

ALGORITMI U TEORIJI BROJEVA

probni završni ispit

1. Je li broj $n = 1105$ jaki pseudoprost broj u bazi $b = 4$?

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

2. Faktorizirajte broj $n = 2449$ Pollardovom ρ metodom, uz $f(x) = x^2 - 1$ i $x_0 = 2$.

Navedite odgovarajuće vrijednosti x_i, y_i .

3. Faktorizirajte broj $n = 633211$ Pollardovom $p - 1$ metodom, uz $B = 8$ i $a = 2$.

Navedite i koliko je $a^m \bmod n$.

4. Faktorizirajte broj $n = 25511$ metodom verižnog razlomka. Navedite i pripadne vrijednosti $(-1)^{t_i}$ korištene u faktorizaciji.

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.