TEORIJA BROJEVA U KRIPTOGRAFIJI

3. zadaća

17. 3. 2004.

1. Riješite sustav kongruencija

$$x \equiv 3 \pmod{6}, \quad x \equiv 5 \pmod{35}, \quad x \equiv 7 \pmod{143}, \quad x \equiv 11 \pmod{323}.$$

2. Za $r = 1, 2, 3, \ldots, 10$ nađite najmanji prirodan broj $d(r)$ sa svojstvom da je duljina perioda u razvoju u jednostavni verižni razlomak broja $\sqrt{d(r)}$ jednaka r.

3. Prikažite broj 17389 kao zbroj kvadrata dva cijela broja primjenom Hermiteove ili Legendreove konstrukcije.

4. Pomoću Tonellijevog algoritma nađite rješenje kongruencije

$$x^2 \equiv 302 \pmod{2081}.$$

5. Neka je p neparan prost broj. Dokažite da kvadratni ostatak modulo p ne može biti primitivni korijen modulo p. Pokažite primjerom da kvadratni neostatak modulo p ne mora biti primitivni korijen modulo p. Mora li najmanji kvadratni neostatak modulo p biti primitivni korijen modulo p?

6. Dokažite je prirodan broj n potpun kvadrat ako i samo ako je $(\frac{n}{p}) = 1$ za svaki prost broj p koji ne dijeli n.

Rok za predaju zadaće je 7.4.2004. Andrej Dujella