ALGORITMI U TEORIJI BROJEVA

zadaća 4.25

1. Odredite proste brojeve p i q te tajni eksponent d u RSA kriptosustavu ako je poznato da je $n = 3211063$, $\varphi(n) = 3207400$ i $e = 17$.

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

$$n = 6496207, \quad e = 17, \quad d = 636353$$

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.