Prvý test z predmetu Základy kryptografie

21.10.2015

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 a číslo z AIS.
- Na prvú stranu tiež uveďte, koľko papierov odovzdávate.
- Zadanie si môžete nechať.

Úlohy:

1. (4 body) Pomocou Euklidovho algoritmu nájdite multiplikatívne inverzný prvok k 7 v $\mathbb{Z}_{23}$.
2. (3 body) Uvažujte kongruenciu $ax \equiv 15 \pmod{10000}$, kde $a \in \mathbb{Z}_{10000}$. Zvoľte hodnotu a tak, aby kongruencia mala iba jedno riešenie. Koľko možností pre voľbu hodnoty a máte, ak chcete, aby kongruencia mala iba jedno riešenie?
3. (3 body) Nech $n_1, n_2 \in \mathbb{N}$. Ak $n_1 < n_2$, platí potom, že $\varphi(n_1) < \varphi(n_2)$? (t.j. Je Eulerova funkcia rastúca?) Zdôvodnite.
4. (3 body) Vypočítajte hodnotu $J\left(\frac{132}{155}\right)$ bez toho, aby ste rozkladali číslo 155 na súčin prvočísel.
5. (6 bodov) Nájdite všetky celočíselné riešenia kongruencie $x^2 \equiv 1 \pmod{77}$ v intervale $[0, 77)$.
6. (6 bodov) Nájdite všetky celočíselné riešenia sústavy:

$$\begin{aligned} 2x &\equiv 4 \pmod{6} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 5 \pmod{7} \end{aligned}$$

   v intervale $[0, 210)$. Pozor, všimnite si tvar prvej rovnice v sústave!

7. (Prémia za 3 body) Nech $k_1, k_2, a_1, a_2, m_1, m_2 \in \mathbb{N}$ a nech platí $\gcd(k_1 m_1, k_2 m_2) = 1$. Uvažujme sústavu:

$$\begin{aligned} k_1 x &\equiv k_1 a_1 \pmod{k_1 m_1} \\ k_2 x &\equiv k_2 a_2 \pmod{k_2 m_2} \end{aligned}$$

   Koľko má sústava riešení v intervale $[0, k_1 m_1 k_2 m_2)$? Zdôvodnite.