

ALGORITMI U TEORIJI BROJEVA

završni ispit – grupa A

13.6.2024.

1. Je li broj $n = 377$ jaki pseudoprost broj u bazi $b = 12$?

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).

Rješenje:

2. Faktorizirajte broj $n = 1207$ Pollardovom ρ metodom, uz $f(x) = x^2 - 1$ i $x_0 = 2$. Navedite odgovarajuće vrijednosti x_i, y_i .

Rješenje:

3. Faktorizirajte broj $n = 283529$ Pollardovom $p - 1$ metodom, uz $B = 8$ i $a = 2$. Navedite i koliko je $a^m \bmod n$.

Rješenje:

4. Faktorizirajte broj $n = 11521$ 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