1. PELLOVA JEDNADŽBA

$$x^2 - y^2 d = 1$$

- d nije potpun kvadrat ($\sqrt{d}$ nije element iz N)
- TRIVIJALNA RJEŠENJA: $x_0=1$, $y_0=0$
- FUNDAMENTALNA RJEŠENJA: x_1 i y_1

METODE NALAŽENJA FUNDAMENTALNOG RJEŠENJA:

- pogađanje
- korištenje verižnog razlomka

NALAŽENJE FUNDAMENTALNOG RJEŠENJA KORIŠTENJEM VERIŽNOG RAZLOMKA:

Neka je L duljina perioda ponavljanja istih a-ova u verižnom razlomku.

Npr. $[5; \overline{2, 1, 1, 2, 10}]$ - ovdje je period 5.

L je paran:

$x^2 - y^2 d = -1$ *nema rješenja*

$x^2 - y^2 d = 1$ *ima rješenja*

$x_n = p_{nL-1}$

$y_n = q_{nL-1}$

L je neparan:

$x^2 - y^2 d = -1$ *ima rješenja*

$x_n = p_{(2n-1)L-1}$

$y_n = q_{(2n-1)L-1}$

$x^2 - y^2 d = 1$ *ima rješenja*

$x_n = p_{2nL-1}$

$y_n = q_{2nL-1}$

RAČUNANJE p I q:

$p_{-2} = 0$, $p_{-1}=1$, $p_0=a_0$ $\quad p_{n+2} = a_{n+2}p_{n+1} + p_n$ $\quad q_{-2}=1$, $q_{-1}=0$, $q_0=1$ $\quad q_{n+2}=a_{n+2}q_{n+1}+q_n$

VERIŽNI RAZLOMAK:

Ako imamo broj oblika α:

$$a_0 = \lfloor \alpha \rfloor, \quad \alpha = a_0 + \frac{1}{\alpha_1}, \quad a_1 = \lfloor \alpha_1 \rfloor, \quad \alpha_1 = a_1 + \frac{1}{\alpha_2}, \quad a_2 = \lfloor \alpha_2 \rfloor, \ldots.$$

Ako imamo broj oblika $\frac{s_0 + \sqrt{d}}{t_0}$:

$$a_0 = \lfloor \sqrt{d} \rfloor \qquad a_i = \left\lfloor \frac{s_i + a_0}{t_i} \right\rfloor, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}$$

2. GRUPE

Polugrupa (G,*) zadovoljava:

- zatvorenost: a,b ε G ➔ a * b ε G
- asocijativnost: (a*b)*c = a*(b*c) a,b,c ε G

Monoid je polugrupa (G,*) koja ima neutralni element:

- a * e = e * a = a

Grupa je monoid (G,*) koji ima inverz svakog elementa u skupu G:

- $a * a^{-1} = a^{-1} * a = e$ a^{-1} ε G

Abelova grupa je grupa (G,*) na kojoj vrijedi komutativnost:

- a * b = b * a a,b ε G

ALGORITAM ZA DOKAZIVANJE DA JE NAD NEKIM SKUPOM ZA ZADANU OPERACIJU FORMIRANA GRUPA:

- dokazati zatvorenost, asocijativnost, postojanje neutralnog elementa i postojanje inverza za svaki element (Za dokaz Abelove grupe još dokazati i komutativnost)

ALGORITAM ZA DOKAZIVANJE DA JE NEKA FUNKCIJA HOMOMORFIZAM:

- provjeriti iz definicije je li funkcija homomorfizam

  Npr. Imamo grupe (G , **op_1**) i (H , **op_2**) - tada je funkcija f:G ➔ H za koju vrijedi f(x **op_1** y) = f(x) **op_2** f(y) homoformizam.

- Provjeriti kakva je ta funkcija - ako je injekcija onda je monomorfizam, ako je surjekcija onda je epimorfizam i ako je bijekcija, onda je izomorfizam.

RED ELEMENTA je broj elemenata skupa koji su generirani uzastopnom primjenom operacije nad tim elementom.

Npr. Imamo grupu (Z_5, +).

Tada gledamo: 1 = 1

1+1= 2

1+1+1=3

1+1+1+1=4

1+1+1+1+1=0

Skup koji 1 generira je {0,1,2,3,4} pa je njegov red 5.

CIKLIČKA GRUPA JE GENERIRANA SAMO JEDNIM ELEMENTOM. (Z_5, +) je ciklička grupa jer se može generirati samo jednim elementom (1).

KAD IMAMO GRUPU (Z_M, ⊙) gdje je M modul, a ⊙ operacija, red te grupe je φ(M) (Euler).

ZA NORMALNU PODGRUPU (Y, *) VRIJEDI Yx = xY za svaki x iz nadgrupe (X, *)

3. PRSTENI I POLJA

(R, +, *) je prsten ako:

- (R,+) čini abelovu grupu
- (R, *) čini polugrupu
- vrijedi distributivnost

HOMOMORFIZAM PRSTENA JE FUNKCIJA f: Prsten1 ➔ Prsten2 za koju vrijedi:

f(x + y) = f(x) + f(y) i f(x * y) = f(x) * f(y)

IDEAL PRSTENA JE ZA PRSTEN ISTO ŠTO I NORMALNA PODGRUPA ZA GRUPU

INTEGRALNA DOMENA je prsten gdje nema djelitelja nule. X je djelitelj nule ako pomnožen sa Y daje 0, a X i Y nisu 0.

Z_m postaje integralna domena kad je m prost.

POLJE je prsten za kojeg je (R, +) abelova grupa i (R, *) abelova grupa.

ALGORITAM ZA DOKAZIVANJE POLJA:

- pokazati zatvorenost za razliku dva elementa (time se dokaže da je (R,+) abelova grupa)
- pokazati zatvorenost za umnožak dva elementa (time se dokaže da je (R, *) abelova grupa)

Primjer:

Dokažimo da brojevi oblika $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$, *čine polje.*

Rješenje: Označimo sa $P = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, te uzmimo $a + b\sqrt{2}$, $c + d\sqrt{2} \in P$. Iz

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in P$$

slijedi da je $(P, +)$ abelova grupa.

Pretpostavimo sada da je $c + d\sqrt{2} \neq 0$. Tada je

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2})^{-1} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2} \in P$$