ALGORITMI U TEORIJI BROJEVA

završni ispit – grupa A

12.6.2025.

1. Odredite najmanji prirodan broj n koji je pseudoprost broj u bazi 4, a nije Eulerov pseudoprost broj u bazi 4.

   Rješenje:

2. Je li broj $n = 1649$ jaki pseudoprost broj u bazi $b = 12$?

   Navedite ostatke $b^{2^r \cdot t} \bmod n$, $r = 0, 1, \ldots, s$ koji to dokazuju (ovdje je $n - 1 = 2^s \cdot t$ i t je neparan).

   Rješenje:

3. Faktorizirajte broj $n = 1219$ Pollardovom ρ metodom, uz $f(x) = x^2 - 1$ i $x_0 = 2$. Navedite odgovarajuće vrijednosti x_i, y_i.

   Rješenje:

4. Faktorizirajte broj $n = 286901$ Pollardovom $p - 1$ metodom, uz $B = 8$ i $a = 2$. Navedite i koliko je $a^m \bmod n$.

   Rješenje:

5. Faktorizirajte broj $n = 12091$ metodom verižnog razlomka. Navedite i pripadne vrijednosti $(-1)^i t_i$ korištene u faktorizaciji.

   Rješenje:

Dozvoljeno je korištenje džepnog kalkulatora, te dva papira s formulama.
Kalkulatori se mogu koristiti za standardne operacije, ali nije dozvoljeno korištenje gotovih funkcija za algoritme iz teorije brojeva.

Andrej Dujella