TKKVFMF 2026-02-17 asistent Samed Bajrić.
1. kolokvij bo 15. 4. 2026.

N
S pomočjo evklidovega algoritma izračunaj GCD(125, 35)

evklidov algoritem:
$a, b \in \mathbb{Z}$; $|a| \geq |b|$

$s_1, s_2, \ldots$ $\quad r_1, r_2, \ldots$

$a = s_1 b + r_1$

$b = s_2 \cdot r_1 + r_2$

$r_1 = s_3 \cdot r_2 + r_3$

$r_2 = s_4 \cdot r_3 + r_4$

...

$|b| > r_1 > r_2 > \ldots \geq 0$

denimo, da je v k-tem koraku $r_k = 0$, $r_{k-1} \neq 0$. tedaj $\gcd(a,b) = r_{k-1}$.

. če pogledamo k-ti zadnji koraku:

$r_{k-2} = s_k \cdot r_{k-1} + r_k \Rightarrow r_{k-1} | r_{k-2}$

$r_{k-3} = s_{k-1} r_{k-2} + r_{k-1} \Rightarrow r_{k-1} | r_{k-3}$

$r_i = s_{i+2} \cdot r_{i+1} + r_{i+2}$

$r_i \geq 2 \cdot r_{i+1} + r_{i+2}$

--- odmor ---

$\gcd(243, 198) = 243x + 198y$
$\quad \| \quad 9$

N
Izračunajte 27^{-1} mod 256. pogoj: $\gcd(a,b) = 1$

$256 = 9 \cdot 27 + 13$

$27 = 2 \cdot 13 + 1$

$13 = 1 \cdot 13 + 0$

... 27^{-1} mod $256 = 19$

N
koliko elementov ima $\mathbb{Z}_{25}^*$? A je $18 \in \mathbb{Z}_{25}^*$? poišči njegov inverz, če je.

$|\mathbb{Z}_n^*| = \varphi(n)$ – eulerjeva f-ja (koliko št. pod n je tujih z n).

$\varphi(n) = \prod_{p|n} (1 - \frac{1}{p})$ $\qquad \varphi(25) = \varphi(5^2) = 5^2 - 5^1 = 20$

$\varphi(p^k) = p^k - p^{k-1}$ za p praštevilo

preverimo, če je 18 tuj s 25: $\gcd(18, 25) = 1$? da.

torej $18 \in \mathbb{Z}_{25}^*$. ... inverz je 7.

N
Zašifrivajte sporočilo MIG z afino šifro s ključem (7,3). delamo v $\mathbb{Z}_{25}$. nato dobljeno sporočilo odšifrirajte z istim ključem.

- Afina šifra: $B = C = \mathbb{Z}_n$ $\qquad D_k(y) = a^{-1}(y - b) \bmod n$

$K: \mathbb{Z}_n^* \times \mathbb{Z}_n$

$E_{k=(a,b)}(x) = ax + b \bmod n$

vsaka črka je ločeno sporočilo
A – 0 B – 1 C – 2 ... Ž – 24

M-13 I-9 Š-19

$E_{(7,3)}(M) = 7 \cdot 13 + 3 \bmod 25 = 19 \rightarrow$ Š

-"- I -"- -"- P

-"- Š -"- -"- K

MI Š → GPK

$7^{-1} \bmod 25 = 18$

$D_{(7,3)}(Š) = 18(19-3) \bmod 26 = 13 \rightarrow$ M

.. P . . . I

K Š

prostor ključev je velik $\varphi(25) \cdot 25 = 20 \cdot 25 = 500$

...

tralali, tralala. tututu tatata ...