Zadatak 1.

a) Riješite kongruenciju 159x ≡ 66 (mod 201).

201 = 159×1+42
159 = 42×3+33
42 = 33×1+9
33 = 9×3 + 3   d=3

a' = 159/3 = 53   b'= 66/3 = 22   m'= 201/3 = 67

53x ≡ 22 (mod 67)

67 = 53×1 + 14
53 = 14×3 + 1
14 = 11×1 + 3
11 = 3×3 + 2
3 = 3×1 + 1

$y_i = y_{i-2} - q_i \times y_{i-1}$

i	-1	0	1	2	3	4	5
q_i			1	3	1	3	1
y_i	0	1	-1	4	-5	19	-24

(-24) ×53x ≡ (-24)×22 (mod 67) → x ≡ (-24)×22 (mod 67) → x ≡ -528 (mod 67)

x ≡ -528 (mod 67) → *(670-528=142)* → x ≡ 142 (mod 67) → *ostatak(142/67)* → <u>x ≡ 8 (mod 67)</u>

d=3 → 3 riješenja:

x_1 ≡ 8 (mod 201)
x_2 ≡ (8 + 67×1) (mod 201) ≡ 75 (mod 201)
x_3 ≡ (8 + 67×2) (mod 201) ≡ 142 (mod 201)

b) Odredite sve prirodne brojeve *n* iz intervala [1100,1400] koji zadovoljava kongruenciju 159*n* ≡ 66 (mod 201).

n_1 = (8 + 67×17) = 1147
n_2 = (8 + 67×18) = 1214
n_3 = (8 + 67×19) = 1281
n_4 = (8 + 67×20) = 1348

c) Odredite sve prirodne brojeve *m* za koje vrijedi 159 ≡ 66 (mod *m*).

$m = 159 - 66 = 93$ jer $159 \div 93 = 1$ i $ostatak$ 66.

Zadatak 2.
a) Odredite sve prirodne brojeve *n* takve da je φ(*n*)=100.

Djeljenici od 100: p(i) ϵ {1, 2, 4, 5, 10, 20, 25, 50, 100}.

Uvećani za 1: p(i-1) ϵ {2, 3, 5, 6, 11, 21, 26,51, 101}.

Prosti brojevi iz prethodnog skupa: p(i-1) ϵ {2,3,5,11,101}.

$$(2^{a_1-1} \times 1)(3^{a_2-1} \times 2)(5^{a_3-1} \times 4)(11^{a_4-1} \times 10)(101^{a_5-1} \times 100)$$

$(101^{a_5-1} \times 100) = 100$ za a_5 = 1 pa je n_1 = 101^{a_5} = 101.

$(2^{a_1-1} \times 1)(101^{a_5-1} \times 100)$ = 100 za a_5 = 1 i a_1 = 1 pa je n_2 = $2^{a_1} \times 101^{a_5}$ = 202.

$(5^{a_3-1} \times 4)$ = 100 za a_3 = 3 pa je n_3 = 5^{a_3} = 125.

$(2^{a_1-1} \times 1)(5^{a_3-1} \times 4)$ = 100 za a_1 = 1 i a_3 = 3 pa je je n_4 = $2^{a_1} \times 5^{a_3}$ = 250.

<u>n={101,202,125,250}.</u>

b) Postoji li prirodan broj n > 1 takav da je φ(*n*) = *n* ? Obrazložite odgovor.

Da bi φ(*n*) = *n* vrijedilo, to bi značilo da su svi prethodnici broja *n* relativno prosti s *n*.

Za *n*= ${p_1}^{a_1} \times {p_2}^{a_2} \times ... {p_r}^{a_r}$ vrijedi

φ(*n*) = ${p_1}^{a_1-1}(p_1 - 1) \times {p_2}^{a_2-1}(p_2 - 1) \times ... {p_r}^{a_r-1}(p_r - 1)$.

Za φ(*n*) = *n:*

$$n = {p_1}^{a_1-1}(p_1 - 1) \times {p_2}^{a_2-1}(p_2 - 1) \times ... {p_r}^{a_r-1}(p_r - 1)$$

$$n = {p_1}^{a_1}(1 - {p_1}^{-1}) \times {p_2}^{a_2}(1 - {p_2}^{-1}) \times ... {p_r}^{a_r}(1 - {p_r}^{-1})$$

$$n = {p_1}^{a_1} \times {p_2}^{a_2} \times ... {p_r}^{a_r} \times (1 - {p_1}^{-1}) \times (1 - {p_2}^{-1}) \times ... (1 - {p_r}^{-1})$$

$$n = n \times (1 - {p_1}^{-1}) \times (1 - {p_2}^{-1}) \times ... (1 - {p_r}^{-1})$$

$$1 = (1 - {p_1}^{-1}) \times (1 - {p_2}^{-1}) \times ... (1 - {p_r}^{-1})$$

Kako ne postoje prosti faktori veći od 0 koji bi zadovoljili gornju jednadžbu (umnošci brojeva manjih od 1 trebaju dati 1), tako i ne postoji broj *n*.

Zadatak 3.
a) Iskažite i dokažite mali Fermatov teorem.

Neka je p prost broj, p є P, takav da p nije djeljiv s a. Tad vrijedi a^{p-1} ≡ 1 (mod p).

b) Odredite ostatak pri dijeljenju broja 2013^{2013} sa 19.

2013^{2013} ≡ m (mod 19) → $m = 2013$ mod 19 = 18.

c) Neka je p neparan prost broj. Dokažite da je $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1}$ ≡ -1 (mod p).

Zadatak 4.
Odredite sve Pitagorine trokute sa stranicom duljine 125.

d=1, 5, 25.

Stranice trokuta:

$x = d\ (m^2 - n^2)$
$y = 2dmn$
$z = d\ (m^2 + n^2)$

d=1:

$m^2 - n^2$ = $(m-n)(m+n) = 125$

m-n =1
m+n = 125 → m=63, n=62 → <u>(x,y,z) = (125, 7812, 7813)</u>

m-n=5
m+n=25 → m=15, n=10 → <u>(x,y,z)=(125, 300, 325)</u>

$m^2 + n^2 = 125$ → m=11, n=2 → <u>(x,y,z)=(117, 44 , 125)</u>

d=5:

$(m^2 + n^2)$ = 25 → m=4, n=3 → <u>(x,y,z)=(35,120,125)</u>

$m^2 - n^2$ = 25 → m=13, n=12 → <u>(x,y,z)=(125, 1560, 1565)</u>

d=25:

$m^2 + n^2 = 5$ → m=2, n=1 → <u>(x,y,z)=(75,100,125)</u>

Zadatak 5.

a) Izračunajte Jacobijeve simbole ($\frac{-19}{2013}$) i ($\frac{-23}{2013}$) .

Pravila za Jacobi simbol:

1) (1/*n*) = 1 i (0/*n*) = 0.
2) Ako je a prost broj tad (*a/n*) = (*b/n*) ako je $a = b$ mod n , inače se radi faktorizacija (*a/n*)=(*c/n*)(*d/n*).
3) Ako su m i n prosti, tad (*m/n*) = (*n/m*)$(-1)^{(\frac{m-1}{2}\frac{n-1}{2})}$.
4) (-1/*n*) = $(-1)^{(\frac{n-1}{2})}$.
5) (2/*n*) = $(-1)^{(\frac{n^2-1}{8})}$.

(-1/2013)(19/2013) = (18/19) = -(9/19) = -(1/9) = -1

(-1/2013)(23/2013) = (12/23) = (6/23) = (3/23) = -(2/3) = (1/3) = 1

b) Odredite sve brojeve p takve da je ($\frac{-3}{p}$) = 1.

(-3/*p*) = (-1/*p*)(3/*p*) = 1.

Podjela na dva slučaja:

1) (-1/*p*) = 1, (3/*p*) = 1.

(-1/*p*) = 1 → $p \equiv 1 \pmod 4$

(3/*p*) = 1 → $p \equiv 1 \pmod{12}$

$p \equiv 1 \pmod{48}$

2) (-1/*p*) = -1, (3/*p*) = -1.

(-1/*p*) = -1 → $p \equiv 3 \pmod 4$

(3/*p*) = -1 → $p \equiv 5 \pmod{12}$

$p \equiv 7 \pmod{24}$

Iz $p \equiv 1 \pmod{48}$ i $p \equiv 7 \pmod{24}$ → $p \equiv 49 \pmod{192}$.

Zadatak 6.

a) Dokažite da skup svih matrica oblika $\begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix}$, x ϵ $R^* = R \ \backslash \{0\}$, čini grupu s obzirom na matrično množenje.

Skup G je grupa ako zadovoljava sljedeća svojstva.

Zatvorenost – za sve a,b ϵ G, vrijedi ab ϵ G.

$$\begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} y & y \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} xy & xy \\ 0 & 0 \end{bmatrix}$$

Asocijativnost - za sve a,b, c ϵ G, vrijedi a(bc) = (ab)c.

$$\begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix} \times (\begin{bmatrix} y & y \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} z & z \\ 0 & 0 \end{bmatrix}) = (\begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} y & y \\ 0 & 0 \end{bmatrix}) \times \begin{bmatrix} z & z \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} xyz & xyz \\ 0 & 0 \end{bmatrix}$$

Neutralnost – postoji jedinični neutralni element e za kojeg vrijedi ae = ea = a.

$$\begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix}, e = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

Inverz – za svaki a postoji inverzni element za koji vrijedi $aa^{-1} = a^{-1}\, a = e$.

Iz jednadžbe $\begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} y & y \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ je vidljivo da je xy=1, tj. inverz je $\begin{bmatrix} 1/x & 1/x \\ 0 & 0 \end{bmatrix}$.

b) Je li grupa iz a) dijela zadatka izomorfna multiplikativnoj grupi realnih brojeva R^* ? Ukoliko jest, konstruirajte odgovarajući izomorfizam. Svoje tvrdnje dokažite.

Za dokaz izoformizma između grupa (R_m^*,•) i (R^*,•) mora vrijediti bijekcija $f(xy) = f(x) \times f(y)$ i grupe moraju imati isti kardinalni broj.

$$f(xy) = \begin{bmatrix} xy & xy \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} y & y \\ 0 & 0 \end{bmatrix} = f(x) \times f(y)$$

Zadatak 7.
a) Je li prsten $(Z_{143}, +_{143}, \bullet_{143})$ integralna domena? Ukoliko jest, dokažite tu tvrdnju, a ukoliko nije navedite odgovarajući kontraprimjer.

Prsten Z_n je integralna domena samo ako je *n* prost broj; integralnu domenu čini svaki prsten za kojeg ne postoje djelitelji nule, to jest, brojevi $a \neq 0,\ b\ \neq 0$ za koje vrijedi $ab = 0$.

U ovom slučaju Z_{143} nije integralna domena što se može vidjeti po prisustvu djelitelja nule jer u prstenu Z_{143} vrijedi da je $13\ \times 11 = 0$.

b) Je li skup P = {*a* + *bi*: *a*, *b* ϵ **Z**} prsten uz uobičajeno zbrajanje i množenje kompleksnih brojeva ? Ukoliko jest, dokažite tu tvrdnju, a ukoliko nije navedite odgovarajući kontraprimjer.

Prsten je bilo koji skup $R\ \neq 0$, zajedno s dvije operacije: množenje i zbrajanje, tako da vrijedi:

1) asocijativnost zbrajanja $(a + b) + c = a + (b + c)$

$$a + bi + (c + di + e + fi) = (\ a + bi) + c + di + e + fi = (a + c + e) + (b + d + f)i$$

2) postoji element $0 \in R$ tako da je $a + 0 = 0 + a = a$

$$a + bi + (0 + 0i) = a + bi$$

3) za svaki element $a \in R$ postoji suprotni element $- a \in R$ tako da je $a + (-a) = (-a) + a = 0$

$$a + bi + (-a - bi) = 0 + 0i$$

4) komutativnost zbrajanja $a + b = b + a$

$$a + bi\ + c + di = c + di + a + bi\ =\ (a + c) + (b + d)i$$

5) asocijativnost množenja $a(bc) = (ab)c$

$$\begin{aligned}(a + bi)(c + di)(e + fi) &= (ac\ + adi + bci - bd\ )(e + fi)\\ &= ace + acfi + adei - adf + bcei - bcf - bde + bdfi\end{aligned}$$

$$\begin{aligned}(a + bi)(c + di)(e + fi) &= (a + bi)(ce + cfi + dei - df)\\ &= ace + acfi + adei - adf + bcei - bcf - bde - bdfi\end{aligned}$$

6) zakon distribucije $a(b + c) = ab + ac$

$$(a + bi)(c + di + e + fi) = ac + adi + ae + afi + bci - bd + bei - bf$$

$$(a + bi)(c + di)\ + (a + bi)(e + fi) = ac + adi + bci - bd + ae + afi + bei - bf$$

c) Dokažite da je (**Z**,+, •) prsten glavnih ideala.

Glavni ideal je unutar komutativnog prstena R skup višekratnika elementa *a* oblika $(a) = \{ra \in\ R\ :\ r\ \in R\}$. Da je (**Z**,+, •) prsten glavnih ideala se vidi što je oblika $(a) = \{\dots, -2k, -k, 0, k, 2k, \dots\}$ te provjerom svojstava ideala:

1) za $ra, rs\ \in (a)$ uvijek vrijedi $ra - rs = (r - s)a\ \in (a)$,

2) za $ra\ \in (a)$ i bilo koji $s\ \in R$ vrijedi $s(ra) = (sr)a\ \in R$.

Zadatak 8.

Odredite parametre a, b, c takve da polinom $p(x) = x^6 + ax^4 + bx^3 + cx^2 + x + 1$ bude inverz polinoma $q(x) = x^3 + 1$ u polju F_{2^8} reprezentiranom kao $Z_2[t]/(h(t))$, gdje je $h(t) = t^8 + t^4 + t^3 + t + 1$ polinom ireducibilan nad Z_2.

Zadatak 9.
Alice je poslala istu poruku *m* nekolicini 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

$$n_1 = 39, \quad c_1 = 5,$$
$$n_2 = 85, \quad c_2 = 10,$$
$$n_3 = 77, \quad c_3 = 69$$

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

Sustav: x ≡ 5 (mod 39) , x ≡ 10 (mod 85), x ≡ 69 (mod 77).

m = $m_1 \times m_2 \times m_3 = 39 \times 85 \times 77 = 255255$

$n_1 = \frac{m}{m_1} = 6545, \;\; n_2 = \frac{m}{m_2} = 3003, \;\; n_3 = \frac{m}{m_3} = 3315.$

1) $6545x_1 \equiv 5 \pmod{39}$

$32x_1 \equiv 5 \pmod{39}$

39 = 32×1 + 7
32 = 7×4 + 4
7 = 4×1 + 3
4 = 3×1 + 1

$y_i = y_{i-2} - q_i \times y_{i-1}$

i	-1	0	1	2	3	4
q_i			1	4	1	1
y_i	0	1	-1	5	-6	11

$x_1 \equiv 11 \times 5 \pmod{39} \;\; \rightarrow \;\; x_1 \equiv 55 \pmod{39} \;\; \rightarrow \;\; \underline{x_1 \equiv 16 \pmod{39}}$

2) $3003x_2 \equiv 10 \pmod{85}$

$28x_2 \equiv 10 \pmod{85}$

85 = 28×3 + 1

i	-1	0	1
q_i			3
y_i	0	1	-3

$x_2 \equiv (-3) \times 10 \pmod{85} \;\; \rightarrow \;\; x_2 \equiv -30 \pmod{85} \;\; \rightarrow \;\; \underline{x_2 \equiv 55 \pmod{85}}$

3) $3315x_3 \equiv 69 \pmod{77}$

$4x_3 \equiv 69 \pmod{77}$

77 = 4×19 + 1

i	-1	0	1
q_i			19
y_i	0	1	-19

$x_3 \equiv (-19)\times 69 \pmod{77} \rightarrow x_3 \equiv -1311 \pmod{77} \rightarrow \underline{x_3 \equiv 75 \pmod{77}}$

$x_0 = n_1x_1 + n_2x_2 + n_3x_3 = 518510$

$x \equiv x_0 \pmod{m}$

$x \equiv 518510 \pmod{255255}$

$x \equiv 8000 \pmod{255255}$

Poruka M : $M = \sqrt[3]{8000} = 20$