Prvý test z predmetu Základy kryptografie

17.10.2014

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. (5bodov) Nájdite všetky celočíselné riešenia kongruencie $12x \equiv 8 \pmod{44}$ z intervalu $[0, 44]$. Na nájdenie multiplikatívne inverzného prvku použite Euklidov algoritmus.
2. (4body) Nájdite riešenie sústavy:

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{11} \end{aligned}$$

   v intervale $[0, 385)$.
3. (3body) Nájdite zvyšok čísla 5^{2402} po delení 13.
4. (5bodov) Vypočítajte hodnotu $J\left(\frac{68}{105}\right)$ bez toho, aby ste rozkladali číslo 105 na súčin prvočísel. Je možné na základe hodnoty $J\left(\frac{68}{105}\right)$ určiť, či kongruencia $x^2 \equiv 68 \pmod{105}$ má celočíselné riešenie alebo nemá?
5. (8bodov) Nájdite všetky celočíselné riešenia sústavy:

$$\begin{aligned} x^2 &\equiv 1 \pmod{35} \\ 2x &\equiv 3 \pmod{11} \end{aligned}$$

   v intervale $[0, 385)$.
6. (Prémia za 5bodov) Nech p je prvočíslo také, že $p \equiv 5 \pmod{8}$. Nech a je kvadratický zvyšok modulo p. Uvažujte nasledujúci algoritmus:
   - Najprv sa vypočíta $d = a^{\frac{p-1}{4}} \pmod{p}$
   - Ak $d = 1$, vypočíta sa $r = a^{\frac{p+3}{8}} \pmod{p}$
   - Ak $d = -1$, vypočíta sa $r = 2a(4a)^{\frac{p-5}{8}} \pmod{p}$
   - Algoritmus vráti dvojicu $(r, -r)$

   Dokážte, že výstupy z algoritmu budú odmocninami z a modulo p. (Teda, že platí $r^2 = a \pmod{p}$)