ALGORITMI U TEORIJI BROJEVA

zadaća 4.47

1. U RSA kriptosustavu s javnim ključem (n, e) i tajnim eksponentom d, gdje je

$$n = 11312143, \quad e = 7, \quad d = 2153335$$

odredite najmanji prirodan broj k takav da za broj $m = (ed - 1)/2^k$ postoji neki prirodan broj a takav da je $\text{nzd}(a, n) = 1$ i $a^m \not\equiv 1 \pmod{n}$. Odredite i najmanji pripadni prirodni broj a.

2. Neka je $(n, e) = (17720267, 2796571)$ javni RSA ključ. Poznato je da tajni eksponent d zadovoljava nejednakost $d < \frac{1}{3}\sqrt[4]{n}$. Odredite d pomoću Wienerovog napada.

3. Odredite najmanji prirodan broj n koji je pseudoprost broj u bazi 53, a nije Eulerov pseudoprost broj u bazi 53.