow X = 15^{-1} \pmod{26}$

$X_{26} = (1, 0) \qquad X_{15} = (0, 1)$

$X_{11} = X_{26} - X_{15} = (1,0) - (0,1) = (1,-1)$

$X_4 = X_{15} - X_{11} = (0,1) - (1,-1) = (-1, 2)$

$X_3 = X_{11} - 2X_4 = (1,-1) - (-2,4) = (3,-5)$

$X_1 = X_4 - X_3 = (-1,2) - (3,-5) = (-4,7)$

$\Rightarrow 1 = 26 \cdot (-4) + 15 \cdot 7$

$\Rightarrow X = 15^{-1} = 7 \equiv 26 - 7 \equiv 19 \pmod{26}$

$15 \cdot 19 \equiv 1 \pmod{26}$