

1	2	3	4	5	6	Σ

JMBAG

IME I PREZIME

Teorija brojeva

1. kolokvij, 6.5.2022.

NAPOMENE: Vrijeme rješavanja je 120 minuta. Ima ukupno šest zadataka. Zadaci se rješavaju na ovim papirima. Odmah se **čitljivo** potpišite. Dozvoljeno je korištenje kalkulatora i dva papira A4 s formulama.

1. Odredite $g = \text{nzd}(a, b)$ i nađite cijele brojeve x, y takve da je $ax + by = g$, ako je $a = 11286, b = 4080$.

2. Riješite sustav kongruencija

$$x \equiv 45 \pmod{52},$$

$$x \equiv 6 \pmod{65},$$

$$x \equiv 11 \pmod{70}.$$

3. Nađite sva rješenja jednadžbe $\varphi(n) = 232$.

4. Riješite kongruenciju

$$x^4 + x^2 - 3x - 1 \equiv 0 \pmod{7^4}.$$

5. (a) Nađite najmanja dva primitivna korijena modulo 53.
- (b) Riješite (pomoću indeksa) kongruenciju: $3x^5 \equiv 5 \pmod{53}$.

6. (a) Izračunajte sljedeće Legendreove simbole: $\left(\frac{1000}{677}\right)$, $\left(\frac{251}{397}\right)$.
- (b) Odredite sve proste brojeve p takve da je 3 kvadratni ostatak modulo p .

Rješenja:

1. $g = 6 = 201 \cdot 11286 + (-556) \cdot 4080$

2. $x \equiv 1761 \pmod{1820}$

3. $n = 233, 295, 466, 472, 590, 708$

4. $x \equiv 634 \pmod{2401}$

5. (a) 2,3 (b) $x \equiv 11 \pmod{53}$

6. (a) $\left(\frac{1000}{677}\right) = 1, \left(\frac{251}{397}\right) = -1, \quad$ (b) $p \equiv 1, 11 \pmod{12}, p = 2$