Tema - seminar 2

1.) numărul minim de pași: 1 pas (când un număr este multiplul celuilalt)
numărul maxim de pași: n-1 pași (n fiind numărul mai mare dintre cele două)

2) numărul de operații elementare = numărul de împărțiri cu rest (notăm cu k)

3) numărul de operații elementare pentru algoritmul extins = numărul de împărțiri (k) + calculul coeficienților la fiecare împărțire (2k)
$= 3k$

6) 7. $(78901, 10987) = 1$ $78901 = (1,0)$; $10987 = (0,1)$

$78901 = 7 \cdot 10987 + 1992 \longrightarrow X_{1992} = (1,0) - 7(0,1) = (1,-7)$

$10987 = 5 \cdot 1992 + 1027 \longrightarrow X_{1027} = (0,1) - 5(1,-7) = (-5, 36)$

$1992 = 1 \cdot 1027 + 965 \longrightarrow X_{965} = (1,-7) - 1(-5,36) = (6,-43)$

$1027 = 1 \cdot 965 + 62 \longrightarrow X_{62} = (-5,36) - 1(6,-43) = (-11,79)$

$965 = 15 \cdot 62 + 35 \longrightarrow X_{35} = (6,-43) - 15(-11,79) = (171,-1228)$

$62 = 1 \cdot 35 + 27 \longrightarrow X_{27} = (-11,79) - 1 \cdot (171,-1228) = (-182, 1307)$

$35 = 1 \cdot 27 + 8 \longrightarrow X_8 = (171,-1228) - 1(-182,1307) = (353,-2535)$

$27 = 3 \cdot 8 + 3 \longrightarrow X_3 = (-182,1307) - 3(353,-2535) = (-1241, 8912)$

$8 = 2 \cdot 3 + 2 \longrightarrow X_2 = (353,-2535) - 2 \cdot (-1241, 8912) = (2835, -20359)$

$3 = 1 \cdot 2 + \boxed{1} \longrightarrow X_1 = (-1241, 8912) - 1 \cdot (2835, -20359) = (-4076, 29271)$

$2 = 2 \cdot 1 + 0$

$\Rightarrow 1 = (-4076) \cdot 78901 + 29271 \cdot 10987$

7) 7. inversul modular al lui 12 modulo 19.

$12X \equiv 1 \pmod{19} \Rightarrow X = 12^{-1} \pmod{19} = \boxed{8}$

$(12, 19) = 1$ $19 = (1,0)$; $12 = (0,1)$

$19 = 1 \cdot 12 + 7 \longrightarrow X_7 = (1,0) - (0,1) = (1,-1)$

$12 = 1 \cdot 7 + 5 \longrightarrow X_5 = (0,1) - (1,-1) = (-1,2)$

$7 = 1 \cdot 5 + 2 \longrightarrow X_2 = (1,-1) - (-1,2) = (2,-3)$

$5 = 2 \cdot 2 + \boxed{1} \longrightarrow X_1 = (-1,2) - 2 \cdot (2,-3) = (-5, 8)$

$2 = 2 \cdot 1 + 0$

$\Rightarrow 1 = -5 \cdot 19 + 8 \cdot 12$

4. $\sum_{d|n} \varphi(d) = n$ – suma funcției Euler $\varphi(d)$ pt toți divizorii d ai lui n este egală cu n

Fie n un nr. întreg pozitiv, fie d divizorii lui n
Construim mulțimea numerelor de la 1 la n : $\{1,2,\dots,n\}$
Grupăm numerele în clase de resturi modulo d, astfel:

$\{0,1,2,\dots,d-1\}, \{d,d+1,\dots,2d-1\}, \dots, \{n-d, n-d+1,\dots,n-1\}$.

Obs că aceste numere sunt disjuncte și acop. toată mulțimea $\{1,2,\dots n\}$
Obs. că numărul total de astfel de grupuri este n/d.
Fiecare grup conține exact $\varphi(d)$ numere prime cu d.
Dacă parcurgem toți divizorii d ai lui n, at fiecare număr k din mulțimea $1,2,\dots n$ apare exact o dată într-un astfel de grup
Astfel, nr total de nr. este sumă: $\sum_{d|n} \varphi(d) = n$.

Exemplu:

$n=8$, calculăm suma $\sum_{d|12} \varphi(d)$

divizorii lui 8 sunt: 1, 2, 4, 8

$\varphi(1) = 1 \to \{1\}$
$\varphi(2) = 1 \to \{1\}$
$\varphi(4) = 2 \to \{1,3\}$
$\varphi(8) = 4 \to \{1,3,5,7\}$

$\sum_{d|12} \varphi(d) = 1+1+2+4 = 8$ ✓