Zadatak 1. (5+2)

(a) Odredite najmanji prirodan broj n takav da $3^2 \mid n$, $4^2 \mid n+1$ i $5^2 \mid n+2$.

(b) Postoji li prirodan broj n takav da $2^2 \mid n$, $3^2 \mid n+1$ i $4^2 \mid n+2$? Obrazložite!

Zadatak 2. (3+4)

(a) Razvijte u jednostavni verižni razlomak $\frac{146}{177}$.

(b) Odredite realan broj čiji je rastav u jednostavni verižni razlomak oblika [2;3,1,1].

Zadatak 3. (4+5)

(a) Koliko ima primitivnih korijena modulo 31? Odredite ih sve!

(b) Riješite kongruenciju $29\ x^8 \equiv 13 \pmod{31}$.

Zadatak 4. (7) Odredite najmanja rješenja (u prirodnim brojevima) Pellovih jednadžbi $x^2-57y^2=1$ i $x^2-57y^2=-1$ (ako postoje).

Zadatak 5. (6) Odredite sve neparne proste brojeve p takav da je $\left(\frac{-60}{p}\right) = -1$.

Zadatak 6. (3+2+2) Zadani su skupovi

$$S=\{z \in C, \mid z \mid =1\}$$

$$K_n=\{z \in C, z^n=1, \text{ n prirodan broj}\}$$

$$K=\bigcup_{n=1}^{\infty} Kn$$

(a) Dokažite da *S* grupa s obzirom na množenje kompleksnih brojeva.

(b) Dokažite da je K_n podgrupa od *S* za svaki prirodan broj n.

(c) Je li *K* podgrupa od *S*? Sve svoje tvrdnje dokažite!

Zadatak 7. (2+2+3)

(a) Neka je $f:(P_1,+,\bullet) \rightarrow (P_2,+,\bullet)$ izomorfizam prstena P_1 i P_2. Dokažite: Ako je P_1 integralna domena, onda je i P_2 integralna domena.

(b) Dokažite da u tijelu nema pravih ideala.

(c) Dokažite da je $(\mathbf{Z},+,\bullet)$ prsten glavnih ideala.

Zadatak 8. (4) Odredite parametre a,b,c takve da polinom $p(x)=x^6+ax^3+bx^2+cx+1$ bude inverz polinoma $q(x)=x^3+1$ u polju $\mathbf{F}_2{}^8$ reprezentiranom kao $\mathbf{Z}_2(t)/h(t)$, gdje je $h(t)=t^8+t^4+t^3+t+1$ polinom ireducibilan nad $\mathbf{Z}_2$.

Zadatak 9. (6) U Rabinovom kriptosustavu s parametrima (n,p,q)=(437,19,23), dešifrirajte šifrat y=35. Poznato je da je otvoreni tekst prirodan broj z<n kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.