Criptografie
tema-2

① Numarul minim si maxim de pasi in alg. lui Euclid.

- Cazul optim: când unul dintre numere divide perfect pe celălalt.

  ⇝ Nr min este 1

- Teorema lui Lamé → Numărul maxim de pași este mai mic de 5d, unde d e nr de cifre ale nr mai mic

② Numărul de operații elementare pt. algoritmul lui Euclid.

La fiecare pas calculăm restul împărțirii:

$(a,b) = (b, a \bmod b)$.

- Pentru fiecare împărțire avem $2n^2$ împ pași.
- În cel mai rău caz (numerele consecutive ale șirului Fibonacci) numărul de operații este n (numărul de biți)

⇒ Numărul total de operații este $2n^3$.

③ Numărul de operații elementare pt. algoritmul lui Euclid extins.

- La fiecare pas calculăm și restul:
  Nr deja am calculat ⇒ $2n^2$.
- La algoritmul extins mai în plus 2 înmulțiri (înmulțirea numărului cu vectorul) și 2 scăderi (scăderea de vectori de lungime 2).
  Înmulțirea are $2k^2 - 3k + 1$ pași și scăderea $k-1$ operații
  ⇒ $4n^2 - 6n + 2 + 2k - 2 = 4n^2 - 4n$.

⇒ Numărul total de op. este $4n^2 - 4n$.

(4) $\sum_{d \mid n} \varphi(d) = n$ //

Pt $\forall k \in \{1, 2, \ldots, n\}$ are cmmdc cu n, not $d = \text{cmmdc}(k, n)$
Atunci d e un divizor al n.

Def multimea S_d pt $\forall$ div d al lui n:

$S_d = \{ k \in \{1, \ldots, n\} \mid \text{cmmdc}(k, n) = d \}$

Dacă $(k,n)=d \Rightarrow k = d\cdot m$, $m \in \mathbb{Z}$

- Condiția $(k,n)=d \Rightarrow (m, \frac{n}{d})=1$
- $k = d\cdot m$ și $n = d\cdot\frac{n}{d}$, deci $(d\cdot m, d\cdot\frac{n}{d}) = d\,(m,\frac{n}{d})$.
- $(k,n)=d$
- $|B_d| = \varphi(\frac{n}{d})$

Deoarece mulțimea B_d partiționează mulțimea $\{1,\dots,n\}$, avem

$$n = \sum_{d|n} |B_d| = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$$

Când d parcurge toți divizorii lui n și $\frac{n}{d}$ parcurge aceeași mulțime de divizori

$$\sum_{d|n} |B_d| = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d) = n.$$

(6) $21 \cdot x \equiv 1 \pmod{37}$

37 ebam $\Rightarrow (21, 37) = 1$.

$37 = 1 \cdot 21 + 16$ $\quad x_{37} = (1,0)$, $x_{21} = (0,1)$

$21 = 1 \cdot 16 + 5$ $\quad x_{16} = x_{37} - x_{21} = (1,0) - (0,1) = (1,-1)$

$16 = 5 \cdot 3 + 1$ $\quad x_5 = x_{21} - x_{16} = (0,1) - (1,-1) = (-1,2)$

$5 = 5 \cdot 1 + 0$ $\quad x_1 = x_{16} - 3x_5 = (1,-1) - 3(-1,2) = (4,-7)$

$\Rightarrow 4 \cdot 37 - 7 \cdot 21 = 1$

$\Rightarrow x = -7$, $21 \cdot (-7) = 1 \pmod{37}$

$-7 \equiv 37 - 7 = 30 \pmod{37}$

$\Rightarrow 21^{-1} \equiv 30 \pmod{37}$.

(5) $(34567, 76543) = d$

$76543 = 2 \cdot 34567 + 7409$

$34567 = 4 \cdot 7409 + 4931$

$7409 = 1 \cdot 4931 + 2478$

$4931 = 1 \cdot 2478 + 2453$

$2478 = 1 \cdot 2453 + 25$

$2453 = 98 \cdot 25 + 3$

$25 = 8 \cdot 3 + 1$

$8 = 8 \cdot 1 + 0$

$\Rightarrow (34567, 76543) = 1$

$x_{76543} = (1,0)$, $x_{34567} = (0,1)$

$x_{7409} = x_{76543} - 2x_{34567}$
$= (1,0) - 2(0,1) = (1,-2)$

$x_{4931} = x_{34567} - 4x_{7409}$
$= (0,1) - 4(1,-2) = (-4,9)$

$x_{2478} = x_{7409} - x_{4931}$
$= (1,-2) - (-4,9) = (5,-11)$

$x_{2453} = x_{4931} - x_{2478}$
$= (-4,9) - (5,-11) = (-9,20)$

$x_{25} = x_{2478} - x_{2453}$
$= (5,-11) - (-9,20) = (14,-31)$

$x_3 = x_{2453} - 98 \cdot x_{25}$
$= (-9,20) - 98(14,-31)$
$= (-1381, 3058)$

$x_1 = x_{25} - 8x_3 = (14,-31) - 8(-1381, 3058) = (11062, -24495)$

$11062 \cdot 76543 - 24495 \cdot 34567 = 1$