1(7) Odredite podgrupu od

a) $(\mathbb{Z}_{11}, +_{11})$ generiranu elementom 5

b) $(\mathbb{Z}_{11}^*, \cdot_{11})$ generiranu elementom 5

c) $(\mathbb{C}^*, \cdot)$ generiranu elementom $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$

2(6) Neka je $f: X \to Y$ homomorfizam grupa X i Y

a) Dokažite da f preslikava neutralni element grupe X u neutralni element grupe Y

b) Neka je b inverzni element od a u grupi X.
Dokažite da je $f(b)$ inverzni element od $f(a)$ u grupi Y.

c) Dokažite da je jezgra homomorfizma $f: X \to Y$ podgrupa od X.

3(5) Dokažite da je skup

$$P = \{a + b\sqrt[3]{5} + c\sqrt[3]{25} : a, b, c \in \mathbb{Z}\}$$

prsten uz uobičajeno zbrajanje i množenje realnih brojeva.
Je li P polje? Obrazložite!

4(5) a) Dokažite da je polinom $h(t) = t^2 + t + 2$ ireducibilan nad $\mathbb{Z}_3$.

b) Nadite jedan generator multiplikativne grupe F_9^* polja F_9 reprezentiranog kao $\mathbb{Z}_3[t]/(h(t))$?

c) Kolika je red elementa $t+2$ u F_9^*?

5(6) U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (3149, 47, 67)$$

dešifrirajte šifrat $y = 665$. Poznato je da je otvoreni tekst prirodan broj kojemu su zadnja 4 bita u binarnom zapisu jedinica 0101.

6(6) Alice je poslala istu poruku u nekoliciini agenata. Eva je presrela šifrate c_1, c_2, c_3 za trojicu agenata čiji su javni ključevi n_1, n_2 i n_3. Poznato je da Alice i agenti koriste RSA kriptosustav s javnim eksponentom $e = 3$. Za zadane

$$n_1 = 35, \quad c_1 = 1$$
$$n_2 = 33, \quad c_2 = 11$$
$$n_3 = 58, \quad c_3 = 55$$

pokažite kako će Eva otkriti poruku m (bez poznavanja faktorizacije modula n_1, n_2, n_3).

7. (5) Zadan je ElGamalov kriptosustav s ključem

$K = (p = 79, \alpha = 3, a = 4, \beta = 2)$.

Dešifrirajte šifrat $(y_1, y_2) = (36, 8)$.

8. (5) Zadan je Merkle-Hellmanov kriptosustav s ključem

$K = (v, p, a, t)$ gdje je

$v = (2, 4, 10, 23, 62, 114, 236, 466)$

$p = 499$, $a = 5$,

$t = (10, 20, 50, 115, 310, 182, 334)$.

Dešifrirajte šifrat $y = 317$.