Odjel za matematiku, Sveučilište u Osijeku

grupa A

Prvi kolokvij iz Uvoda u teoriju brojeva

11. svibnja 2011.

1. [**20 bod.**] Neka su $a, b \in \mathbb{Z}$, $(a, b) = 1$. Dokažite da je tada $(a+b, a-b) = 1$ ili 2.

2. [**10 bod.**] Pronađite ostatak pri djeljenju broja $13 \cdot 12^{45}$ brojem 47.

3. [**10 bod.**] Neka je n prirodan broj. Ako $\varphi(n)$ dijeli $n-1$, pokažite da je tada n kvadratno slobodan, odnosno za $a \neq 1$, $a^2 \nmid n$.

4. [**20 bod.**] U RSA kriptosustavu s javnim ključem $(65, 11)$ dešifrirajte sljedeću poruku

$$49 \quad 11 \quad 28 \quad 1.$$

Dobiveni brojevi predstavljaju redom koeficijente u linearnoj diofantskoj jednadžbi koja je postavljena u 5. zadatku (pod a)).

5. a) [**10 bod.**] Riješite jednadžbu $\_\_\_x + \_\_\_y + \_\_\_z = \_\_\_$?

   b) [**10 bod.**] Postoji li rješenje jednadžbe $x^2 + 2y^2 = 21$.

6. [**20 bod.**] Dokažite sljedeću tvrdnju. Neka je p prost neparan broj. Ako $p | F_n = 2^{2^n} + 1$ i $n \geq 2$ onda postoji $k \in \mathbb{Z}$ takav da je $p = k2^{n+1} + 1$.

Odjel za matematiku, Sveučilište u Osijeku

grupa B

Prvi kolokvij iz Uvoda u teoriju brojeva

11. svibnja 2010.

1. [**20 bod.**] Neka je $p > 3$ i neka su p i $p+2$ prosti prirodni brojevi. Dokažite da je tada $2p+2$ djeljivo s 12.

2. [**10 bod.**] Pronađite ostatak pri djeljenju broja $14 \cdot 13^{49}$ brojem 51.

3. [**10 bod.**] Neka je n prirodan broj. Ako $\varphi(n)$ dijeli $n-1$, pokažite da je tada n kvadratno slobodan, odnosno za $a \neq 1$, $a^2 \not| n$.

4. [**20 bod.**] U RSA kriptosustavu s javnim ključem $(85, 13)$ dešifrirajte sljedeću poruku

   $$32 \quad 4 \quad 20 \quad 1.$$

   Dobiveni brojevi predstavljaju redom koeficijente u linearnoj diofantskoj jednadžbi koja je postavljena u 5. zadatku (pod a)).

5. a) [**10 bod.**] Riješite jednadžbu $\_\_\_x + \_\_\_y + \_\_\_z = \_\_\_$?

   b) [**10 bod.**] Postoji li rješenje jednadžbe $x^2 + 3y^2 = 17$.

6. [**20 bod.**] Dokažite sljedeću tvrdnju. Neka je p prost neparan broj. Ako $p | F_n = 2^{2^n} + 1$ i $n \geq 2$ onda postoji $k \in \mathbb{Z}$ takav da je $p = k2^{n+1} + 1$.