Prvý test z predmetu Základy kryptografie

13.10.2016

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 nájdite multiplikatívne inverzný prvok k 8 v $\mathbb{Z}_{27}$.
2. (4 body) Vypočítajte hodnotu $J\left(\frac{92}{175}\right)$ bez toho, aby ste rozkladali číslo 175 na súčin prvočísel.
3. (6 bodov) Nájdite všetky celočíselné riešenia kongruencie $x^2 \equiv 1 \pmod{91}$ v intervale $[0, 91)$.
4. (3 body) Nájdite všetky celočíselné riešenia kongruencie $12x \equiv 8 \pmod{44}$ z intervalu $[0, 44)$.
5. (5 bodov) Nájdite všetky celočíselné riešenia sústavy:

$$\begin{aligned} 2x &\equiv 4 \pmod{14} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

   v intervale $[0, 70)$. Pozor, všimnite si tvar prvej rovnice v sústave!
6. (3 body) Eulerova veta nám hovorí, že pre každé $a \in \mathbb{Z}_m$ také, že $\gcd(a, m) = 1$ platí, že

$$a^{\varphi(m)} = 1 \pmod{m} \tag{1}$$

   Môže rovnica (1) platiť aj pre $a \in \mathbb{Z}_m$ také, že $\gcd(a, m) > 1$? Zdôvodnite.
7. (Prémia za 3 body) O Eulerovej funkcii vieme, že ak $\gcd(a, b) = 1$, potom platí, že $\varphi(ab) = \varphi(a) \times \varphi(b)$. Hovoríme, že Eulerova funkcia je multiplikatívna. Je aj Carmichaelova funkcia multiplikatívna? (Teda, platí, že ak $\gcd(a, b) = 1$, potom $\lambda(ab) = \lambda(a) \times \lambda(b)$?) Zdôvodnite.