# Prvý test z predmetu Základy kryptografie

11.10.2017

Inštrukcie:

- Na vypracovanie písomky máte 90 minút.
- Príklady vypracujte aj s postupom, aby bolo jasné, ako ste dané výsledky dostali.
- Na každom papieri na odovzdanie uveďte svoje meno, číslo z AIS a meno fakulty, ktorú navštevujete (FEI alebo FIIT).
- Na prvú stranu tiež uveďte, koľko papierov odovzdávate.
- Ak v zadaní nie je uvedené inak, multiplikatívne inverzné prvky nemusíte hľadať Euklidovým algoritmom.
- Zadanie si môžete nechať.

Úlohy:

1. (4 body) Pomocou Euklidovho algoritmu v maticovom tvare nájdite multiplikatívne inverzný prvok k 7 v $\mathbb{Z}_{19}$.
2. (3 body) Vypočítajte hodnotu $J\left(\frac{76}{155}\right)$ bez toho, aby ste rozkladali číslo 155 na súčin prvočísel.
3. (3 body) Nájdite všetky celočíselné riešenia kongruencie $15x \equiv 10 \pmod{55}$ z intervalu $[0, 55)$.
4. (8 bodov) Nájdite všetky celočíselné riešenia kongruencie $3x^2 \equiv 3 \pmod{165}$ v intervale $[0, 165)$.
5. (3 body) Nech $M = \{0, 1, \ldots, 26\}$. Nech $a, b \in M$. Definujme funkciu $\alpha : M \to M$ nasledujúcim predpisom:

   $$\alpha(x) = ax + b \pmod{27}$$

   Akú podmienku musí spĺňať $a$, aby bola funkcia $\alpha$ permutáciou? Odpoveď dôkladne zdôvodnite.
6. (4 body) Bez použitia kalkulačky vypočítajte $3^{63} \pmod{450}$. Svoju odpoveď dôkladne zdôvodnite.