

**Prvi kolokvij iz Uvoda u teoriju brojeva**

16. svibnja 2016.

1. [20 bodova] Neka je  $n \in \mathbb{N}$ . Dokažite da su elementi skupa

$$S = \{n!i + 1 : i \in \{1, 2, \dots, n\}\}$$

u parovima relativno prosti.

2. [20 bodova] Neka je  $k \in \mathbb{N}$ ,  $k > 2$ . Dokažite da je broj  $4^k - 1$  produkt barem tri prirodna broja različita od 1.
3. [10 bodova] Dokažite da broj oblika  $n = 12m + 9$ ,  $(3, m) = 1$ , ne može biti savršen.
4. [20 bodova] Odredite najmanji dozvoljeni  $e$  tako da  $(3193, e)$  bude javni ključ RSA kriptosustava i vrijedi

$$e \equiv 1 \pmod{12}, \quad e \equiv 29 \pmod{56}.$$

5. [30 bodova] Neka je  $p$  neparan prost broj.

(a) Ako je  $a = (p - 3)!$ , odredite ostatak pri dijeljenju broja  $2^{2p}a$  s  $p$ .

(b) Ako  $p|b^4 + 1$ ,  $b \in \mathbb{N}$ , odredite red od  $b$  modulo  $p$ .

**Napomena.** Sve svoje tvrdnje obrazložite.