Kriptografija
Zbirka rešenih zadataka

Anja Bukurov

maj 2022.

Ovaj materijal predstavlja skriptu za izborni kurs "Kriptografija", na master studijama na Matematičkom fakultetu Univerziteta u Beogradu. Skripta je koncipirana na osnovu beleški sa časova vežbi u akademskoj 2020/2021. godini. Skripta sadrži kombinovane materijale iz prethodnih akademskih godina i teorijsku osnovu koja prati skriptu prof. dr Miodraga Živkovića[1].

Kao i svaki nerecenzirani materijal ovog tipa, i ovaj tekst je podložan propustima u njegovom pripremanju. Ukoliko uočite bilo kakvu grešku, možete se javiti putem elektronske pošte na adresu `anja_bukurov@matf.bg.ac.rs`. Potrebno je da u naslovu elektronske poruke stavite tekst "`[KG] Skripta`". Svi komentari, sugestije, kritike, ali i pohvale vezane za ovaj materijal su dobrodošli.

[1] http://poincare.matf.bg.ac.rs/~ezivkovm/

Sadržaj

1 Uvodni zadaci

Zadatak 1.1 *Dokazati da* $6 \mid m(m^2+5)$ *važi za proizvoljan prirodan broj* m.

Rešenje: Dokaz ćemo izvesti matematičkom indukcijom.

Baza indukcije: Za $m = 1$ izraz $m(m^2+5)$ jednak je 6, što je deljivo sa 6.

Induktivna hipoteza: Pretpostavimo da za $m \geq 1$ važi $6 \mid m(m^2+5)$.

Induktivni korak: Treba dokazati da važi $6 \mid (m+1)((m+1)^2+5)$.

$$\begin{aligned}
&(m+1)((m+1)^2+5) = \\
&(m+1)(m^2+2m+6) = \\
&m(m^2+5)+m(2m+1)+m^2+2m+6 = \\
&m(m^2+5)+3m^2+3m+6 = \\
&m(m^2+5)+3(m(m+1)+2)
\end{aligned}$$

Na osnovu induktivne hipoteze, prvi sabirak je deljiv brojem 6 te ostaje da proverimo da li je drugi sabirak deljiv sa 6. Da bi broj bio deljiv brojem 6 znamo da on mora biti deljiv brojevima 2 i 3. Drugi sabirak je uvek deljiv brojem 3 jer predstavlja umnožak broja 3. Na kraju, proveravamo da li važi $2 \mid (m(m+1)+2)$, odnosno $2 \mid m(m+1)$. Pošto su u pitanju dva uzastopna broja jedan od njih će sigurno biti paran, a samim tim i deljiv brojem 2. Pošto je i drugi sabirak deljiv brojevima 2 i 3, odnosno brojem 6, zaključujemo da je izraz deljiv brojem 6 što je trebalo pokazati.

■

Drugi način je da izraz $m(m^2+5)$ transformišemo na sledeći način:

$$\begin{aligned}
&m(m^2+5) = m^3 - m + 6m = \\
&m(m^2-1)+6m = m(m-1)(m+1)+6m
\end{aligned}$$

Slično kao u prethodnom dokazu, posmatraćemo pojedinačne sabirke. Drugi sabirak je uvek deljiv brojem 6 jer predstavlja umnožak broja 6. Prvi sabirak predstavlja proizvod tri uzastopna broja. Jedan od tri broja mora biti deljiv brojem 3. Takođe, među ovim brojevima se mora naći makar jedan paran broj, pa je prvi sabirak deljiv i brojem 2, a samim tim i brojem 6. Kako su oba sabirka deljiva brojem 6 onda je i zbir deljiv brojem 6 što je trebalo pokazati.

■

Zadatak 1.2 *Dokazati da* $30 \mid m^5 - m$ *važi za proizvoljan prirodan broj* m.

Rešenje: Izraz $m^5 - m$ ćemo transformisati na sledeći način:

$$m^5 - m = m(m^4-1) = m(m-1)(m+1)(m^2+1)$$

Da bi smo pokazali da je izraz deljiv brojem 30 dovoljno je da pokažemo da je deljiv brojevima 5 i 6. Izraz je deljiv brojem 6 jer sadrži proizvod tri uzastopna broja, što je objašnjeno u prethodnom zadatku. Ostaje da pokažemo da važi $5 \mid m(m-1)(m+1)(m^2+1)$.

Broj m možemo zapisati kao $m = 5k \pm r$, za $r \in \{0, 1, 2\}$

- Ako je $r = 0$ onda je $m = 5k$. Pošto je broj m deljiv brojem 5, ceo izraz je deljiv brojem 5.
- Ako je $r = \pm 1$ onda je $m = 5k \pm 1$. Jedan od brojeva $m - 1$ i $m + 1$ deljiv je brojem 5 pa je i ceo izraz je deljiv brojem 5.
- Ako je $r = \pm 2$ onda je $m = 5k \pm 2$. Broj $m^2 + 1$ ima vrednost $25k^2 \pm 10k + 5$ što je deljivo brojem 5 pa je i ceo izraz je deljiv brojem 5.

Pošto je izraz deljiv sa 5 za sve oblike broja m, pokazali smo da je izraz deljiv brojem 5 za proizvoljan prirodan broj m čime smo dokazali da je izraz deljiv brojem 30.

■

Zadatak 1.3 *Dokazati da* $30 \mid mn(m^4 - n^4)$ *važi za proizvoljne prirodne brojeve* m *i* n.

Rešenje: Izraz $mn(m^4 - n^4)$ ćemo transformisati na sledeći način:

$$mn(m^4 - n^4) = m^5n - mn^5 + mn - mn = n(m^5 - m) - m(n^5 - n)$$

Izraz je deljiv brojem 30 ukoliko su umanjenik i umanjilac deljivi brojem 30. Prema dokazu iz prethodnog zadatka, oba broja jesu deljiva brojem 30 pa je i ceo izraz deljiv brojem 30 što je trebalo pokazati.

■

Zadatak 1.4 *Dokatati da* $42 \mid m^7 - m$ *važi za proizvoljan prirodan broj* m.

Rešenje: Izraz $m^7 - m$ ćemo transformisati na sledeći način:

$$m^7 - m = m(m^6 - 1) = m(m^3 - 1)(m^3 + 1) =$$
$$m(m - 1)(m + 1)(m^2 + m + 1)(m^2 - m + 1)$$

Da bismo pokazali da je izraz deljiv brojem 42, proverićemo deljivost izraza brojevima 6 i 7. Izraz je deljiv brojem 6 jer sadrži proizvod tri uzastopna broja. Ostaje da proverimo da li je izraz deljiv brojem 7. Broj m možemo zapisati kao $m = 7k \pm r$ za $r \in \{0, 1, 2, 3\}$.

- Ako je $r = 0$ onda je $m = 7k$. Pošto je broj m deljiv brojem 7, ceo izraz je deljiv brojem 7.
- Ako je $r = \pm 1$ onda je $m = 7k \pm 1$. Jedan od brojeva $m - 1$ i $m + 1$ deljiv je brojem 7 pa je i ceo izraz deljiv brojem 7.
- $r = \pm 2$ onda je $m = 7k \pm 2$. Proizvod $(m^2 + m + 1)(m^2 - m + 1)$ možemo zapisati kao $m^4 + m^2 + 1$. Ostatak pri deljenju m^4 sa 7 je 2, ostatak pri deljenju m^2 sa 7 je 4 i slobodan član je 1. Ostaci u zbiru daju 7 iz čega se može zaključiti da je izraz deljiv brojem 7.
- $r = \pm 3$ onda je $m = 7k \pm 2$. Ostatak pri deljenju m^4 sa 7 je 4, ostatak pri deljenju m^2 sa 7 je 2 i slobodan član je 1. Ostaci u zbiru daju 7 iz čega se može zaključiti da je izraz deljiv brojem 7.

Pošto je izraz deljiv sa 7 za sve oblike broja m, pokazali smo da je izraz deljiv brojem 7 za proizvoljan prirodan broj m čime smo dokazali da je izraz deljiv brojem 42.

■

Zadatak 1.5 *Dokazati da* $2^m \mid (m+1)(m+2)\cdot\ldots\cdot(m+m)$ *važi za proizvoljan prirodan broj* m.

Rešenje: Izraz $(m+1)(m+2)\ldots(m+m)$ ćemo transformisati u $\frac{(2m)!}{m!}$. Dokaz ćemo izvesti matematičkom indukcijom.

Baza indukcije: Za m = 1 izraz $\frac{(2m)!}{m!}$ ima vrednost 2, što je deljivo sa $2^1 = 2$.

Induktivna hipoteza: Pretpostavimo da za $m \geq 1$ važi $2^m \mid \frac{(2m)!}{m!}$.

Induktivni korak: Treba dokazati da važi $2^{m+1} \mid \frac{(2(m+1))!}{(m+1)!}$

$$\frac{(2(m+1))!}{(m+1)!} = \frac{(2m)!\cdot(2m+1)\cdot 2\cancel{(m+1)}}{m!\cdot\cancel{(m+1)}} = \frac{(2m)!}{m!}\cdot 2(2m+1)$$

Prema induktivnoj hipotezi, 2^m deli $\frac{(2m)!}{m!}$ i $2(2m+1)$ je deljivo brojem 2 pa je ceo izraz deljiv sa 2^{m+1} što je trebalo pokazati.

■

Zadatak 1.6 *Dokazati da je broj deljiv brojem 3 akko mu je zbir cifara deljiv brojem 3.*

Rešenje: Neka su brojevi $a_0, a_1, \ldots, a_m$ cifre broja n, pri čemu je cifra a_0 cifra jedinica. Onda broj n možemo zapisati kao

$$\sum_{k=0}^{m} a_k \cdot 10^k,$$

dok zbir sifara zapisujemo kao

$$\sum_{k=0}^{m} a_k.$$

Dovoljno je da pokažemo da je razlika broja i sume njegovih cifara deljiva brojem 3 da bismo pokazali tvrđenje:

$$\sum_{k=0}^{m} a_k \cdot 10^k - \sum_{k=0}^{m} a_k = \sum_{k=0}^{m} a_k \cdot (10^k - 1) =$$

$$0 + \underbrace{(10-1)}_{=9}\cdot a_1 + \underbrace{(100-1)}_{=99}\cdot a_2 + \underbrace{(10^m - 1)}_{=\underbrace{99..99}_{m-1}}\cdot a_m = 9 \cdot \sum_{k=0}^{m-1} 10^k \cdot a_k$$

Pošto svaki od sabiraka sadrži umnožak broja 9 početni izraz je deljiv brojem 3.

■

Zadatak 1.7 *Dokazati da je $NZD(a+b, a-b) \leq 2$ ukoliko su a i b uzajamno prosti brojevi.*

Rešenje: Neka je $k = NZD(a+b, a-b)$. To znači da broj k deli $a+b$ i $a-b$. Takođe, važi da k deli zbir i razliku ovih brojeva:

$$k \mid ((a+b)+(a-b)) \ \wedge \ k \mid ((a+b)-(a-b)) \implies k \mid 2a \ \wedge \ k \mid 2b$$

Pošto su a i b uzajamno prosti brojevi, onda važi $NZD(a,b) = 1$. Broj 1 možemo zapisati kao linearnu kombinaciju brojeva a i b:

$$1 = m \cdot a + n \cdot b$$

Broj k deli $2a$ i $2b$ pa deli i njihove umnoške $2a \cdot m$ i $2b \cdot n$, kao i zbir tih umnožaka:

$$2a \cdot m + 2b \cdot n = 2(\underbrace{m \cdot a + n \cdot b}_{=1}) = 2$$

Vrednost izraza koji k deli jednaka je 2 iz čeka zaključujemo da k ne može biti veće od 2 odnosno da važi $NZD(a+b, a-b) \leq 2$ što je trebalo pokazati.

■

Zadatak 1.8 *Dokazati da zbir kvadrata pet uzastopnih celih brojeva ne može biti potpuni kvadrat.*

Rešenje: Pretpostavimo suprtono - zbir kvadrata pet uzastopnih celih brojeva je potpuni kvadrat. Zbir kvadrata pet uzastopnih celih brojeva možemo zapisati na sledeći način:

$$a_1^2 + a_2^2 + a_3^2 + a_3^2 + a_4^2 + a_5^2 = (n-2)^2 + (n-1)^2 + n^2 + (n+1)^2 + (n+2)^2 = 5n^2 + 10 = 5(n^2+2)$$

Da bi broj bio poptun kvadrat, svaki faktor treba da bude stepenovan na paran broj. Stoga zaključujemo da broj (n^2+2) mora biti deljiv brojem 5 da bi suma bila potpun kvadrat. Da bismo to proverili, prestavićemo broj n kao $5k \pm r$, $k \in \mathbb{Z}$, $r \in \{0,1,2\}$

- $r = 0$: $n = 5k \longrightarrow (n^2+2) = 25k^2 + 2$ ↯
- $r = 1$: $n = 5k \pm 1 \longrightarrow (n^2+2) = 25k^2 \pm 10k + 3$ ↯
- $r = 2$: $n = 5k \pm 2 \longrightarrow (n^2+2) = 25k^2 \pm 20k + 6$ ↯

Kako ni u jednom slučaju broj 5 ne deli n^2+2, pokazali smo suprotno od pretpostavke odnosno da zbir kvadrata pet uzastopnih celih brojeva ne može biti potpuni kvadrat.

■

Zadatak 1.9 *Koliko činilaca ima broj 945?*

Rešenje: Prema osnovnoj teoremi aritmetike, u skupu $\mathbb{Z}$, svaki ceo broj veći od 1 može se na jedinstven način predstaviti kao proizvod prostih brojeva:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

pri čemu su α_i pozitivni celi brojevi. Svi pozitivni delioci su oblika $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}$, za $0 \leq \beta_i \leq \alpha_i$, $i \in \{1, 2, \ldots, k\}$. Za svako α_i ima $\alpha_i + 1$ različitih vrednosti koje se dobijaju računanjem $p_i^{\alpha_i}$. Prema tome, ukupan broj različitih delilaca broja n jednak je $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$. Primenimo to na rešavanje ovog zadatka. Broj 945 razlažemo na proste činioce:

$$945 = 3^3 \cdot 5 \cdot 7$$

Vrednosti stepenova su $\alpha_1 = 3, \alpha_2 = \alpha_3 = 1$. Na osnovu toga, broj činioca je $4 \cdot 2 \cdot 2 = 16$.

1.1 Zadaci za vežbu

Zadatak 1.10 *Dokazati da* $24 \mid (p^2 - q^2)$ *važi za proste brojeve* $p, q \geq 5$.

Zadatak 1.11 *Dokazati da je broj deljiv brojem 11 ukoliko je razlika sume cifara na parnim pozicijama i sume cifara na neparnim pozicijama deljiva sa 11.*

Zadatak 1.12 *Ako su a i b uzajamno prosti prirodni brojevi i ako je* $a \cdot b$ *kvadrat prirodnog broja, pokazati da su i a i b kvadrati prirodnih brojeva.*

Zadatak 1.13 *Koliko činilaca ima broj 2499?*

2 Euklidov algoritam

Najveći zajednički delilac dva cela broja a i b je najveći ceo broj koji deli i broj a i broj b. Euklidov algoritam je tehnika efikasnog pronalaženja NZD-a dva cela broja. Algoritam prati sledeće korake:

- Ako je $a = 0$, onda je $NZD(a, b) = b$ jer je $NZD(0, b) = b$ i postupak se završava.
- Ako je $b = 0$, onda je $NZD(a, b) = a$ jer je $NZD(a, 0) = a$ i postupak se završava.
- Ako su $a, b > 0$, onda broj a predstavljamo preko broja b, odgovarajućeg količnika i ostatka pri deljenju broja a brojem b:

  $$a = q \cdot b + r$$

  Zatim ponoviti postupak za brojeve b i r.

Postupak se ponavlja dok se ne dođe do ostatka koji je jednak 0 (na osnovu prva dva koraka). Najveći zajednički delilac predstavlja poslednji ostatak koji nije jednak 0, odnosno ostatak iz pretposlednjeg koraka.

Dobijeni NZD može se predstaviti kao linearna kombinacija brojeva a i b. Polazi se od poslednje jednačine u kojoj je ostatak nije jednak 0 (odnosno od jednačine koja sadrži NZD). Ostatak se predstavlja kao razlika preostalih brojeva, a postupak se ponavlja dok se dođe do prve jednačine koja sadrži brojeve a i b.

Zadatak 2.1 *Izračunati najveći zajednički delilac datih brojeva, a zatim nzd predstaviti kao linearnu kombinaciju tih brojeva:*

a) 549 i 387

b) 589 i 343

Rešenje: Za svaki par brojeva primenićemo Eukidov algoritam.

a) $NZD(549, 387)$

$$\begin{aligned}
549 &= 1 \cdot 387 + 162 \\
387 &= 2 \cdot 162 + 63 \\
162 &= 2 \cdot 63 + 36 \\
63 &= 1 \cdot 36 + 27 \\
36 &= 1 \cdot 27 + \underline{9} \\
27 &= 3 \cdot 9 + 0
\end{aligned}$$

NZD je poslednji ostatak različit od 0. U ovom slučaju to je broj 9. Broj 9 sada predstavljamo kao linearnu kombinaciju brojeva 549 i 387:

$$\begin{aligned}
9 &= 36 - 1 \cdot 27 \\
&= 36 - 1 \cdot (63 - 1 \cdot 36) \\
&= -1 \cdot 63 + 2 \cdot (162 - 2 \cdot 63) \\
&= 2 \cdot 162 - 5 \cdot (387 - 2 \cdot 162) \\
&= -5 \cdot 387 + 12 \cdot (549 - 1 \cdot 387) \\
&= 12 \cdot 549 - 17 \cdot 387
\end{aligned}$$

b) $NZD(589, 343)$

$$\begin{aligned}
589 &= 1 \cdot 343 + 246 \\
343 &= 1 \cdot 246 + 97 \\
246 &= 2 \cdot 97 + 52 \\
97 &= 1 \cdot 52 + 45 \\
52 &= 1 \cdot 45 + 7 \\
45 &= 6 \cdot 7 + 3 \\
7 &= 2 \cdot 3 + \underline{1} \\
3 &= 3 \cdot 1 + 0
\end{aligned}$$

Dakle, $NZD(589, 343) = 1$ odnosno, ovi brojevi su uzajamno prosti. Predstavimo NZD kao linearnu kombinaciju brojeva 589 i 343:

$$\begin{aligned}
1 &= 7 - 2 \cdot 3 \\
&= 7 - 2 \cdot (45 - 6 \cdot 7) \\
&= -2 \cdot 45 + 13 \cdot (52 - 45) \\
&= 13 \cdot 52 - 15 \cdot (97 - 52) \\
&= -15 \cdot 97 + 28 \cdot (246 - 2 \cdot 97) \\
&= 28 \cdot 246 - 71 \cdot (343 - 246) \\
&= -71 \cdot 343 + 99 \cdot (589 - 343) \\
&= 99 \cdot 589 - 170 \cdot 343
\end{aligned}$$

2.1 Multiplikativni inverz

Euklidov algoritam može da se iskoristi za računanje inverza broja po modulu. Ukoliko je potrebno izračunati $b^{-1}(mod\ a)$, potrebno je da proverimo da li su brojevi a i b uzajamno prosti odnosno odredimo $NZD(a, b)$. Ukoliko $NZD(a, b)$ nije jednak broju 1, broj b nije invertibilan po modulu a. Ukoliko $NZD(a, b)$ jeste jednak broju 1, određujemo linearnu kombinaciju brojeva a i b. Ako je

$$NZD(a, b) = m \cdot a + n \cdot b = 1,$$

onda važi da je

$$b^{-1}(mod\ a) = n.$$

Zadatak 2.2 *Izračunati:*

a) $160^{-1}(mod\ 841)$

b) $27^{-1}(mod\ 256)$

Rešenje:

a) Prvi korak je da proverimo da li su brojevi uzajamno prosti. To ćemo uraditi

$$\begin{aligned} 841 &= 5 \cdot 160 + 41 \\ 160 &= 3 \cdot 41 + 37 \\ 41 &= 37 + 4 \\ 37 &= 9 \cdot 4 + \underline{1} \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

Pošto je $NZD(841, 160) = 1$, možemo da odredimo inverz. Za to je potrebno predstaviti broj 1 kao linearnu kombinaciju brojeva 841 i 160:

$$\begin{aligned} 1 &= 37 - 9 \cdot 4 \\ &= 37 - 9 \cdot (41 - 37) \\ &= -9 \cdot 41 + 10 \cdot (160 - 3 \cdot 41) \\ &= 10 \cdot 160 - 39 \cdot (840 - 5 \cdot 160) \\ &= -39 \cdot 840 + \underline{205} \cdot 160 \end{aligned}$$

Dakle, $160^{-1}(mod\ 841) = 205$. Možemo se uveriti u to tako što ćemo pomnožiti brojeve 160 i 205 po modulu 841. Ukoliko smo ispravno izračunali inverz, vrednost tog proizvoda treba da bude 1.

$$160 \cdot 205 = 32800 \equiv 1(mod\ 841).$$

b) $27^{-1}(mod\ 256)$

$$\begin{aligned} 256 &= 9 \cdot 27 + 13 \\ 27 &= 2 \cdot 13 + \underline{1} \\ 13 &= 13 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 27 - 2 \cdot 13 \\ &= 27 - 2 \cdot (256 - 9 \cdot 27) \\ &= -2 \cdot 256 + \underline{19} \cdot 27 \end{aligned}$$

Dakle, $27^{-1}(mod\ 256) = 19(mod\ 256)$.

2.2 Rešavanje jednačina

Zadatak 2.3 *Odraditi sva celobrojna rešenja jednačine* $53x + 47y = 1$.

Rešenje: Prvi korak u rešavanju ove jednačine jeste određivanje $NZD(53, 47)$ i linearni kombinacije brojeva 53 i 47.

$$\begin{aligned} 53 &= 47 + 6 \\ 47 &= 7 \cdot 6 + 5 \\ 6 &= 1 \cdot 5 + \underline{1} \end{aligned}$$

$$\begin{aligned} 1 &= 6 - 5 \\ &= 6 - (47 - 7 \cdot 6) \\ &= -47 + 8 \cdot (53 - 47) \\ &= 8 \cdot 53 - 9 \cdot 47 \end{aligned}$$

Na osnovu linearne kombinacije dobijamo jedno rešenje jednačine: $x = 8, y = -9$. Da bismo odredili sva rešenja, dobijenu jednačinu oduzećemo od početne:

$$\begin{aligned} 53(x - 8) + 47(y + 9) &= 0 \\ 53(x - 8) &= -47(y + 9) \end{aligned}$$

Kako su 53 i 47 uzajamno prosti brojevi, to znači da postoji $k \in \mathbb{Z}$ tako da važi:

$$x = 8 + 47k$$
$$y = -9 - 53k$$

što je rešenje početke jednačine.

Zadatak 2.4 *Odraditi sva celobrojna rešenja jednačine* $22x + 32y = 18$.

Rešenje: Na početku primećujemo da se jednačina može skratiti brojem 2 pa je jendačina koju rešavamo:

$$11x + 16y = 9$$

Rešavanje ćemo početi na isti način kao u prethodnom zadatku - određivanjem NZD-a i linearne kombinacije.

$$\begin{aligned} 16 &= 11 + 5 \\ 11 &= 2 \cdot 5 + \underline{1} \end{aligned}$$

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 11 - 2 \cdot (16 - 11) \\ &= -2 \cdot 16 + 3 \cdot 11 \end{aligned}$$

U početnoj jednačini se sa desne strane nalazi broj 9 pa ćemo dobijenu linearnu kombinaciju pomnožiti baš tim brojem, a zatim i oduzeti od početne:

$$11(x - 27) + 16(y + 18) = 0$$
$$11(x - 27) = -16(y + 18)$$

Kako su 11 i 16 uzajamno prosti brojevi, to znači da postoji $k \in \mathbb{Z}$ tako da važi:

$$x = 27 + 16k$$
$$y = -18 - 11k$$

2.3 Rešavanje kongruencija

Neka je data kongruencija $ax \equiv b(mod\ m)$. Potrebno je pronaći x za koje važi data kongruencija. To se radi po sledećim pravilima:

1. Ako je $NZD(a, m) = 1$, onda je $x \equiv a^{-1}b(mod\ m)$, a rešenje su brojevi oblika:

$$x = a^{-1}b + km, k \in \mathbb{Z}$$

2. Ako je $NZD(a, m) = g(> 1)$, onda se broj a ne može invertovati po modulu m i razlikujemo dva slučaja:

   2.1. $g \mid b$ - kongruenciju delimo brojem g i dobijamo:

$$\frac{a}{g}x \equiv \frac{b}{g}\Big(mod \quad \frac{m}{g}\Big).$$

   Sada imamo brojeve koji su uzajamno prosti i postupak se nastavlja korakom pod 1 pa je rešenje oblika:

$$x = \Big(\frac{a}{g}\Big)^{-1}\frac{b}{g} + k\frac{m}{g}, k \in \mathbb{Z}$$

   2.2. $g \nmid b$ - kongruencija nema rešenja.

Zadatak 2.5 *Odrediti sve rešenja kongruencija:*

a) $3x \equiv 4(mod\ 7)$

b) $3x \equiv 4(mod\ 12)$

c) $9x \equiv 12(mod\ 21)$

d) $27x \equiv 25(mod\ 256)$

Rešenje:

a) $3x \equiv 4(mod\ 7)$

Pošto je $NZD(3,7) = 1$, u pitanju je prvo pravilo. Potrebno je da odredimo inverz broja 3 po modulu 7. Kako je $1 = 7 - 2 \cdot 3$, važi da je $3^{-1}(mod\ 7) = 2$, a rešenje kongruencije je oblika

$$x = 2 \cdot 4 + 7k = 6 + 7k = -1 + 7k, k \in \mathbb{Z}$$

b) $3x \equiv 4(mod\ 12)$

$NZD(3,12) = 3$ zbog čega se kongruencija rešava po drugom pravilu. Pošto $3 \nmid 4$, zaključujemo da kongruencija *nema rešenja.*

c) $9x \equiv 12(mod\ 21)$

$NZD(9,21) = 3$ zbog čega se kongruencija rešava po drugom pravilu. Pošto $3 \mid 12$, kongruenciju delimo brojem 3 i dobijamo

$$3x \equiv 4(mod\ 7)$$

što je kongruencija iz dela zadatka pod a). Rešenje kongruencije je oblika

$$x = -1 + 7k, k \in \mathbb{Z}$$

d) $27x \equiv 25(mod\ 256)$

U zadatku 2.2, u delu pod b), odredili smo da je $NZD(256,27) = 1$ i izračunali inverz broja 27 po modulu i dobili vrednost 19. Rešenje kongruencije, po prvom pravilu, je oblika:

$$x = 19 \cdot 25 + 256k = 475 + 256k = 219 + 256k = -37 + 256k, k \in \mathbb{Z}$$

2.4 Programi

Zadatak 2.6 *Napisati Python funkciju koja određuje najveći zajednički delilac dva cela pozitivna broja.*

Rešenje: Funkcija `gcd(a, b)` vraća vrednost najvećeg zajedničkog delioca brojeva a i b.

```
def gcd(a, b):
    if b == 0:
        return a
    return (b, a % b)
```

Zadatak 2.7 *Napisati Python funkciju koja određuje najveći zajednički delilac dva cela pozitivna broja i njihovu linearnu kombinaciju.*

Rešenje: Funkcija `extended_gcd(a, b)` vraća vrednost najvećeg zajedničkog delioca brojeva a i b kao i brojeve m i n iz jednačine

$$NZD(a, b) = m \cdot a + n \cdot b = 1,$$

```
def extended_gcd(a, b):
    if b == 0:
        return (a, 1, 0)
    d, m, n = extended_gcd(b, a % b)
    return (d, n, m - a // b * n)
```

Zadatak 2.8 *Napisati Python funkciju koja određuje multiplikativni inverz broja a po modulu x.*

Rešenje: Funkcija `mod_inv(a, x)` koristi funkciju `extended_gcd(a, b)` iz prethodnog zadatka čime se dobija vrednost NZD-a ova dva broja. Ukoliko su brojevi uzajamno prosti, inverz je broj m iz prethodne jednačine, u suprotnom, broj a nije invertibilan po modulu x.

```
def mod_inv(a, x):
    d, m, n = extended_gcd(a, x)
    if d != 1:
        print("Vrednosti a i x nisu uzajamno proste!")
    else:
        return m % x
```

2.5 Zadaci za vežbu

Zadatak 2.9 *Izračunati najveći zajednički delilac datih brojeva, a zatim nzd predstaviti kao linearnu kombinaciju tih brojeva:*

a) 12606 i 6494

b) 6188 i 4709

Zadatak 2.10 *Izračunati:*

a) $103^{-1}(mod\ 676)$

b) $3^{-1}(mod\ 100)$

Zadatak 2.11 *Odraditi sva celobrojna rešenja jednačine*

a) $21x + 27y = 15$

b) $13x + 59y = 1.$

Zadatak 2.12 *Odrediti sve rešenja kongruencija:*

a) $27x \equiv 72(mod\ 900)$

b) $103x \equiv 612(mod\ 676)$

c) $106x \equiv 108(mod\ 424)$

3 Ojlerova funkcija

Ojlerova funkcija, u oznaci $\varphi(n)$, određuje broj uzajamno prostih brojeva sa brojem n koji su manji od n. Vrednost $\varphi(n)$ određuje se na sledeći način:

- Ukoliko je p prost broj važe jednakosti:

$$\varphi(p) = p - 1$$
$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$

- Ukoliko je $n = p \cdot q$, pri čemu važi $NZD(p, q) = 1$ onda važi:

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$$

- Inače, treba izvršiti faktorizaciju broja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ i primeniti prethodne formule:

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \cdot \ldots \cdot p_k^{\alpha_k - 1}(p_k - 1) \\ &= \frac{n}{p_1 \cdot p_2 \cdot \ldots \cdot p_k} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1)\end{aligned}$$

Faktorizacija brojeva vrši se uzastopnim deljenjem prostim brojevima dok deljenik ne postane 1.

Zadatak 3.1 *Rastaviti na proste činioce brojeve 827998848 i 81057226635.*

Rešenje:

$$82798848 = 2^8 \cdot 323433 = 2^8 \cdot 3^5 \cdot 1331 = 2^7 \cdot 3^4 \cdot 11^3$$

$$\begin{aligned}81057226635 &= 3^3 \cdot 3002119505 = 3^3 \cdot 5 \cdot 600423901 \\ &= 3^3 \cdot 5 \cdot 7^3 \cdot 1750507 = 3^3 \cdot 5 \cdot 7^3 \cdot 11^2 \cdot 14467 \\ &= 3^3 \cdot 5 \cdot 11^2 \cdot 17 \cdot 851 = 3^3 \cdot 5 \cdot 11^2 \cdot 17 \cdot 23 \cdot 37\end{aligned}$$

Zadatak 3.2 *Rastaviti na proste činioce brojeve 10! i 15!.*

Rešenje:

$$10! = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 \cdot 7 \cdot 2^3 \cdot 3^2 \cdot 2 \cdot 5 = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$$
$$15! = 10! \cdot 11 \cdot 2^2 \cdot 3 \cdot 13 \cdot 2 \cdot 7 \cdot 3 \cdot 5 = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$$

Zadatak 3.3 *Odrediti $\varphi(n)$ za svako $n \in [90, 100]$.*

Rešenje:

$$\varphi(90) = \varphi(2 \cdot 3^2 \cdot 5) = \varphi(2) \cdot \varphi(3^2) \cdot 5 = 1 \cdot 3 \cdot 2 \cdot 4 = 24$$
$$\varphi(91) = \varphi(7) \cdot \varphi(13) = 6 \cdot 12 = 72$$
$$\varphi(92) = \varphi(2^2) \cdot \varphi(23) = 2 \cdot 22 = 44$$
$$\varphi(93) = \varphi(3) \cdot \varphi(31) = 2 \cdot 30 = 60$$
$$\varphi(94) = \varphi(2) \cdot \varphi(47) = 46$$
$$\varphi(95) = \varphi(5) \cdot \varphi(19) = 4 \cdot 18 = 72$$
$$\varphi(96) = \varphi(2^5) \cdot \varphi(3) = 16 \cdot 2 = 32$$
$$\varphi(97) = 96$$
$$\varphi(98) = \varphi(2) \cdot \varphi(7^2) = 42$$
$$\varphi(99) = \varphi(3^2) \cdot \varphi(11) = 6 \cdot 10 = 60$$
$$\varphi(100) = \varphi(2^2) \cdot \varphi(5^2) = 2 \cdot 20 = 40$$

Zadatak 3.4 *Odrediti $\varphi(n)$ za svako $n \in \{375, 720, 957\}$.*

Rešenje:

$$\varphi(375) = \varphi(3) \cdot \varphi(5^3) = 2 \cdot 100 = 200$$
$$\varphi(720) = \varphi(2^4) \cdot \varphi(3^2) \cdot \varphi(5) = 8 \cdot 6 \cdot 4 = 192$$
$$\varphi(957) = \varphi(3) \cdot \varphi(11) \cdot \varphi(29) = 2 \cdot 10 \cdot 28 = 560$$

Zadatak 3.5 *Dokazati da je je broj p prost ako i samo ako $\varphi(p) = p - 1$.*

Rešenje:
Smer $\Rightarrow$: Ako je broj prost, onda su svi brojevi manji od njega uzajamno prosti sa njim, a takvih brojeva ima $p - 1$ pa po definiciji Ojlerove funkcije važi $\varphi(p) = p - 1$.

Smer $\Leftarrow$: Ako važi da je $\varphi(p) = p - 1$, onda po definiciji Ojlerove funkcije važi da su svi brojevi manji od njega uzajamno prosti sa njim što znači da je broj p prost.

■

Zadatak 3.6 *Odrediti broj a ako je poznato da je $\varphi(a) = 120$, $a = p \cdot q$ i $p - q = 2$, pri čemu su p i q prosti brojevi.*

Rešenje: Na osnovu činjenice da su p i q prosti brojevi i prve dve jednakosti dobijamo jednačinu:

$$\begin{aligned}&\varphi(a) = 120\\&\varphi(p \cdot q) = 120\\&\varphi(p) \cdot \varphi(q) = 120\\&(p-1)(q-1) = 120\end{aligned}$$

Sada imamo sistem jednačina:

$$\begin{aligned}&(p-1)(q-1) = 120\\&p - q = 2 \longrightarrow p = q + 2\end{aligned}$$

Rešavanjem ovog sistema jednačina dobijamo da je $q = 11$, $p = 13$, i na kraju $a = 13 \cdot 11 = 143$.

3.1 Mala Fermaova teorema

Teorema 3.1 *Ako je p prost broj i $a \in \mathbb{Z}$ onda važi*

$$a^p \equiv a(mod\ p)$$

Dodatno, ako $p \mid a$ onda

$$a^{p-1} \equiv 1(mod\ p)$$

Opštije, $NZD(a, m) = 1$ onda

$$a^{\varphi(m)} \equiv 1(mod\ m)$$

Zadatak 3.7 *Izračunati vrednost ostataka:*

a) $2^{1000000}(mod\ 7)$

b) $3^{23645}(mod\ 35)$

Rešenje:

a) Brojevi 2 i 7 su uzajamno prosti i važi $\varphi(7) = 6$. Onda važi:

$$2^6(mod\ 7) \equiv 1(mod\ 7)$$

Sada možemo mnogo lakše da izračunamo ovu vrednost:

$$2^{1000000}(mod\ 7) \equiv (2^6)^{166666} \cdot 2^4(mod\ 7) \equiv 1^{166666} \cdot 16(mod\ 7) \equiv 2(mod\ 7)$$

b) Brojevi 3 i 35 su uzajamno prosti i važi $\varphi(35) = \varphi(5) \cdot \varphi(7) = 24$. Onda važi:

$$3^{24} \equiv 1(mod\ 35)$$

Sada možemo mnogo lakše da izračunamo ovu vrednost:

$$3^{23645}(mod\ 35) \equiv (3^{24})^{985} \cdot 3^5(mod\ 35) \equiv 1^{985} \cdot 243(mod\ 35) \equiv 33(mod\ 35)$$

3.2 Programi

Zadatak 3.8 *Napisati Python funkciju koja faktoriše broj na proste činioce.*

Rešenje: Funkcija `factorize(n)` vrši faktorizaciju broja uzastopnim deljenjem prostim brojevima sve dok deljenik ne postane 1. Kako deljenje polazi od manjih faktora ka većim dovoljno je iterirati kroz neparne brojeve kao moguće kandidate, jer u slučaju provere deljivosti sa nekim od složenih neparnih brojeva činioci tog neparnog složenog broja su već obrađeni pa tekući deljenik sigurno neće biti deljiv njime.

```
def factorize(n):
    if n <= 3:
        return [n]

    factors = []

    while n % 2 == 0:
        factors.append(2)
        n = n // 2

    i = 3
    while n > 1:
        if n % i == 0:
            factors.append(i)
            n = n // i
        else:
            i = i + 2

    return factors
```

Zadatak 3.9 *Napisati Python funkciju koja računa vrednost Ojlerove funkcije zadatog broja n.*

Rešenje: Funkcija `phi(n)` primenjuje formulu za računanje Ojlerove funkcije koju smo izveli na početku ove sekcije.

```
def phi(n):
    factors = set(factorize(n))
    res = 1

    for factor in factors:
        n = n // factor
        res = res * (factor - 1)

    return n * res
```

3.3 Zadaci za vežbu

Zadatak 3.10 *Rastaviti na proste činioce brojeve 159034225581 i 76432896.*

Zadatak 3.11 *Rastaviti na proste činioce brojeve 20! i 30!.*

Zadatak 3.12 *Odrediti $\varphi(n)$ za svako $n \in \{988, 1200, 4320, 16473\}$.*

4 Stepenovanje kvadriranjem

Ideja algoritma jeste da se stepen n može predstaviti kao zbir stepena broja 2. Na primer:

$$25 = 2^0 + 2^3 + 2^4 = (11001)_2$$

Vrednost a^n onda može da se pretvori u zapis sa dobijenim zbirom:

$$a^{25} = a^{2^0} + a^{2^3} + a^{2^4} = a^1 \cdot a^8 \cdot a^{16}.$$

Vrednost a^n jednaka je proizvodu brojeva a^{2^i} za svaku poziciju i na kojoj se nalazi jedinica. Vrednost stepena $a^{2^{i+1}}$ dobija se kao kvadrat prethodne vrednosti a^{2^i}:

$$\left(a^{2^i}\right)^2 = a^{2^i \cdot 2} = a^{2^{i+1}}$$

Zadatak 4.1 *Izračunati vrednost sledećih izraza:*

a) $57^{1616} (mod\ 97)$

b) $11^{1536} (mod\ 105)$

c) $43^{257} (mod\ 59)$

Rešenje:

a) Broj 97 je prost i $NZD(57, 97) = 1$ pa možemo primeniti Malu Fermaovu teoremu. Pored toga, iskoristićemo činjenicu da je $80 = 64 + 16$.

$$57^{1616} (mod\ 97) = 57^{96 \cdot 16} \cdot 57^{80} (mod\ 97) = 57^{80} (mod\ 97) = 57^{64} \cdot 57^{16} (mod\ 97)$$

Odredimo vrednosti 57^{2^i}, za $i \in [1, 6]$ po modulu 97:

$$57^2 \equiv 48 \qquad 57^{16} \equiv 91^2 \equiv (-6)^2 \equiv 36$$
$$57^4 \equiv 48^2 \equiv 73 \qquad 57^{32} \equiv 36^2 \equiv 35$$
$$57^8 \equiv 73^2 \equiv 91 \qquad 57^{64} \equiv 35^2 \equiv 61$$

Sada lako računamo vrednost izraza:

$$57^{1616} (mod\ 97) = 57^{64} \cdot 57^{16} (mod\ 97) = 61 \cdot 36 (mod\ 97) \equiv 62 (mod\ 97)$$

b) Važi da je $NZD(105, 11) = 1$ pa možemo primeniti Malu Fermaovu teoremu.

$$11^{1536} (mod\ 105) = 11^{48 \cdot 32} (mod\ 105) = 1 (mod\ 105)$$

Primenom Male Fermaove teoreme dobili smo broj 1 zbog čega nema razloga da primenjujemo algoritam stepenovanja.

c) Broj 59 je prost i $NZD(59, 43) = 1$ pa možemo primeniti Malu Fermaovu teoremu:

$$43^{257}(mod\ 59) = 43^{25}(mod\ 59) = 43^{16} \cdot 43^8 \cdot 43(mod\ 59)$$

Odredimo vrednosti 43^{2^i}, za $i \in [1, 4]$ po modulu 59:

$$43^2 \equiv 20 \qquad 43^8 \equiv 46^2 \equiv 51$$
$$43^4 \equiv 20^2 \equiv 46 \qquad 43^{16} \equiv 51^2 \equiv 5$$

Sada lako računamo vrednost početnog izraza:

$$43^{253}(mod\ 59) = 43^{16} \cdot 43^8 \cdot 43(mod\ 59) = 5 \cdot 51 \cdot 43(mod\ 59) = 50$$

Zadatak 4.2 *Neka je n proizvod različitih prostih brojeva takvih da za svaki prost broj p koji deli broj n važi $p - 1 \mid de - 1$, $d, e \in \mathbb{N}$. Dokazati da je $a^{de} \equiv a(mod\ n)$ za svako a, čak i ako je $NZD(a, n) > 1$.*

Rešenje: Kongruencija koju treba dokazati može se zapisati kao $n \mid a^{de-a} = a(a^{de-1} - 1)$. Kako je $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ za neke proste brojeve p_i, dovoljno je da pokažemo da za svaki broj p_i koji deli n važi $p_i \mid a(a^{de-1} - 1)$. Razlikujemo dva slučaja:

1. $NZD(a, p_i) = p_i$ - trivijalan slučaj.
2. $NZD(a, p_i) = 1$ - možemo primeniti Malu Fermaovu teoremu. Na osnovu teoreme važi $p_i \mid a^{p_i - 1}$. Na osnovu pretpostavke zadatka važi $p-1 \mid de-1$, a onda postoji i broj m takav da je $de-1 = m(p-1)$. Onda se desni deo izraza može zapisati kao:

$$a^{de-1} - 1 = a^{m(p-1)} - 1 = (a^{p-1})^m - 1^m$$

što je deljivo sa $a^{p-1} - 1$, a to je deljivo sa p čime je dokazano tvrđenje.

■

4.1 Programi

Zadatak 4.3 *Napisati funkciju koja izračunava $a^n(mod\ m)$ uzastopnim kvadriranjem.*

Rešenje:

```
def mod_pow(a, n, m):
    a = a % m
    res = 1
    while n > 0:
        # Za svaku jedinicu u binarnom zapisu n
        if n % 2 == 1:
            # Rezultat je stara vrednost rezultata * a^2{i} za i-tu poziciju
            res = (res * a) % m
        a = (a * a) % m
        # n gubi poslednju cifru u binarnom zapisu
        n = n // 2
    return res
```

5 Konačna polja

Neka je p prost broj. Grupa $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ sadrži p elemenata $\{0, 1, \ldots, p-1\}$ sa operacijama $+, -, \times$. Za elemente $\alpha \neq 0$ važi $NZD(\alpha, p) = 1$ pa možemo odrediti α^{-1}. Zbog toga se može deliti bilo kojim nenula elementom.

U skupu $\mathbb{F}_p^* = \{1, \ldots, p-1\}$ se mogu koristiti operacije $\times$ i $/$. Ova grupa je ciklična tj. da sadrži bar jedan element g takav da je $\{1, g, g^2, \ldots\} = \mathbb{F}_p^*$ koji nazivamo generator[2]. Grupa $\mathbb{Z}/p\mathbb{Z}^*$ ima $\varphi(p-1)$ različitih generatora. Neki element $x \in \mathbb{F}_p^*$ je generator grupe ako i samo ako je njegov red[3] jednak $p-1$.

Ako je g generator grupe $\mathbb{Z}/p\mathbb{Z}^*$ onda svi brojevi iz te grupe mogu da se dobiju pomoću g.

$$\{g, g^2, \ldots, g^{p-1}\} = \{1, 2, \ldots, p\}$$

Formalnije:

$$g \text{ je generator grupe } \mathbb{Z}/p\mathbb{Z}^* \Rightarrow \forall x \in \mathbb{Z}/p\mathbb{Z}^*,\ \exists k \in \mathbb{Z} :\ x = g^k.$$

Primetimo da su skupovi $\{g, g^2, \ldots, g^{p-1}\}$ i $\{1, 2, \ldots, p\}$ jednaki iako su njihovi elementi možda napisani različitim redosledom.

Teorema 5.1 *Ako je g generator ciklične grupe F_p^*, onda će i g^k biti generator te grupe ako i samo ako $NZD(k, p-1) = 1$.*

Zadatak 5.1 *Napraviti tabelu indeksa po modulu 29 sa osnovom 2.*

Rešenje:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$2^n (mod\ 29)$	1	2	4	8	16	3	6	12	24	19	9	18	7	14	28
n	15	16	17	18	19	20	21	22	23	24	25	26	27	28	
$2^n (mod\ 29)$	27	25	21	13	6	23	17	5	10	20	11	22	15	1	

Iz ove tabele možemo zaključiti da je broj 2 generator multiplikativne grupe ostataka $\mathbb{Z}/29\mathbb{Z}^*$ pošto se u tabeli nalaze svi celi brojevi manji od 29 bez ponavljanja.

Zadatak 5.2 *Napraviti tabelu indeksa po modulu 23 sa osnovom 2.*

Rešenje:

n	0	1	2	3	4	5	6	7	8	9	10	11
$2^n (mod\ 23)$	1	2	4	8	16	9	18	13	3	6	12	1
n	12	13	14	15	16	17	18	19	20	21	22	
$2^n (mod\ 23)$	2	4	8	16	9	18	13	3	6	12	1	

Iz ove tabele možemo zaključiti da broj 2 nije generator multiplikativne grupe ostataka $\mathbb{Z}/23\mathbb{Z}^*$ pošto se u tabeli ne nalaze svi brojevi iz intervala $[1, 22]$ i neki brojevi se ponavljaju.

[2] Generator grupe nazivamo još i primitivni koren po modulu p.
[3] Red elementa predstavlja broj različitih elemenata u skupu $\{x, x^2, x^3, \ldots\}$

Zadatak 5.3 *Napraviti tabelu indeksa po modulu 23 sa osnovom 5.*

Rešenje:

n	0	1	2	3	4	5	6	7	8	9	10	11
$5^n (mod\ 23)$	1	5	2	10	4	20	8	17	16	11	9	22
n	12	13	14	15	16	17	18	19	20	21	22	
$5^n (mod\ 23)$	18	21	13	19	3	15	6	7	12	14	1	

Iz ove tabele zaključujemo da je broj 5 generator multiplikativne grupe ostataka $\mathbb{Z}/23\mathbb{Z}^*$ pošto se u tabeli nalaze svi celi brojevi manji od 23 bez ponavljanja.

Zadatak 5.4 *Odrediti x ako važi:*

a) $52^x \equiv 38 (mod\ 29)$

b) $23^x \equiv 9 (mod\ 29)$

c) $3^x \equiv 7 (mod\ 29)$

d) $3^x \equiv 6 (mod\ 23)$

Rešenje: Ideja koju ćemo koristiti za svaku jednačinu jeste predstavljanje datih brojeva preko generatora odgovarajuće grupe. To radimo tako što broj tražimo u donjem redu tabele indeksa i menjamo ga sa g^n.

a) Pošto su brojevi 52 i 38 veći od 29, prvo ih svodimo na modul 29, a zatim dobijene brojeve predstavljamo preko stepena broja 2 pošto je to generator grupe $\mathbb{Z}/29\mathbb{Z}^*$:

$$23^x \equiv 9 (mod\ 29)$$

Dalje rešavanje jednačine isto je kao u delu pod b).

b)

$$\begin{aligned} &23^x \equiv 9 (mod\ 29) \\ &2^{20x} \equiv 2^{10} (mod\ 29) \\ &2^{20x-10} \equiv 1 (mod\ 29) \\ &2^{20x-10} \equiv 2^{28} (mod\ 29) \\ &\underbrace{20x-10}_{\text{nije deljivo sa 4}} \equiv 28k \not\downarrow \end{aligned}$$

Ova jednačina nema rešenja.

c)

$$\begin{aligned} &3^x \equiv 7 (mod\ 29) \\ &2^{5x} \equiv 2^{12} (mod\ 29) \\ &2^{5x-12} \equiv 1 (mod\ 29) \\ &2^{5x-12} \equiv 2^{28} (mod\ 29) \\ &5x-12 \equiv 28k \end{aligned}$$

Da bismo lakše proverili da li 28 deli $5k-12$, računamo $NZD(12,28)=4$. Broj x možemo zapisati kao $4z, z \in \mathbb{N}$ i dobijamo:

$$20z-12=28k$$
$$5z-3=7k$$

Sada ostaje da proverimo da li 7 deli $5z-3$. Ovaj izraz možemo transformisati dodavanjem -7 (neće promeniti deljivost celog izraza jer je -7 deljivo brojem 7):

$$5z-3=5z-10=5(z-2)$$

Da bi $5(z-2)$ bilo deljivo brojem 7, $z-2$ mora biti deljivo brojem 7, odnosno, broj z mora biti oblika $7k+2$. Odatle dobijamo rešenje jednačine:

$$x=28k+8, k \in \mathbb{Z}$$

d)

$$3^x \equiv 6(mod\ 23)$$
$$5^{16x} \equiv 5^{18}(mod\ 23)$$
$$5^{16x-18} \equiv 5^{22}(mod\ 23)$$
$$16x-18 \equiv 22k$$
$$8x-9 \equiv 11k$$

Da bismo lakše proverili da li ovo važi, i za koje x, $8x-9$ transformišemo dodavanjem broja -11, a zatim ponoviti postupak za novi izraz sve dok umnožak broja x ne bude jendak 1:

$$8x-9=8x-20=4(2x-5)$$
$$2x-5=2x-16=2(x-8)$$

Pošto treba da važi $11 \mid (x-8)$, rešenje jednačine je

$$x=11k+8, k \in \mathbb{Z}.$$

Zadatak 5.5 *Odrediti sve generatore $\mathbb{Z}/n\mathbb{Z}^*$ za $n=23$.*

Rešenje: Primenićemo teoremu 5.1. Znamo da je jedan generator ovde grupe broj 5 pa je svaka vrednost oblika 5^k takođe generator ako važi da je $NZD(k,22)=1$. Brojevi koji su uzajamno prosti sa 22 pripadaju skupu:

$$\{1,3,5,7,9,13,15,17,19,21\}.$$

Na osnovu tog skupa dobijamo i generatore:

$$\{5,10,20,17,11,21,19,15,7,14\}.$$

Zadatak 5.6 *Odrediti sve generatore* $\mathbb{Z}/n\mathbb{Z}^*$ *za* $n = 29$.

Rešenje: Primenićemo teoremu 5.1. Znamo da je jedan generator ovde grupe broj 2 pa je svaka vrednost oblika 2^k takođe generator ako važi da je $NZD(k, 28) = 1$. Brojevi koji su uzajamno prosti sa 28 pripadaju skupu:

$$\{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}.$$

Na osnovu tog skupa dobijamo i generatore:

$$\{2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15\}.$$

Zadatak 5.7 *Izračunati:*

a) $5^{-1}(mod\ 29)$

b) $(-1)^{-1}(mod\ 23)$

Rešenje: Svaki od izraza $a^{-1}(mod\ m)$ možemo transformisati u $ax \equiv 1(mod\ m)$, a zatim rešiti dobijenu jednačinu. Korišćenjem odgovarajućeg generatora pri čemu ćemo broj x predstaviti u obliku g^y i rešavati jednačinu po y.

a)

$$\begin{aligned}
&5x \equiv 1(mod\ 29)\\
&2^{22} \cdot 2^y \equiv 2^{28}(mod\ 29)\\
&2^{22+y} \equiv 2^{28}(mod\ 29)\\
&22 + y = 28\\
&y = 6\\
&x = 2^6(mod\ 29) \equiv 6(mod\ 29)
\end{aligned}$$

b)

$$\begin{aligned}
&-1(mod\ 23) = 22(mod\ 23)\\
&22x \equiv 1(mod\ 23)\\
&5^{11} \cdot 5^y \equiv 5^{22}(mod\ 23)\\
&5^{11+y} \equiv 5^{22}(mod\ 23)\\
&11 + y = 22\\
&y = 11\\
&x = 5^{11}(mod\ 23) \equiv 22(mod\ 23)
\end{aligned}$$

5.1 $\mathbb{F}_2[x]$

Neka je $\mathbb{F}_2[x]$ skup polinoma sa koeficijentima iz $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. U ovom skupu $-1 = 1$ pa je oduzimanje isto što i sabiranje. Polinomi se množe na uobičajeni način pri čemu se sa koeficijentima računa u $\mathbb{F}_2$.

Kažemo da je polinom *nesvodljiv* nad poljem ukoliko se ne može rastaviti u proizvod polinoma nižeg

stepena sa koeficijentima iz tog polja. Na primer, nad poljem $\mathbb{F}_2[x]$ polinom x^2+x+1 je nesvodljiv jer nije deljiv nijednim polinomom stepena 1, kao i polinomi x^3+x+1 i x^3+x^2+1. koji nisu deljivi polinomima prvog ni drugog stepena. Nesvodljive polinome možemo odrediti tako što sa spiska svih polinoma grupe izbacimo umnoške nesvodljivih polinoma.

Posmatrajmo polinome u $\mathbb{F}_2[x]$ i njihove ostatke po modulu nesvodljivog polinoma x^3+x+1. Ostaci će biti polinomi manjeg stepena i važi $x^3+x+x\equiv 0$ odnosno $x^3\equiv x+1$[4]. Nad skupom $\mathbb{F}_2[x]$ su definisane uobičajene operacije $+$ i $\times$, pri čemu važi $x^3=x+1$.

Zadatak 5.8 *Odrediti sve nesvodljive polinome stepena ≤ 3 u $\mathbb{F}_2[x]$.*

Rešenje: Polinomi koji pripadaju ovom skupu su:

$$
\begin{aligned}
0\{&\ \underline{1}\\
1\{&\ \underline{x}\\
&\ \underline{x+1}\\
2\{&\ x^2=x\cdot x\\
&\ x^2+1=(x+1)^2\\
&\ x^2+x=x(x+1)\\
&\ \underline{x^2+x+1}\\
3\{&\ x^3=x^2\cdot x=x\cdot x\cdot x\\
&\ x^3+1=(x^2+x+1)(x+1)\\
&\ x^3+x=x(x^2+1)=x(x+1)^2\\
&\ \underline{x^3+x+1}\\
&\ x^3+x^2=x^2(x+1)=x\cdot x(x+1)\\
&\ \underline{x^3+x^2+1}\\
&\ x^3+x^2+x=x(x^2+x+1)\\
&\ x^3+x^2+x+1=(x^2+1)(x+1)=(x+1)^3
\end{aligned}
$$

Podvučeni polinomi su nesvodljivi polinomi jer ne mogu da se rastave na proizvod polinoma nižeg stepena. Dakle, skup nesvodljivih polinoma stepena manjeg od 3 u $\mathbb{F}_2[x]$ je $\{1, x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1\}$.

Zadatak 5.9 *Da li je polinom $x^4+x^3+x^2+x+1$ nesvodljiv u $\mathbb{F}_2[x]$?*

Rešenje: Pokušaćemo da polinom $x^4+x^3+x^2+x+1$ predstavimo kao proizvod nesvodljivih polinoma nižeg stepena. Moguće kombinacije su polinom prvog i trećeg stepena ili dva polinoma drugog stepena. Dovoljno je da proverimo deljivost datog polinoma polinomima x, $x+1$ i x^2+x+1. Polinom očigledno nije deljiv polinomom x jer daje ostatak 1. Proverimo ostale.

$$
\begin{array}{l}
(x^4+x^3+x^2+x+1):(x+1)=x^3+x\\
\ x^4+x^3\\
\hline
\qquad x^2+x+1\\
\qquad x^2+x\\
\hline
\qquad\qquad 1
\end{array}
\qquad\qquad
\begin{array}{l}
(x^4+x^3+x^2+x+1):(x^2+x+1)=x^2\\
\ x^4+x^3+x^2\\
\hline
\qquad\qquad x+1
\end{array}
$$

[4]Ovu kongruenciju po modulu ćemo posmatrati kao jednakost.

Pošto polinom nije deljiv nijednim polinomom stepena 1, nije deljiv ni polinomima stepena 3. Takođe, polinom nije deljiv nesvodljivim polinomom stepena 2 pa zaključujemo da polinom $x^4+x^3+x^2+x+1$ jeste nesvodljiv u $\mathbb{F}_2[x]$.

Zadatak 5.10 *Napraviti tablicu množenja, tablicu inverza i proveriti da li je x generator u sledećim poljima:*

a) $\mathbb{F}_2[x]/(x^2+x+1)^*$

b) $\mathbb{F}_2[x]/(x^3+x^2+1)^*$

Rešenje:

a) Tablica inverza dobija se na osnovu tablice množenja. Invertni su polinomi koji u preseku kolne i vrste sadrže broj 1. Prilikom množenja vodimo računa da u ovom polju važi $x^2 = x+1$.

$\cdot$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

p	p^{-1}
1	1
x	$x+1$
$x+1$	x

Ostaje još da proverimo da li je x generator skupa $\mathbb{F}_2[x]/(x^2+x+1)^*$. To ćemo jednostavno uraditi računanjem stepena polinoma x. Pošto je zadati polinom stepena 2, u skupu ima 3 (2^2-1) ne-nula elemenata pa računamo $x^k, \forall k \in [0,3]$. Ukoliko je x generator, svaki element skupa $\mathbb{F}_2[x]/(x^2+x+1)^*$ odgovaraće tačno jednom stepenu polinoma x i važi će jednakost $x^3 = 1$.

$$x^0 = 1$$
$$x^1 = x$$
$$x^2 = x+1$$
$$x^3 = x^2 \cdot x = (x+1)x = x^2 + x = x+1+x = 1$$

Dobijeni su svi elementi te zaključujemo da x jeste generator ovog skupa.

b) Prilikom množenja vodimo računa da u ovom polju važi $x^3 = x^2+1$.

$\cdot$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	x^2+1	x^2+x+1	1	$x+1$
$x+1$	$x+1$	x^2+x	x^2+1	1	x	x^2+x+1	x^2
x^2	x^2	x^2+1	1	x^2+x+1	$x+1$	x	x^2+x
x^2+1	x^2+1	x^2+x+1	x	$x+1$	x^2+x	x^2	1
x^2+x	x^2+x	1	x^2+x+1	x	x^2	$x+1$	x^2+1
x^2+x+1	x^2+x+1	$x+1$	x^2	x^2+x	1	x^2+1	x

p	p^{-1}
1	1
x	x^2+x
$x+1$	x^2
x^2	$x+1$
x^2+1	x^2+x+1
x^2+x	x
x^2+x+1	x^2+1

Pošto je zadati polinom stepena 3, u skupu ima 7 (2^3-1) ne-nula elemenata pa računamo $x^k, \forall k \in [0,7]$. Ukoliko je x generator, svaki element skupa $\mathbb{F}_2[x]/(x^3+x^2+1)^*$ odgovaraće tačno jednom stepenu polinoma x i važi će jednakost $x^7 = 1$.

$$x^0 = 1 \qquad x^4 = x^2 + x + 1$$
$$x^1 = x \qquad x^5 = x + 1$$
$$x^2 = x^2 \qquad x^6 = x^2 + x$$
$$x^3 = x^2 + 1 \qquad x^7 = 1$$

Dobijeni su svi elementi te zaključujemo da x jeste generator ovog skupa.

Zadatak 5.11 *Napisati tablicu stepenova u* $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ *ako je* x *generator. Uz pomoć tablice izračunati* $(x^2 + 1)(x^2 + x + 1)$.

Rešenje:

k	0	1	2	3	4	5	6	7
x^k	1	x	x^2	x^2+1	x^2+x+1	$x+1$	x^2+x	1

Na osnovu tabele lako računamo proizvod:

$$(x^2 + 1)(x^2 + x + 1) = x^3 \cdot x^4 = x^7 = 1$$

Zadatak 5.12 *Pomoću Euklidovog algoritma odrediti* $(x^4)^{-1}$ *u polju* $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$.

Rešenje: Invertovanje polinoma $q(x)$ nad poljem $\mathbb{F}_2[x]/p(x)$ vrši se primenom Euklidovog algoritma na polinome $p(x)$ i $q(x)$. U ovom slučaju, to su polinomi x^4 i $x^5 + x^2 + 1$.

Prvo ćemo odrediti NZD ovih polinoma:

$$x^5 + x^2 + 1 = x \cdot x^4 + (x^2 + 1)$$
$$x^4 = (x^2 + 1) \cdot (x^2 + 1) + \underline{1}$$

Zatim, određujemo linearnu kombinaciju polinoma koja daje vrednost njihovog NZD-a:

$$\begin{aligned} 1 &= x^4 + (x^2 + 1) \cdot (x^2 + 1) \\ &= x^4 + (x^2 + 1) \cdot (x^5 + x^2 + 1 + x \cdot x^4) \\ &= (x^2 + 1) \cdot (x^5 + x^2 + 1) + (x^3 + x + 1) \cdot x^4 \end{aligned}$$

Iz linearne kombinacije dobijamo da je $(x^4)^{-1} = x^3 + x + 1$ u polju $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$.

Zadatak 5.13 *Pomoću Euklidovog algoritma odrediti* $(x^4 + x^3 + 1)^{-1}$ *u polju* $\mathbb{F}_2[x]/(x^6 + x + 1)$.

Rešenje: Prvo ćemo odrediti NZD ovih polinoma:

$$x^6 + x + 1 = (x^2 + x + 1) \cdot (x^4 + x^3 + 1) + (x^3 + x^2)$$
$$x^4 + x^3 + 1 = x \cdot (x^3 + x^2) + \underline{1}$$

Zatim, određujemo linearnu kombinaciju polinoma koja daje vrednost njihovog NZD-a:

$$\begin{aligned} 1 &= (x^4 + x^3 + 1) + x \cdot (x^3 + x^2) \\ &= (x^4 + x^3 + 1) + x \cdot ((x^6 + x + 1) + (x^2 + x + 1) \cdot (x^4 + x^3 + 1)) \\ &= x \cdot (x^6 + x + 1) + (x^3 + x^2 + x + 1) \cdot (x^4 + x^3 + 1) \end{aligned}$$

Iz linearne kombinacije dobijamo da je $(x^4 + x^3 + 1)^{-1} = (x^3 + x^2 + x + 1)$ u polju $\mathbb{F}_2[x]/(x^6 + x + 1)$.

5.2 Zadaci za vežbu

Zadatak 5.14 *Napraviti tabelu indeksa po modulu 37 sa osnovom 3. Da li je broj 3 generator grupe* $\mathbb{Z}/37\mathbb{Z}^*$*?*

Zadatak 5.15 *Napraviti tabelu indeksa po modulu 37 sa osnovom 5. Da li je broj 5 generator grupe* $\mathbb{Z}/37\mathbb{Z}^*$*?*

Zadatak 5.16 *Odrediti sve generatore grupe* $\mathbb{Z}/37\mathbb{Z}^*$*.*

Zadatak 5.17 *Odrediti* x *ako važi:*

a) $70^x \equiv 99(mod\ 37)$

b) $31^x \equiv 36(mod\ 37)$

c) $12^x \equiv 9(mod\ 37)$

Zadatak 5.18 *Izračunati:*

a) $7^{-1}(mod\ 29)$

b) $21^{-1}(mod\ 29)$

c) $39^{-1}(mod\ 23)$

d) $28^{-1}(mod\ 37)$

e) $9^{-1}(mod\ 37)$

Zadatak 5.19 *Odrediti sve nesvodljive polinome stepena 4 u* $\mathbb{F}_2[x]$*.*

Zadatak 5.20 *Napraviti tablicu množenja, tablicu inverza i proveriti da li je* x *generator u polju* $\mathbb{F}_2[x]/(x^3+x+1)^*$*.*

Zadatak 5.21 *Invertovati sledeće elemente u polju* $\mathbb{F}_2[x]/(x^5+x^2+1)^*$*:*

a) x^4+x^3+1

b) x^3+x^2+x+1

Zadatak 5.22 *Napraviti tablicu inverza u polju* $\mathbb{F}_2[x]/(x^4+x+1)^*$*.*

6 SAES

Algoritmi proširivanja ključa i šifrovanja u SAES koriste tabelu (funkcija) S čija struktura se opisuje korišćenjem konačnog polja od 16 elemenata. Neka je $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$. Nibl označava četvorku bita $b_0b_1b_2b_3$ kojoj se može pridružiti element $b_0x^3 + b_1x^2 + b_2x + b_3$ polja $\mathbb{F}_{16}$.

Funkcija S predstavlja bijektivno preslikavanje niblova u niblove $S : \{0,1\}^4 \to \{0,1\}^4$. Ova funkcija je kompozicija dva preslikavnaja:

1. **Inverzija nibla** u $\mathbb{F}_{16}$. U ovom koraku vrši se inverzija polinoma, kao što smo prikazali u zadatku 5.12. Izuzetak je nibl 0000 koji nije invertibilan i preslikava se u samog sebe. Dobijenom niblu $(b_0b_1b_2b_3)$ pridružuje se element $N(Y) = b_0y^3 + b_1y^2 + b_2y + b_3$ prstena[5] $\mathbb{F}_2[y]/(y^4 + 1)$.
2. **Transformacija nibla** $N(y)$ u $a(y)N(y) + b(y)$ u prstenu $\mathbb{F}_2[y]/(y^4 + 1)$ gde je $a(y) = y^3 + y^2 + 1$ i $b(y) = y^3 + 1$. Množenje u ovom prstenu slično je kao u $\mathbb{F}_{16}$, jedino što se računa po modulu $y^4 = 1$.

Zadatak 6.1 *Odrediti matrice A i B takve da se druga komponenta preslikavanja S u algoritmu SAES može predstaviti u obliku $AY + B$, gde je Y vektor-kolona (nibl) dobijen iz prve komponenete S.*

Rešenje: Kolona nibl Y može se zapisati kao:

$$Y = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Onda je $N(Y) = b_0y^3 + b_1y^2 + b_2y + b_3$. Neka je $T(N)$ transformacija nibla:

$$\begin{aligned} T(N) &= (y^3 + y^2 + 1)(b_0y^3 + b_1y^2 + b_2y + b_3) + (y^3 + 1) \\ &= y^3(b_0 + b_2 + b_3 + 1) + \\ &\quad y^2(b_0 + b_1 + b_3) + \\ &\quad y(b_0 + b_1 + b_2) + \\ &\quad 1(b_1 + b_2 + b_3 + 1) \end{aligned}$$

Iz ove jednakosti dobijamo matrice A i B. Redovi matrica odgovaraju, redom, vrednostima uz y^3, y^2, y^1, y^0. Kolone matrice A odgovaraju koeficijentima uz, redom, b_0, b_1, b_2, b_3, dok kolona matrice B odgovara koeficijentima uz slobodan član uz odgovarajući stepen y:

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Zadatak 6.2 *Odrediti tabelu S preslikavanja.*

Rešenje: Prvo ćemo prikazati postupno računanje za sve niblove a onda sve to spojiti u tabelu. Sa $\xrightarrow{1}$ obeležavamo primenu prvog preslikavanja (inverzija), a sa $\xrightarrow{2}$ primenu drugog preslikavanja (transformacija). Inverz je izračunat pomoću Euklidovog algoritma s tim da ćemo postupak ovog puta izostaviti.

[5] $\mathbb{F}_2[y]/(y^4 + 1)$ nije polje jer polinom $(y^4 + 1)$ nije nesvodljiv.

$0000 = 0 \xrightarrow{1} 0 = 0000 \xrightarrow{2} 0 \cdot (y^3 + y^2 + 1) + y^3 + 1 = y^3 + 1 = 1001$

$0001 = 1 \xrightarrow{1} 1 = 0001 \xrightarrow{2} 1 \cdot (y^3 + y^2 + 1) + y^3 + 1 = y^2 = 0100$

$0010 = x \xrightarrow{1} x^3 + 1 = 1001 \xrightarrow{2} (y^3 + 1) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y^3 + y = 1010$

$0011 = x + 1 \xrightarrow{1} x^3 + x^2 + x = 1110 \xrightarrow{2} (y^3 + y^2 + y) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y^3 + y + 1 = 1011$

$0100 = x^2 \xrightarrow{1} x^3 + x^2 + 1 = 1101 \xrightarrow{2} (y^3 + y^2 + 1) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y^3 + y^2 + 1 = 1101$

$0101 = x^2 + 1 \xrightarrow{1} x^3 + x + 1 = 1011 \xrightarrow{2} (y^3 + y + 1) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = 1 = 0001$

$0110 = x^2 + x \xrightarrow{1} x^2 + x + 1 = 0111 \xrightarrow{2} (y^2 + y + 1) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y^3 = 1000$

$0111 = x^2 + x + 1 \xrightarrow{1} x^2 + x = 0110 \xrightarrow{2} (y^2 + y) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y^2 + 1 = 0101$

$1000 = x^3 \xrightarrow{1} x^3 + x^2 + x + 1 = 1111 \xrightarrow{2} (y^3 + y^2 + y + 1) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y^2 + y = 0110$

$1001 = x^3 + 1 \xrightarrow{1} x = 0010 \xrightarrow{2} y \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y = 0010$

$1010 = x^3 + x \xrightarrow{1} x^3 + x^2 = 1100 \xrightarrow{2} (y^3 + y^2) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = 0 = 0000$

$1011 = x^3 + x + 1 \xrightarrow{1} x^2 + 1 = 0101 \xrightarrow{2} (y^2 + 1) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y + 1 = 0011$

$1100 = x^3 + x^2 \xrightarrow{1} x^3 + x = 1010 \xrightarrow{2} (y^3 + y) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y^3 + y^2 = 1100$

$1101 = x^3 + x^2 + 1 \xrightarrow{1} x^2 = 0100 \xrightarrow{2} y^2 \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y^3 + y^2 + y = 1110$

$1110 = x^3 + x^2 + x \xrightarrow{1} x + 1 = 0011 \xrightarrow{2} (y + 1) \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y^3 + y^2 + y + 1 = 1111$

$1111 = x^3 + x^2 + x + 1 \xrightarrow{1} x^3 = 1000 \xrightarrow{2} y^3 \cdot (y^3 + y^2 + 1) + (y^3 + 1) = y^2 + y + 1 = 0111$

NIBL	S(NIBL)
0000	1001
0001	0100
0010	1010
0011	1011
0100	1101
0101	0001
0110	1000
0111	0101
1000	0110
1001	0010
1010	0000
1011	0011
1100	1100
1101	1110
1110	1111
1111	0111

6.1 Proširivanje ključa

Algoritam SAES ima 16-bitni ključ $k_0k_1 \dots k_{15}$. Od njega treba formirati niz od 48 bita (prvih 16 bita su originalni ključ) procesom proširivanja ključa. Neka je

$$RC[i] = x^{i+2} \in \mathbb{F}_{16}$$
$$RCON[i] = RC[i]0000$$

Ako su N_0 i N_1 niblovi, onda N_0N_1 predstavlja njihovu konkatenaciju. Definišemo sledeće funkcije:

1. $RotNib(N_0N_1) = N_1N_0$ - rotacija niblova u kojoj niblovi menjaju mesta;

2. $SubNib(N_0N_1) = S(N_0)S(N_1)$ - substitucija niblova u kojoj se niblovi preslikavaju u nove niblove funkcijom S.

Neka je W niz bajtova. $W[0]$ i $W[1]$ su prvih, odnosno drugih, 8 bita ključa. Ostali članovi niza $W[i], 2 \leq i \leq 5$, definišu se rekurentnom relacijom:

$$W[i] = \begin{cases} W[i-2] \oplus RCON[i/2] \oplus SubNib(RotNib(W[i-1])), & i \equiv 0(mod\ 2) \\ W[i-2] \oplus W[i-1], & i \not\equiv 0(mod\ 2) \end{cases}$$

pri čemu $\oplus$ označava sabiranje po modulu dva, bit po bit.

Zadatak 6.3 *Primeniti proširivanje ključa na ključ "Qe".*

Rešenje: Ključ ćemo zapisati u binarnom obliku: 01010001 01100101. Na osnovu ključa određujemo:

$$W[0] = 0101\ 0001$$
$$W[1] = 0110\ 0101$$

Da bismo odredili $W[2]$ potrebno je da odredimo vrednost $RCON[1] = RC[1]0000$:

$$RC[1] = x^3 = 1000$$
$$RCON[1] = 1000\ 0000$$

Zatim, računamo $SubNib(RotNib(W[i-1])$:

$$SubNib(RotNib(W[1]) = SubNib(RotNib(0110\ 0101)) = 0001\ 1000$$

Sada treba sabrati dobijenu vrednost sa $W[0]$ i $RCON[1]$ po modulu dva, bit po bit:

$$\begin{aligned} W[2] &= W[0] \oplus RCON[1] \oplus SubNib(RotNib(W[1]) \\ &= 0101\ 0001 \oplus 1000\ 0000 \oplus 0001\ 1000 \\ &= 1100\ 1001 \end{aligned}$$

Sledeća vrednost koju računamo jeste $W[3]$:

$$\begin{aligned} W[3] &= W[1] \oplus W[2] \\ &= 0110\ 0101 \oplus 1100\ 1001 \\ &= 1010\ 1100 \end{aligned}$$

Za $W[4]$ potrebno je odrediti $RCON[2]$ i $SubNib(RotNib(W[3])$:

$$RC[2] = x^4 = x + 1 = 0011$$
$$RCON[2] = 0011\ 0000$$
$$SubNib(RotNib(W[3]) = 1100\ 0000$$

Sada možemo izračunati $W[4]$:

$$\begin{aligned} W[4] &= W[2] \oplus RCON[2] \oplus SubNib(RotNib(W[3]) \\ &= 1100\ 1001 \oplus 0011\ 0000 \oplus 1100\ 0000 \\ &= 0011\ 1001 \end{aligned}$$

Na kraju ostaje $W[5]$:

$$\begin{aligned} W[5] &= W[3] \oplus W[4] \\ &= 1010\ 1100 \oplus 0011\ 1001 \\ &= 1001\ 0101 \end{aligned}$$

Prošireni ključ je $W_0W_1W_2W_3W_4W_5$ odnosno:

$$0101\ 0001\ 0110\ 0101\ 1100\ 1001\ 1010\ 1100\ 0011\ 1001\ 1001\ 0101$$

6.2 Šifrovanje algoritmom SAES

Uprošćeni AES algoritam transformiše 16 bita otvorenog teksta u 16 bita šifrata pri čemu koristi prošireni ključ od 48 bita i primenjuje kompoziciju 8 funkcija:

$$A_{K_2} \circ SR \circ NS \circ A_{K_1} \circ MC \circ SR \circ NS \circ A_{K_0}$$

Pre nego što definišemo ponašanje svake od funkcija, uvedimo pojam stanje. Stanje je četvorka niblova

$b_0b_1b_2b_3$	$b_8b_9b_{10}b_{11}$
$b_4b_5b_6b_7$	$b_{12}b_{13}b_{14}b_{15}$

Funkcija A_{K_i} (engl. *add key*) na trenutno stanje dodaje vrednost ključa K_i. Sabiranje se vrši bit po bit po modulu 2, a indeksi bita stanja i bita ključa treba da se slažu po modulu 16.

$b_0b_1b_2b_3$ $\oplus\ k_0k_1k_2k_3$	$b_8b_9b_{10}b_{11}$ $\oplus\ k_8k_9k_{10}k_{11}$
$b_4b_5b_6b_7$ $\oplus\ k_4k_5k_6k_7$	$b_{12}b_{13}b_{14}b_{15}$ $\oplus\ k_{12}k_{13}k_{14}k_{15}$

Funkcija NS (engl. *nibble substitution*) na svaki nibl primenjuje funkciju S odnosno svaki nibl N_i zamenjuje sa $S(N_i)$.

N_0	N_2	$\longrightarrow$	$S(N_0)$	$S(N_2)$
N_1	N_3		$S(N_1)$	$S(N_3)$

Funkcija SR (engl. *shift row*) pomera drugi red za jedno mesto:

N_0	N_2	$\longrightarrow$	N_0	N_2
N_1	N_3		N_3	N_1

Funkcija MC (engl. *mix column*) transformiše kolone stanja. Jednoj koloni stanja sa niblovima N_i i N_j odgovara element N_iz+N_j polja $\mathbb{F}_{16}[z]/(z^2+1)$. Tako zapisana kolona množi se polinomom $c(z) = x^2z+1$. Rezultujući polinom se deli na deo uz z i slobodan deo. Deo uz z predstavlja gornji nibl transformisane kolone, a slobodan deo je donji nibl. Predstavimo to preko vrednosti bita niblova. Račun se vrši po modulima $z^2 + 1$, $x^4 + x + 1$ i 2:

$$(N_iz + N_j)(x^2z + 1) = N_ix^2z^2 + N_iz + N_jx^2z + N_j = z(N_i + N_jx^2) + N_ix^2 + N_j$$

Prvi red transformisane kolne dobija se po formuli $N_i + N_ix^2$, a drugi po formuli $N_ix^2 + N_j$. Formule možemo dalje razviti tako da dobijemo kombinacije bitova koje daju nove niblove. Sada polinome računamo po modulu $x^4 + x + 1$, a bitove po modulu 2:

$$\begin{aligned} N_i + N_ix^2 &= b_0x^3 + b_1x^2 + b_2x + b_3 + (b_4x^3 + b_5x^2 + b_6x + b_7)x^2 \\ &= b_0x^3 + b_1x^2 + b_2x + b_3 + b_4x^5 + b_5x^4 + b_6x^3 + b_7x^2 \\ &= b_0x^3 + b_1x^2 + b_2x + b_3 + b_4x^2 + b_4x + b_5x + b_5 + b_6x^3 + b_7x^2 \\ &= x^3(b_0 + b_6) + x^2(b_1 + b_4 + b_7) + x(b_2 + b_4 + b_5) + (b_3 + b_5) \end{aligned}$$

$$\begin{aligned} N_ix^2 + N_j &= (b_0x^3 + b_1x^2 + b_2x + b_3)x^2 + b_4x^3 + b_5x^2 + b_6x + b_7 \\ &= b_0x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x^3 + b_5x^2 + b_6x + b_7 \\ &= b_0x^2 + b_0x + b_1x + b_1 + b_2x^3 + b_3x^2 + b_4x^3 + b_5x^2 + b_6x + b_7 \\ &= x^3(b_2 + b_4) + x^2(b_0 + b_3 + b_5) + x(b_0 + b_1 + b_6) + (b_1 + b_7) \end{aligned}$$

Iz ovi jednačine dobijamo preslikavanje kolone:

$$\begin{array}{|c|}\hline b_0b_1b_2b_3 \\ \hline b_4b_5b_6b_7 \\ \hline \end{array} \longrightarrow \begin{array}{|cccc|}\hline b_0 \oplus b_6 & b_1 \oplus b_4 \oplus b_7 & b_2 \oplus b_4 \oplus b_5 & b_3 \oplus b_5 \\ \hline b_2 \oplus b_4 & b_0 \oplus b_3 \oplus b_5 & b_0 \oplus b_1 \oplus b_6 & b_1 \oplus b_7 \\ \hline \end{array}$$

Algoritam se sastoji iz dve runde, pri čemu je prva runda $A_{K_1} \circ MC \circ SR \circ NS$, druga je $A_{K_2} \circ SR \circ NS$, a prvoj prethodi funkcija A_{K_0}. Dakle, funkcije se primenjuju zdesna.

Zadatak 6.4 *Šifrovati otvoreni tekst "Ok" algoritmom SAES, ako je ključ "Qe".*

Rešenje: Prvi korak je zapis otvorenog teksta i ključa u binarnom obliku:

$$OT = [0100\ 1111\ 0110\ 1011]$$
$$K = [0101\ 0001\ 0110\ 0101]$$

Nakon toga, potrebno je proširiti ključ, što je već učinjeno u zadatku 6.3 pa znamo vrednosti $W[i]$:

$$W[0] = 0101\ 0001$$
$$W[1] = 0110\ 0101$$
$$W[2] = 1100\ 1001$$
$$W[3] = 1010\ 1100$$
$$W[4] = 0011\ 1001$$
$$W[5] = 1001\ 0101$$

Sada treba primeniti kompoziciju funkcija počevši od A_{K_0}:

$$\begin{array}{|c|c|}\hline 0100 & 0110 \\ \hline 1111 & 1011 \\ \hline \end{array} \xrightarrow{A_{K_0}} \begin{array}{|rc|}\hline 0100 & 0110 \\ \oplus\ 0101 & 0110 \\ \hline 1111 & 1011 \\ \oplus\ 0001 & 0101 \\ \hline \end{array} = \begin{array}{|c|c|}\hline 0001 & 0000 \\ \hline 1110 & 1110 \\ \hline \end{array} \xrightarrow{NS} \begin{array}{|c|c|}\hline 0100 & 1001 \\ \hline 1111 & 1111 \\ \hline \end{array} \xrightarrow{SR} \begin{array}{|c|c|}\hline 0100 & 0000 \\ \hline 1111 & 1111 \\ \hline \end{array}$$

$$\xrightarrow{MC} \begin{array}{|cccc|cccc|}\hline 0 \oplus 1 & 1 \oplus 1 \oplus 1 & 0 \oplus 1 \oplus 1 & 0 \oplus 1 & 1 \oplus 1 & 0 \oplus 1 \oplus 1 & 0 \oplus 1 \oplus 1 & 1 \oplus 1 \\ \hline 0 \oplus 1 & 0 \oplus 0 \oplus 1 & 0 \oplus 1 \oplus 1 & 1 \oplus 1 & 0 \oplus 1 & 1 \oplus 1 \oplus 1 & 1 \oplus 0 \oplus 1 & 0 \oplus 1 \\ \hline \end{array} =$$

$$\begin{array}{|c|c|}\hline 1101 & 0000 \\ \hline 1100 & 1101 \\ \hline \end{array} \xrightarrow{A_{K_1}} \begin{array}{|rc|}\hline 1101 & 0000 \\ \oplus\ 1100 & 1010 \\ \hline 1100 & 1101 \\ \oplus\ 1001 & 1100 \\ \hline \end{array} = \begin{array}{|c|c|}\hline 0001 & 1010 \\ \hline 0101 & 0001 \\ \hline \end{array} \xrightarrow{NS} \begin{array}{|c|c|}\hline 0100 & 0000 \\ \hline 0001 & 0100 \\ \hline \end{array} \xrightarrow{SR} \begin{array}{|c|c|}\hline 0100 & 0000 \\ \hline 0100 & 0001 \\ \hline \end{array}$$

$$\xrightarrow{A_{K_2}} \begin{array}{|rc|}\hline 0100 & 0000 \\ \oplus\ 0011 & 1001 \\ \hline 0100 & 0001 \\ \oplus\ 1001 & 0101 \\ \hline \end{array} = \begin{array}{|c|c|}\hline 0111 & 1001 \\ \hline 1101 & 0100 \\ \hline \end{array}$$

Primenom algoritma dobili smo šifrat 01111101 10010100.

6.3 Dešifrovanje algoritmom SAES

Za dešifrovanje se koristi isti ključ koji je korišćen za šifrovanje. Preciznije, koristi se prošireni ključ. Na šifrat se primenjuje inverz kompozicije funkcija koje su korišćene za šifrovanje. Kako važi da je $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$, kompozicija koja se koristi prilikom dešifrovanja je:

$$A_{K_0}^{-1} \circ NS^{-1} \circ SR^{-1} \circ MC^{-1} \circ A_{K_1}^{-1} \circ NS^{-1} \circ SR^{-1} \circ A_{K_2}^{-1}$$

Kako ćemo odrediti inverze ovih funkcija? Funkcije A_{K_i} i SR (samo u uprošćenoj verziji algoritma) su involucije[6]. Funkcija NS je koristila funkciju S za preslikavanje pojedinačnih niblova pa će NS^{-1} koristiti inverznu funkciju S^{-1}. Kako je funkcija S kompozicija dve funkcije, inverzije i transformacije nibla, funkcija S^{-1} biće obrnuta primena ovih funkcija - transformacija pa inverzija nibla. Da se podsetimo, transformaciju nibla računali smo u prstenu $\mathbb{F}_2[y]/(y^4+1)$ po formuli:

$$T(N) = N(y)a(y) + b(y),$$

gde su polinomi $a(y) = y^3+y^2+1$ i $b(y) = y^3+1$ elementi prstena $\mathbb{F}_2[y]/(y^4+1)$. Da bi smo dobili $N(y)$ potrebno je da jednačinu pomnožimo inverzom polinoma $a(y)$:

$$N(y) = T(N)a(y)^{-1} + a(y)^{-1}b(y),$$

Drugim rečima, potrebno je nibl $T(N)$ pomnožiti polinomom $a(y)^{-1} = y^2+y+1$ i dodati mu polinom $a(y)^{-1}b(y) = y^3+y^2$ u prstenu $\mathbb{F}_2[y]/(y^4+1)$. Drugi korak je inverzija dobijenog nibla u polju $\mathbb{F}_2[x]/(x^4+x+1)$. Dobijena tabela S^{-1} biće jednaka obrnutoj tabeli S odnosno, tabeli S sa zamenjenim kolonama.

Funkcija MC primenjuje se na jednu kolonu stanja, pa će isto važiti i za njen inverz. Element koji je pridružen koloni, N_iz+N_j množili smo polinomom $c(z) = x^2z+1$ u prstenu $\mathbb{F}_{16}[z]/(z^2+1)$. Zbog toga će inverzna funkcija množiti element N_iz+N_j inverzom polinoma $c(z)^{-1} = xz+(x^3+1)$. Možemo odrediti kombinaciju bitova za svaki bit rezultata, kao što smo to uradili za MC:

$$\begin{aligned}(N_iz+N_j)(xz+(x^3+1)) &= N_ixz^2 + N_ix^3z + N_iz + N_jxz + N_jx^3 + N_j\\ &\quad z(N_ix^3+N_i+N_jx) + (N_ix + N_jx^3 + N_j)\end{aligned}$$

$$\begin{aligned}N_ix^3+N_i+N_jx &= (b_0x^3+b_1x^2+b_2x+b_3)x^3 + b_0x^3+b_1x^2+b_2x+b_3 + (b_4x^3+b_5x^2+b_6x+b_7)x\\ &= b_0x^6+b_1x^5+b_2x^4+b_3x^3+b_0x^3+b_1x^2+b_2x+b_3+b_4x^4+b_5x^3+b_6x^2+b_7x\\ &= b_0x^3+b_0x^2+b_1x^2+b_1x+b_2x+b_2+b_3x^3+b_0x^3+b_1x^2+b_2x+b_3+b_4x+b_4\\ &\quad +b_5x^3+b_6x^2+b_7x\\ &= x^3(b_0+b_3+b_0+b_5)+x^2(b_0+b_1+b_1+b_6)+x(b_1+b_2+b_2+b_4+b_7)+(b_2+b_3+b_4)\\ &= x^3(b_3+b_5)+x^2(b_0+b_6)+x(b_1+b_4+b_7)+(b_2+b_3+b_4)\end{aligned}$$

$$\begin{aligned}N_ix+N_jx^3+N_j &= (b_0x^3+b_1x^2+b_2x+b_3)x + (b_4x^3+b_5x^2+b_6x+b_7)x^3 + b_4x^3+b_5x^2+b_6x+b_7\\ &= b_0x^4+b_1x^3+b_2x^2+b_3x+b_4x^6+b_5x^5+b_6x^4+b_7x^3+b_4x^3+b_5x^2+b_6x+b_7\\ &= b_0x+b_0+b_1x^3+b_2x^2+b_3x+b_4x^3+b_4x^2+b_5x^2+b_5x+b_6x+b_6+b_7x^3+b_4x^3\\ &\quad +b_5x^2+b_6x+b_7\\ &= x^3(b_1+b_4+b_7+b_4)+x^2(b_2+b_4+b_5+b_5)+x(b_0+b_3+b_5+b_6+b_6)+(b_0+b_6+b_7)\\ &= x^3(b_1+b_7)+x^2(b_2+b_4)+x(b_0+b_3+b_5)+(b_0+b_6+b_7)\end{aligned}$$

Prema tome, kombinacija bitova rezultujeće kolone je:

$b_0b_1b_2b_3$	$\longrightarrow$	$b_3\oplus b_5$	$b_0\oplus b_6$	$b_1\oplus b_4\oplus b_7$	$b_2\oplus b_3\oplus b_4$
$b_4b_5b_6b_7$		$b_1\oplus b_7$	$b_2\oplus b_4$	$b_0\oplus b_3\oplus b_5$	$b_0\oplus b_6\oplus b_7$

Isto kao kod algoritma šifrovanja, algoritam dešifrovanja primenjuje funkcije zdesna pa je prva funkcija koja se primenjuje A_{K_2}.

[6] Funkcije koje su inverzne same sebi nazivamo *involucijama*.

Zadatak 6.5 *Dešifrovati šifrat 0111 1101 1001 0100 algoritmom SAES, ako je ključ "Qe".*

Rešenje: Prvi korak je proširivanje ključa, što je već učinjeno u zadatku 6.3 pa znamo vrednosti $W[i]$:

$$W[0] = 0101\ 0001$$
$$W[1] = 0110\ 0101$$
$$W[2] = 1100\ 1001$$
$$W[3] = 1010\ 1100$$
$$W[4] = 0011\ 1001$$
$$W[5] = 1001\ 0101$$

Sada treba primeniti kompoziciju funkcija počevši od A_{K_2}:

$$\begin{array}{|c|c|} \hline 0111 & 1001 \\ \hline 1101 & 0100 \\ \hline \end{array} \xrightarrow{A_{K_2}} \begin{array}{|r|r|} \hline 0111 & 1001 \\ \oplus\ 0011 & 1001 \\ \hline 1101 & 0100 \\ \oplus\ 1001 & 0101 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 0100 & 0000 \\ \hline 0100 & 0001 \\ \hline \end{array} \xrightarrow{SR} \begin{array}{|c|c|} \hline 0100 & 0000 \\ \hline 0001 & 0100 \\ \hline \end{array} \xrightarrow{NS} \begin{array}{|c|c|} \hline 0001 & 1010 \\ \hline 0101 & 0001 \\ \hline \end{array}$$

$$\xrightarrow{A_{K_1}} \begin{array}{|r|r|} \hline 0001 & 1010 \\ \oplus\ 1100 & 1010 \\ \hline 0101 & 0001 \\ \oplus\ 1001 & 1100 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 1101 & 0000 \\ \hline 1100 & 1101 \\ \hline \end{array}$$

$$\xrightarrow{MC} \begin{array}{|cccc|cccc|} \hline 1\oplus 1 & 1\oplus 0 & 1\oplus 1\oplus 0 & 0\oplus 1\oplus 1 & 0\oplus 1 & 0\oplus 0 & 0\oplus 1\oplus 1 & 0\oplus 0\oplus 1 \\ \hline 1\oplus 0 & 0\oplus 1 & 1\oplus 1\oplus 1 & 1\oplus 0\oplus 0 & 0\oplus 1 & 0\oplus 1 & 0\oplus 0\oplus 1 & 0\oplus 0\oplus 1 \\ \hline \end{array} =$$

$$\begin{array}{|c|c|} \hline 0100 & 1001 \\ \hline 1111 & 1111 \\ \hline \end{array} \xrightarrow{SR} \begin{array}{|c|c|} \hline 0100 & 1001 \\ \hline 1111 & 1111 \\ \hline \end{array} \xrightarrow{NS} \begin{array}{|c|c|} \hline 0001 & 0000 \\ \hline 1110 & 1110 \\ \hline \end{array} \xrightarrow{A_{K_0}} \begin{array}{|r|r|} \hline 0001 & 0000 \\ \oplus\ 0101 & 0110 \\ \hline 1110 & 1110 \\ \oplus\ 0001 & 0101 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 0100 & 0110 \\ \hline 1111 & 1011 \\ \hline \end{array}$$

Primenom algoritma dobili smo otvoreni tekst 01001111 01101011, odnosno "Ok".

Zadatak 6.6 *Napisati Python program koji omogućava enkripciju i dekripciju algortmom SAES.*

Rešenje:

```
# pip3 install pyfinite
from pyfinite import ffield

class SAES:

    def __init__(self, key):
        # generator za F_16 = F_2[x]/x^4+x+1
        X_generator = 0b10011

        # generator za F_2[y]/y^4+1
        Y_generator = 0b10001

        # generator za F_16[z]/z^2+1
        Z_generator = 0b101

        # polinom a(y) = y^3+y^2+1 za funkciju S
```

```
        self.a = 0b1101

        # polinom b(y) = y^3+1 za funkciju S
        self.b = 0b1001

        # Polja sa odgovarajucim generatorima
        self.X_field = ffield.FField(4, gen=X_generator, useLUT=0)
        self.Y_field = ffield.FField(4, gen=Y_generator, useLUT=0)
        self.Z_field = ffield.FField(4, gen=Z_generator, useLUT=0)

        # inicijalizacija S tabele
        self._init_S()

        # prosirivanje kljuca
        self._extend_key(key)


    def _init_S(self):
        self.S_box = {}
        self.S_box_inv = {}

        for i in range(16):
            # prvo odredjujemo inverz broja i u polju X
            if i == 0:
                N = 0b0
            else:
                N = self.X_field.Inverse(i)

            # zapisujemo inverz kao element polja Y
            Ny = self.Y_field.Multiply(N, 1)

            # vrsimo transformaciju Ny u polju Y: Ny*a(y) + b(y)
            s = self.Y_field.Add(self.Y_field.Multiply(self.a, Ny), self.b)

            # upisujemo vrednost u tabelu
            self.S_box[i] = s
            self.S_box_inv[s] = i


    def S(self, x):
        return self.S_box[x]


    def S_inv(self, x):
        return self.S_box_inv[x]


    # funkcija SubNib
    def _sub_nib(self, nibble_pair):
        n1 = (0b11110000 & nibble_pair) >> 4
        n2 = (0b1111 & nibble_pair)

        n1_sub = self.S(n1)
        n2_sub = self.S(n2)

        return n1_sub * 16 + n2_sub
```

```
    # funkcija RotNib
    def _rot_nib(self, nibble_pair):
        n1 = (0b11110000 & nibble_pair) >> 4
        n2 = (0b1111 & nibble_pair)

        return n2 * 16 + n1


    # pretvaranje bitova u matricu koja opisuje jedno stanje
    def _bytes_to_matrix(self, byte_array):
        return [
            [(byte_array[0] & 0b11110000) >> 4, (byte_array[1] & 0b11110000) >> 4],
            [(byte_array[0] & 0b1111), (byte_array[1] & 0b1111)]
        ]


    # funkcija za prosirivanje kljuca
    def _extend_key(self, key):
        if len(key) != 2:
            raise Exception('Invalid key length')

        W = [ord(key[0]), ord(key[1]), 0, 0, 0, 0]

        RC = []
        x2 = self.X_field.ConvertListToElement([0,1,0,0])

        for i in range(1,4):
            x_i = [0,0,0,0]
            x_i[-i-1] = 1

            xi = self.X_field.ConvertListToElement(x_i)
            RC.append(self.X_field.Multiply(xi, x2))

        RCON = [0] + [rc * 16 for rc in RC]

        for i in range(2,6):
            if i % 2 == 0:
                k = self._sub_nib(self._rot_nib(W[i-1]))
                W[i] = RCON[i//2] ^ k ^ W[i-2]
            else:
                W[i] = W[i-2] ^ W[i-1]

        self.extended_key = W


    # Ak funkcija, dodavanje kljuca bit po bit (involucija)
    def _add_key(self, i, state):
        k_i = self.extended_key[i * 2 : i * 2 + 2]
        key_mat = self._bytes_to_matrix(k_i)

        return [
            [key_mat[0][0] ^ state[0][0], key_mat[0][1] ^ state[0][1]],
            [key_mat[1][0] ^ state[1][0], key_mat[1][1] ^ state[1][1]]
        ]


    # NS funkcija, primena funkcije S na svaki od niblova trenutnog stanja
    def _nibble_substitution(self, state):
```

```
        return [
            [self.S(state[0][0]), self.S(state[0][1])],
            [self.S(state[1][0]), self.S(state[1][1])]
        ]


    # NS inverzna funkcija, primena funkcije S^-1 na svaki od niblova trenutnog stanja
    def _nibble_substitution_inv(self, state):
        return [
            [self.S_inv(state[0][0]), self.S_inv(state[0][1])],
            [self.S_inv(state[1][0]), self.S_inv(state[1][1])]
        ]


    # SR funkcija, pomeranje drugog reda za jedno mesto (involucija)
    def _shift_row(self, state):
        return [
            [state[0][0], state[0][1]],
            [state[1][1], state[1][0]]
        ]


    # MC funkcija, primena formule (N_i*z + N_j)*c(z) = z(N_i + N_j*x^2) + (N_i*x^2 +
    ↪ N_j)
    # na obe kolone trenutnog stanja
    def _mix_column(self, state):
        Ni1 = state[0][0]
        Ni2 = state[0][1]
        Nj1 = state[1][0]
        Nj2 = state[1][1]

        return [
            [
                self.X_field.Add(Ni1, self.X_field.Multiply(Nj1, 0b100)),
                self.X_field.Add(Ni2, self.X_field.Multiply(Nj2, 0b100))
            ],
            [
                self.X_field.Add(Nj1, self.X_field.Multiply(Ni1, 0b100)),
                self.X_field.Add(Nj2, self.X_field.Multiply(Ni2, 0b100))
            ]
        ]


    # MC inverzna funkcija, primena formule (N_i*z + N_j)*c^{-1}(z) = z(N_i*x^3 + N_i
    ↪ + N_j*x) + (N_i*x + N_jx^3 + N_j)
    # na obe kolone trenutnog stanja
    def _mix_column_inv(self, state):
        Ni1 = state[0][0]
        Ni2 = state[0][1]
        Nj1 = state[1][0]
        Nj2 = state[1][1]

        return [
            [
                self.X_field.Add(self.X_field.Multiply(Ni1, 0b1001), self.X_field.
    ↪ Multiply(Nj1, 0b10)),
                self.X_field.Add(self.X_field.Multiply(Ni2, 0b1001), self.X_field.
    ↪ Multiply(Nj2, 0b10))
```

```
        ],
        [
            self.X_field.Add(self.X_field.Multiply(Ni1, 0b10), self.X_field.
↪ Multiply(Nj1, 0b1001)),
            self.X_field.Add(self.X_field.Multiply(Ni2, 0b10), self.X_field.
↪ Multiply(Nj2, 0b1001))
        ]
    ]


# sifrovanje 16bitnog teksta
def _encrypt_bytes(self, data):
    state = self._bytes_to_matrix(data)

    state = self._add_key(0, state)
    state = self._nibble_substitution(state)
    state = self._shift_row(state)
    state = self._mix_column(state)
    state = self._add_key(1, state)
    state = self._nibble_substitution(state)
    state = self._shift_row(state)
    state = self._add_key(2, state)

    return [state[0][0] * 16 + state[1][0], state[0][1] * 16 + state[1][1]]


# desifrovanje 16bitnog sifrata
def _decrypt_bytes(self, data):
    state = self._bytes_to_matrix(data)

    state = self._add_key(2, state)
    state = self._shift_row(state)
    state = self._nibble_substitution_inv(state)
    state = self._add_key(1, state)
    state = self._mix_column_inv(state)
    state = self._shift_row(state)
    state = self._nibble_substitution_inv(state)
    state = self._add_key(0, state)

    return [state[0][0] * 16 + state[1][0], state[0][1] * 16 + state[1][1]]


# funkcija koja dati tekst deli na grupe od 2 karaktera i svaku grupu pojedinacno
↪ sifruje
def encrypt(self, string_data):
    data_bytes = [ord(x) for x in string_data]
    n = len(data_bytes)

    if n % 2 == 1:
        data_bytes.append(ord(' '))

    encrypted_bytes = []

    for i in range(0, n, 2):
        data_bytes_slice = data_bytes[i:i+2]
        encrypted_bytes += self._encrypt_bytes(data_bytes_slice)

    return ''.join([chr(x) for x in encrypted_bytes])
```

```
    # funkcija koja dati sifrat deli na grupe od 2 karaktera i svaku grupu pojedinacno
    ↪ desifruje
    def decrypt(self, encoded_data):
        data_bytes = [ord(x) for x in encoded_data]
        n = len(data_bytes)

        decrypted_bytes = []

        for i in range(0, n, 2):
            data_bytes_slice = data_bytes[i:i+2]
            decrypted_bytes += self._decrypt_bytes(data_bytes_slice)

        return ''.join([chr(x) for x in decrypted_bytes])
```

6.4 Zadaci za vežbu

Zadatak 6.7 *Odrediti tabelu preslikavanja* S^{-1}.

Zadatak 6.8 *Primeniti proširivanje ključa na ključ 0101 1001 0111 1010.*

Zadatak 6.9 *Šifrovati otvoreni tekst "Ed" algoritmom SAES, ako je ključ "Yz".*

Zadatak 6.10 *Dešifrovati šifrat 11111110 11110011 algoritmom SAES ako je ključ "Yz".*

7 Sistemi sa javnim ključem

Zadatak 7.1 *Prikazati razmenu poruka u sistemu RSA ako je* $n = 697$, $p = 17$, $q = 41$, $d = 97$, $e = 33$, $M = 207$.

Rešenje: Da bi osoba A poslala poruku M osobi B, potrebno je da iskoristi javni ključ osobe B i odredi $M^e (mod\ n)$. Vrednost se može odrediti algoritmom stepenovanje kvradriranjem.

$$\begin{aligned} 207^{33}(mod\ 697) &= 207^{32} \cdot 207 \\ 207^{32} &\equiv (207^2)^{16} \equiv (332^2)^8 \equiv (98^2)^4 \equiv (543^2)^2 \equiv 18^2 \equiv 324 \\ 207^{33}(mod\ 697) &= 324 \cdot 207(mod\ 697) \equiv 156(mod\ 697) \end{aligned}$$

Osoba A, dakle, šalje 156 osobi B. Osoba B računa $M^d (mod\ n)$ kako bi dešifrovala poruku:

$$\begin{aligned} 156^{97}(mod\ 697) &= 156^{64} \cdot 156^{32} \cdot 156^1 (mod\ 697) \\ 156^{32} &\equiv (156^2)^{16} \equiv ((-59)^2)^8 \equiv ((-4)^2)^4 \equiv (16^2)^2 \equiv 256^2 \equiv 18 \\ 156^{64} &\equiv (156^{32})^2 \equiv 18^2 \equiv 324 \\ 156^{97}(mod\ 697) &= 324 \cdot 18 \cdot 156(mod\ 697) = 207(mod\ 697) \end{aligned}$$

Zadatak 7.2 *Prikazati postupak Diffie-Helman protokola usaglašavanja ključa za* $q = 97$, $g = 5$, $a_A = 36$, $a_B = 58$ *tj. izračunati* g^{a_A}, g^{a_B} *i* K.

Rešenje: Osoba A određuje svoj javni ključ i šalje ga osobi B:

$$\begin{aligned} g^{a_A} = \ & 5^{36}(mod\ 97) = 5^{32} \cdot 5^4 (mod\ 97) \\ & 5^4 \equiv 25^2 \equiv 43 \\ & 5^{32} \equiv (5^4)^8 \equiv 43^8 \equiv 6^4 \equiv 35 \\ g^{a_A} = \ & 43 \cdot 35(mod\ 97) = 50(mod\ 97) \end{aligned}$$

Osoba B određuje svoj javni ključ i šalje ga osobi A:

$$\begin{aligned} g^{a_B} = \ & 5^{58}(mod\ 97) = 5^{32} \cdot 5^{16} \cdot 5^8 \cdot 5^2 (mod\ 97) \\ & 5^2 \equiv 25 \\ & 5^8 \equiv (5^2)^4 \equiv (25^2)^2 \equiv 43^2 = 6 \\ & 5^{16} \equiv (5^8)^2 \equiv 6^2 \equiv 36 \\ & 5^{32} \equiv 35 \\ g^{a_B} = \ & 25 \cdot 6 \cdot 36 \cdot 35(mod\ 97) = 44(mod\ 97) \end{aligned}$$

Osoba A dobija vrednost ključa tako što javni ključ osobe B stepenuje svojim privatnim ključem:

$$\begin{aligned} K = \ & (g^{a_B})^{a_A} = 44^{36}(mod\ 97) = 44^{32} \cdot 44^4 (mod\ 97) \\ & 44^4 \equiv (44^2)^2 \equiv 93^2 \equiv (-4)^2 \equiv 16 \\ & 44^{32} \equiv (44^4)^8 \equiv 16^8 \equiv 62^4 \equiv 61^2 \equiv 35 \\ K = \ & 35 \cdot 16(mod\ 97) = 75(mod\ 97) \end{aligned}$$

Osoba A dobija vrednost ključa tako što javni ključ osobe B stepenuje svojim privatnim ključem:

$$\begin{aligned} K = \ & (g^{a_A})^{a_B} = 50^{58}(mod\ 97) = 50^{32} \cdot 50^{16} \cdot 50^8 \cdot 50^2(mod\ 97) \\ & 50^2 \equiv 75 \\ & 50^8 \equiv (75)^4 \equiv (96)^2 \equiv 1 \\ & 50^{16} \equiv (50^8)^2 \equiv 1 \\ & 50^{32} \equiv (50^{16})^2 \equiv 1 \\ K = \ & 75 \cdot 1 \cdot 1 \cdot 1(mod\ 97) = 75(mod\ 97) \end{aligned}$$

Sada i osoba A i osoba B imaju vrednost ključa K koji će koristiti za šifrovanje poruka.

Zadatak 7.3 *Prikazati postupak El Gamal protokola za $M = 30$, $q = 97$, $g = 5$, $a_B = 58$, $K = 17$.*

Rešenje: Osoba određuje svoj javni ključ:

$$g^{a_B} = 5^{58}(mod\ 97) = 44$$

Javni podaci su g i g^{a_B}. Osoba A je odabrala slučajan broj $K = 17$, računa vrednosti g^k i $Mg^{a_B k}$ i šalje ih osobi B:

$$\begin{aligned} & g^k = 5^{17}(mod\ 97) = 5^{16} \cdot 5(mod\ 97) = 36 \cdot 5(mod\ 97) = 83(mod\ 97) = -14(mod\ 97) \\ & Mg^{a_B k} = 30 \cdot 44^{17}(mod\ 97) = 30 \cdot 44^{16} \cdot 44(mod\ 97) = 30 \cdot 44 \cdot 16^4(mod\ 97) \\ & = 59 \cdot 62^2(mod\ 97) = 59 \cdot 61(mod\ 97) = 10(mod\ 97) \end{aligned}$$

Da bi osoba B dešifrovala primljenu poruku, potrebno je da odredi $(g^{a_B k})^{-1}$. To lako može uraditi stepenovanjem broja g^k (koji je dobio od osobe A) svojim tajnim ključem a_B i primenom Euklidovog algoritma za određivanje inverza.

$$\begin{aligned} g^{a_B k} = \ & (-14)^{58}(mod\ 97) = (-14)^{32} \cdot (-14)^{16} \cdot (-14)^8 \cdot (-14)^2(mod\ 97) \\ & (-14)^2 \equiv 2 \\ & (-14)^8 \equiv 2^4 \equiv 16 \\ & (-14)^{16} \equiv 16^2 \equiv 62 \\ & (-14)^{32} \equiv 62^2 \equiv 61 \\ g^{a_B k} = \ & 61 \cdot 62 \cdot 16 \cdot 2(mod\ 97) = 65 \end{aligned}$$

Sada, ocoba B primenjuje Euklidov algoritam da bi odredila inverz broja $g^{a_B k}$:

$$\begin{aligned} 97 &= 1 \cdot 65 + 32 & \qquad 1 &= 65 - 2 \cdot (97 - 65) \\ 65 &= 2 \cdot 32 + 1 & \qquad &= -2 \cdot 97 + \underline{3} \cdot 65 \end{aligned}$$

Na kraju, osoba B računa $Mg^{a_B k} \cdot g^{a_B k})^{-1} = M$:

$$M = 10 \cdot 3 = 30$$

Zadatak 7.4 *Prikazati postupak Massey-Omura razmene ključeva za $q = 677$, $M = 470$, $e_A = 255$, $e_B = 421$.*

Rešenje: Osoba A određuje svoj privatni ključ d_A:

$$d_A = e_A^{-1}(mod\ q - 1) = 255^{-1}(mod\ 676)$$

$$
\begin{aligned}
676 &= 2 \cdot 255 + 166 \\
255 &= 1 \cdot 166 + 89 \\
166 &= 1 \cdot 89 + 77 \\
89 &= 1 \cdot 77 + 12 \\
77 &= 6 \cdot 12 + 5 \\
12 &= 2 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1
\end{aligned}
\qquad
\begin{aligned}
1 &= 5 - 2 \cdot (12 - 2 \cdot 5) \\
&= -2 \cdot 12 + 5 \cdot (77 - 6 \cdot 12) \\
&= 5 \cdot 77 - 32 \cdot (89 - 77) \\
&= -32 \cdot 89 + 37 \cdot (166 - 89) \\
&= 37 \cdot 166 - 69 \cdot (255 - 166) \\
&= -69 \cdot 255 + 106 \cdot (676 - 2 \cdot 255) \\
&= 106 \cdot 676 \underline{-281} \cdot 255
\end{aligned}
$$

Osoba B određuje svoj privatni ključ d_B:

$$d_B = e_B^{-1}(mod\ q-1) = 421^{-1}(mod\ 676)$$

$$
\begin{aligned}
676 &= 1 \cdot 421 + 255 \\
421 &= 1 \cdot 255 + 166 \\
255 &= 1 \cdot 166 + 89 \\
166 &= 1 \cdot 89 + 77 \\
89 &= 1 \cdot 77 + 12 \\
77 &= 6 \cdot 12 + 5 \\
12 &= 2 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1
\end{aligned}
\qquad
\begin{aligned}
1 &= 5 - 2 \cdot (12 - 2 \cdot 5) \\
&= -2 \cdot 12 + 5 \cdot (77 - 6 \cdot 12) \\
&= 5 \cdot 77 - 32 \cdot (89 - 77) \\
&= -32 \cdot 89 + 37 \cdot (166 - 89) \\
&= 37 \cdot 166 - 69 \cdot (255 - 166) \\
&= -69 \cdot 255 + 106 \cdot (421 - 255) \\
&= 106 \cdot 421 - 175 \cdot (676 - 421) \\
&= -175 \cdot 676 + \underline{281} \cdot 421
\end{aligned}
$$

Osoba A računa M^{e_A} i to šalje osobi B:

$$
\begin{aligned}
M^{e_A} = 470^{255}(mod\ 677) = & 470^{128} \cdot 470^{64} \cdot 470^{32} \cdot 470^{16} \cdot 470^{8} \cdot 470^{4} \cdot 470^{2} \cdot 470^{1}(mod\ 677) \\
& 470^2 \equiv 198 \\
& 470^4 \equiv 198^2 \equiv 615 \equiv -62 \\
& 470^8 \equiv (-62)^2 \equiv 459 \\
& 470^{16} \equiv 459^2 \equiv 134 \\
& 470^{32} \equiv 134^2 \equiv 354 \\
& 470^{64} \equiv 354^2 \equiv 71 \\
& 470^{128} \equiv 71^2 \equiv 302 \\
M^{e_A} = 302 \cdot 71 \cdot 354 \cdot 134 \cdot & \ 459 \cdot 615 \cdot 198 \cdot 470(mod\ 677) = 292(mod\ 677)
\end{aligned}
$$

Osoba B dobijeni broj stepenuje na e_B, i vraća novu vrednost osobi A:

$$
\begin{aligned}
M^{e_A e_B} = & \ 292^{421}(mod\ 677) = 292^{256} \cdot 292^{128} \cdot 292^{32} \cdot 292^{4} \cdot 292^{1}(mod\ 677) \\
& 292^4 \equiv (292^2)^2 \equiv 639^2\ equiv(-38)^2 \equiv 90 \\
& 292^{32} \equiv (292^4)^8 \equiv (90^2)^4 \equiv 653^4 \equiv ((-24)^2)^2 \equiv 576^2 \equiv 46 \\
& 292^{128} \equiv (292^{32})^4 \equiv (46^2)^2 \equiv 85^2 \equiv 455 \\
& 292^{256} \equiv (292^{128})^2 \equiv 455^2 \equiv 540 \\
M^{e_A e_B} = & \ 540 \cdot 455 \cdot 46 \cdot 90 \cdot 292(mod\ 677) = 156
\end{aligned}
$$

Sada osoba A stepenuje dobijeni broj na d_A i vraća vrednost osobi B:

$$\begin{aligned}
M^{e_A e_B d_A} = \; & 156^{395}(mod\ 677) = 156^{256} \cdot 156^{128} \cdot 156^{8} \cdot 156^{2} \cdot 156^{1}(mod\ 677) \\
& 156^2 \equiv 641 \equiv -36 \\
& 156^8 \equiv (156^2)^4 \equiv ((-36)^2)^2 = 619^2 \equiv 656 \equiv -21 \\
& 156^{128} \equiv (156^8)^{16} \equiv (441^2)^4 \equiv (182^2)^2 \equiv 628^2 \equiv 370 \\
& 156^{256} \equiv (156^{128})^2 \equiv 370^2 \equiv 146 \\
M^{e_A e_B d_A} = \; & 146 \cdot 370 \cdot (-21) \cdot (-36) \cdot 156(mod\ 677) = 313(mod\ 677)
\end{aligned}$$

Na kraju, osoba B stepenuje dobijeni broj na d_B čime dobija originalnu poruku M:

$$\begin{aligned}
M^{e_A e_B d_A d_B} = \; & 313^{281}(mod\ 677) = 313^{256} \cdot 313^{16} \cdot 313^{8} \cdot 313^{1}(mod\ 677) \\
& 313^8 \equiv (313^2)^4 \equiv (481^2)^2 \equiv 504^2 \equiv 141 \\
& 313^{16} \equiv (313^8)^2 \equiv 141^2 \equiv 248 \\
& 313^{256} \equiv (313^{16})^{16} \equiv (248^2)^8 \equiv (574^2)^4 \equiv (454^2)^2 \equiv 308^2 \equiv 84 \\
M^{e_A e_B d_A d_B} = \; & 84 \cdot 248 \cdot 141 \cdot 313(mod\ 677) = 470(mod\ 677)
\end{aligned}$$

7.1 Programi

Zadatak 7.5 *Napisati Python program koji implementara RSA algoritam.*

Rešenje: Implementacija se sastoji iz klase `RSA` i glavnog programa koji koristi funkcionalnosti implementirane klase.

U implementaciji iskorišćena je funkcija `get_prime` za određivanje velikih prostih brojeva. Funkcija `get_prime` implementirana je kao probabilistički algoritam tipa Las Vegas koji koristi funkciju `miller_rabin` kako bi odredila da li je broj prost ili ne. Algoritam Miller Rabin je zasnovan na maloj Fermaovoj teoremi $x^{p-1} \equiv 1(mod\ p)$, gde je p prost broj, i pronalaženju netrivijalnih korena jedinice $x^2 \equiv 1(mod\ p)$ akko $p \mid (x^2 - 1) = (x - 1)(x + 1)$, tj. $x \equiv -1(mod\ p)$ ili $x \equiv 1(mod\ p)$. Ako algoritam vrati vrednost `False`, broj je sigurno složen. U supro-tnom, ako je vraćena vrednost `True`, broj je verovatno prost sa verovatnoćom $p = 4^{-k}$, gde je k parametar algoritma. Detaljnije o algoritmu možete pogledati ovde.

Funkcija `miller_rabin` primenjuje ovaj algoritam pri čemu koristi ranije implementiranu funkciju `mod_pow` za računanje stepena broja po modulu.

```
def miller_rabin(n, k):
    if n <= 3:
        if n == 1:
            return False
        return True

    # n prost => n neparan => n = (2 ^ r) * d + 1
    d = n - 1
    r = 0
    while d % 2 == 0:
        r = r + 1
        d = d // 2

    for i in range(k):
        a = random.randrange(2, n - 1)

        x = mod_pow(a, d, n)

        if x == 1 or x == n - 1:
            continue

        witness = True

        for j in range(r - 1):
            x = mod_pow(x, 2, n)
            if x == 1:
                return False
            if x == n - 1: # n - 1 = -1 (mod n)
                witness = False
                break

        if witness:
            return False

    return True
```

```
def get_prime(limit, k = 20):
    is_prime = False
    while not is_prime:
        n = random.randrange(limit)
        is_prime = miller_rabin(n, k)
    return n
```

```
class RSA:

    def __init__(self, p, q):
        self.p = p
        self.q = q

        self.n = self.p * self.q

        self.phi = (self.p - 1) * (self.q - 1)

        while True:
            e = random.randrange(2, self.phi - 1)
            gcd, m, n = extended_gcd(e, self.phi)

            if gcd == 1:
                self.e = e
                break

        self.d = mod_inv(self.e, self.phi)


    def encrypt(self, m, e):
        return mod_pow(m, e, self.n)


    def decrypt(self, me):
        return mod_pow(me, self.d, self.n)
```

U glavnom delu programa, osoba A šalje poruku osobi B.

```
def main():
    limit = 256
    p = get_prime(2**limit)
    q = get_prime(2**limit)
    A = RSA(p, q)
    B = RSA(p, q)

    m1 = 207

    me = A.encrypt(m1, B.e)
    print("Sifrovano: ", me)

    med = B.decrypt(me)
    print("Desifrovano: ", med)
```

Zadatak 7.6 *Napisati Python program koji implementira Diffie-Helman protokol usaglašavanja ključa.*

Rešenje: Implementacija se sastoji iz klase `Diffie_Helman` i glavnog dela programa koji koristi funkcionalnosti implementirane klase i prati protokol usaglašavanja ključeva.

```
class Diffie_Helman:

    def __init__(self, q, g):
        self.q = q
        self.g = g
        self.pr = random.randrange(2, q)
        self.pub = mod_pow(self.g, self.pr, self.q)


    def get_key(self, pub_key):
        return mod_pow(pub_key, self.pr, self.q)
```

U glavnom delu programa implementiran je protokol usaglašavanja ključeva.

```
def main():
    q = get_prime(2**256)
    g = random.randrange(2, q)

    A = Diffie_Helman(q, g)
    B = Diffie_Helman(q, g)

    print(A.pr, A.pub)
    print(B.pr, B.pub)

    print(A.get_key(B.pub))
    print(B.get_key(A.pub))
```

Zadatak 7.7 *Napisati Python program koji implementira El Gamal protokol.*

Rešenje: Implementacija se sastoji iz klase `El_Gamal` i glavnog dela programa koji koristi funkcionalnosti implementirane klase i prati protokol za razmenu poruka.

```
class ElGamal:

    def __init__(self, q, g):
        self.q = q
        self.g = g
        self.pr = random.randrange(2, q)
        self.pub = mod_pow(g, self.pr, q)


    def encrypt(self, m, pub_key):
        k = random.randrange(2, self.q)
        g_k = mod_pow(self.g, k, self.q)
        e = mod_pow(pub_key, k, self.q)
        me = (m * e) % self.q

        return (me, g_k)
```

```
    def decrypt(self, me, g_k):
        d = mod_inv(mod_pow(g_k, self.pr, self.q), self.q)
        m = (me * d) % self.q

        return m
```

```
def main():
    q = get_prime(2**256)
    g = random.randrange(2, q)

    A = ElGamal(q, g)
    B = ElGamal(q, g)

    m = 123000
    (me, g_k) = A.encrypt(m, B.pub)

    md = B.decrypt(me, g_k)

    print("Sifrovano: ", me)
    print("Desifrovano: ", md)
```

Zadatak 7.8 *Napisati Python program koji implementira Massey-Omura protokol razmene ključeva.*

Rešenje: Implementacija se sastoji iz klase `Massey_Omura` i glavnog dela programa koji koristi funkcionalnosti pomenute klase i prati protokol za razmenu ključeva.

```
class Massey_Omura:

    def __init__(self, q):
        self.q = q

        while True:
            e = random.randrange(2, q-1)
            gcd, _, _ = extended_gcd(e, q-1)

            if gcd == 1:
                self.e = e
                break

        self.d = mod_inv(e, q-1)


    def encrypt(self, k):
        return mod_pow(k, self.e, self.q)


    def decrypt(self, k):
        return mod_pow(k, self.d, self.q)
```

U glavnom delu programa implementiran je protokol korišćenjem klase `Massey_Omura`.

```
def main():
    A = Massey_Omura(677)
    B = Massey_Omura(677)

    print(A.e, A.d)
    print(B.e, B.d)

    # Kljuc koji je odabrala osoba A
    k = 349

    # A sifruje
    k_ea = A.encrypt(k)

    # B sifruje
    k_ea_eb = B.encrypt(k_ea)

    # A desifruje
    k_eada_eb = A.decrypt(k_ea_eb)

    # B desifruje i dobija kljuc koji je osoba A odabrala
    k_eada_ebdb = B.decrypt(k_eada_eb)

    # Vrednost kljuca koju je B dobio
    print(k_eada_ebdb)
```

8 Eliptičke krive

Eliptičke krive su kubne krive oblika $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. U kriptografiji se često koriste Vaještrasove krive za koju važi $a_1 = a_2 = a_3 = 0$ pa je kriva oblika:

$$y^2 = x^3 + a_4x + a_6$$

odnosno, u uobičajenom zapisu:

$$y^2 = x^3 + Ax + B$$

Ove krive se u kriptografiji definišu nad konačnim poljima što znači da su x i y iz konačnih skupova u oznaci $y^2 = x^3 + ax + b(mod\ p)$.

Nad tačkama krive, definisane nad konačnim poljem, osnovna operacija je sabiranje tačaka. Zbir dve tačke P i Q definiše se kao tačka simetrična u odnosu na x-osu presečnoj tački jednačine eliptičke krive i jednačine prave koja prolazi kroz tačke P i Q. Specijalan slučaj predstavljaju tangete krive kada su P i Q jednake. Tada operaciju sabiranja nazivamo operacijom dupliranja tačaka.

Beskonačno udaljena tačka (ili nula-tačka, u oznaci $\varnothing$) predstavlja tačku susreta svih horizontalnih pravih i krive u beskonačnosti i definiše se kao neutral za sabiranje pa važi sledeće:

$$P + \varnothing = \varnothing + P = P$$
$$P + (-P) = \varnothing$$
$$\varnothing + \varnothing = \varnothing$$

Oduzimanje se svodi na sabiranje sa inverznom tačkom pri čemu se inverz tačke $P(x, y)$ tačka $-P = (x, -y)$.

Sabiranje dve različite tačke

Neka su date dve različite tačke $P(x_p, y_p)$ i $Q(x_q, y_q)$ na eliptičkoj krivoj jednačine $y^2 = x^3+Ax+B$. Tačka $R = (x_r, y_r)$ predstavlja tre u tačku preseka prave i eliptičke krive, a njen inverz (tj. njena simetrična tačka) je zbir tačaka P i Q na eliptičkoj krivoj. Neka je $y = kx + n$ jednačina prave koja prolazi kroz tačke P i Q. Tada važi:

$$k = \frac{y_q - y_p}{x_q - y_p} \qquad\qquad n = y_p - kx_p$$

Prava preseca krivu u tri tačke: P, Q i R. Kako su P i Q poznate, lako ćemo odrediti R iz sledećeg sistema:

$$y = kx + n/^2$$
$$y^2 = x^3 + Ax + B$$

$$y^2 = k^2x^2 + 2kxn + n^2$$
$$y^2 = x^3 + Ax + B$$

$$y^2 = k^2x^2 + 2kxn + n^2 = x^3 + Ax + B$$

$$x^3 + Ax + B - k^2x^2 - 2kxn - n^2 = x^3 - k^2x^2 - (A - 2kn)x + B - n^2 = 0$$

Dobijena jednačina predstavlja polinom sa nulama u presečnim tačkama prave i eliptičke krive pa se može izrazti kao proizvod korena kubne jednačine:

$$
\begin{aligned}
&(x - x_p)(x - x_q)(x - x_r) = 0 \\
&(x^2 - xx_q - xx_p + x_p x_q)(x - x_r) = \\
&x^3 - x^2 x_q - x^2 x_p + x x_p x_q - x^2 x_r + x x_q x_r + x x_p x_r + x_p x_q x_r \\
&x^3 - x^2 \underbrace{(x_p + x_q + x_r)}_{=k^2} + x \underbrace{(x_p x_q + x_p x_r + x_q x_r)}_{A-2kn} + \underbrace{x_p x_q x_r}_{B-n^2} = 0
\end{aligned}
$$

Iskoristićemo jednačinu $k^2 = x_p + x_q + x_r$. Vrednosti x_p i x_q su poznate pa se x_r lako računa iz nje, dok se y_r računa iz jednačine prave:

$$
\begin{aligned}
x_r &= k^2 - x_p - x_q \\
y_r &= k x_r + n
\end{aligned}
$$

Kada smo odredili tačku R, potrebno je još da negiramo njenu y koordinatu kako bismo dobili zbir tačaka P i Q:

$$
P + Q = -R = (x_r, -y_r)
$$

Dupliranje tačke

U slučaju da su tačke koje se sabiraju jednake, onda postoje dve umesto tri tačke preseka prave i elpitičke krive. Pošto važi $x_p = x_q$ i $y_p = y_q$, ne možemo da odredimo koeficijent pravca prave po prethodnoj formuli (rezultat bi bio $\frac{0}{0}$ što nije definisano). Ipak, koeficijent se može odrediti. Tražena prava je tangenta eliptičke krive koja prolazi kroz tačku P pa koeficijent pravca računamo kao prvi izvod:

$$
\begin{aligned}
y^2 &= (x^3 + Ax + B) \;/\; \frac{\partial y}{\partial x} \\
2y\frac{\partial y}{\partial x} &= 3x^2 + A \\
k = \frac{\partial y}{\partial x} &= \frac{3x^2 + A}{2y}
\end{aligned}
$$

Slobodan član se računa po istoj formuli kao u prethodnom slučaju:

$$
n = y_p - k x_p
$$

Račun se nastavlja po prethodnim formulama, s tim da uzimamo u obzir da su tačke koje se sabiraju jednake:

$$
\begin{aligned}
x_r &= k^2 - 2x_p \\
y_r &= k x_r + n
\end{aligned}
$$

Kada smo dobili koordinate tačke R ostaje još da odredimo njen inverz što predstavlja dupliranu tačku P.

Višestruko sabiranje tačke eliptičke krive

Višestruko sabiranje tačke P samom sobom označava se sa nP. To se može izračunati uzastopnim sabiranjem tačke P

$$
nP = P + P + P + \ldots + P = 2P + P \ldots + P
$$

što zahteva n sabiranja. Efikasniji pristup je korišćenje što više izračunatih dupliranih sabiraka.

Zadatak 8.1 *Za eliptičku krivu* $E : y^2 = x^3 + 3x + 8$ *nad poljem* $\mathbb{F}_{13}$

a) odrediti skup tačaka;

b) izračunati (1,8)+(9,7);

c) izračunati 2(9,7).

Rešenje:

a) Pošto je kriva nad poljem $\mathbb{F}_{13}$, sve se računa po modulu 13. Stoga, koordinate x i y svih tačaka uzimaju neku od vrednosti iz skupa $\{0, 1, 2, \dots 12\}$ odnosno $\{0, \pm1, \pm2, \dots, \pm6\}$. Naredna tabela prikazuje moguće vrednosti za y^2:

y	0	±1	±2	±3	±4	±5	±6
y^2	0	1	4	9	3	12	10

Sada možemo da za svako $x \in \{0, 1, 2, \dots 12\}$ odredimo vrednost za y^2 jednostavnom zamenom vrednosti u jednačinu krive. Ukoliko dobijemo vrednost koja se nalazi u tabelu, našli smo dve tačke koje pripadaju krivoj:

$x = 0 \to y^2 = 8 \to 8$ se ne nalazi u tabeli, stoga nema tačke za x=0.
$x = 1 \to y^2 = 12 \to$ Iz tabele dobijamo da je $y = \pm5$ pa dobijamo dve tačke krive: (1, 5) i (1, 8).
$x = 2 \to y^2 = 9 \to$ Iz tabele dobijamo da je $y = \pm3$ pa dobijamo dve tačke krive: (2, 3) i (2, 10).
$x = 3 \to y^2 = 5 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=3.
$x = 4 \to y^2 = 6 \to 6$ se ne nalazi u tabeli, stoga nema tačke za x=4.
$x = 5 \to y^2 = 5 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=5.
$x = 6 \to y^2 = 8 \to 8$ se ne nalazi u tabeli, stoga nema tačke za x=6.
$x = 7 \to y^2 = 8 \to 8$ se ne nalazi u tabeli, stoga nema tačke za x=7.
$x = 8 \to y^2 = 11 \to 11$ se ne nalazi u tabeli, stoga nema tačke za x=8.
$x = 9 \to y^2 = 10 \to$ Iz tabele dobijamo da je $y = \pm6$ pa dobijamo dve tačke krive: (9, 6) i (9, 7).
$x = 10 \to y^2 = 11 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=10.
$x = 11 \to y^2 = 7 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=11.
$x = 12 \to y^2 = 4 \to$ Iz tabele dobijamo da je $y = \pm2$ pa dobijamo dve tačke krive: (12, 2) i (12, 11).

Dobijene tačke i $\varnothing$ čine skup tačaka ove krive:

$$E(\mathbb{F}_{13}) = \{\varnothing, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}$$

b) $P = (1, 8)$, $Q = (9, 7)$, $P + Q = -R$
Primenićemo formule sa početka poglavlja, pri čemu računamo po modulu 13:

$$k = \frac{y_p - y_q}{x_p - x_q} = \frac{-1}{8} = -8^{-1} = -5 = 8$$
$$n = y_p - kx_p = 8 - 8 \cdot 1 = 0$$

Jednačina prave koja seče krivu u tačkama P i Q je $y = 8x$.

$$x_r = k^2 - x_p - x_q = 12 - 1 - 9 = 2$$
$$y_r = kx_r + n = 8 \cdot 2 = 3$$

Dakle, $P + Q = (2, -3) = (2, 10)$[7].

[7] Primetimo da se zbir tačaka krive nalazi u skupu tačaka krive. To važi za sve umnoške tačaka iz skupa

c) $P = (9, 7)$, $2P = -R$
Primenićemo formule sa početka poglavlja, pri čemu računamo po modulu 13:

$$k = \frac{3x_p^2 + 3}{2y_p} = \frac{12}{1} = 12$$
$$n = y_p - kx_p = 7 - 12 \cdot 9 = 3$$

Jednačina tangete koja prolazi kroz tačku P je $y = 12x + 3$.

$$x_r = k^2 - 2x_p = 1 - 5 = -4 = 9$$
$$y_r = kx_r + n = 4 + 3 = 7$$

Dakle, $2P = (9, -7) = (9, 6)$.

Zadatak 8.2 *Za eliptičku krivu* $E : y^2 = x^3 + 3x + 8$ *nad poljem* F_{13}

a) pokazati da je tačka $(1, 5)$ *generator i napraviti tabelu umnožaka te tačke;*

b) koristeći tabelu umnožaka izračunati:

- *(12,11)+(2,3),*
- *(12,2)+(9,6),*
- *25(9,7).*

Rešenje:

a) Kako bismo pokazali da je tačka $G = (1, 5)$ generator, potrebno je da odredimo tačke $nG, \forall n \in [2, 8]$ (jer u skupu ima 9 tačaka). Za $n = 0$ dobijamo $\varnothing$, a za $n = 1$ je početna tačka $(1, 5)$.

- $2G = (x_g, y_g) = G + G$

$$k = \frac{3 \cdot 1 + 3}{2 \cdot 5} = 6 \cdot 10^{-1} = 6 \cdot 4 = 11$$
$$n = 5 - 11 \cdot 1 = 7$$

Jednačina tangete koja prolazi kroz tačku G je $y = 11x + 7$.

$$x_g = 11^2 - 2 \cdot 1 = 4 - 2 = 2$$
$$y_g = 11 \cdot 2 + 7 = 9 + 7 = 3$$
$$2G = (2, -3) = (2, 10)$$

- $3G = (x_g, y_g) = 2G + G$

$$k = \frac{10 - 5}{2 - 1} = 5$$
$$n = 10 - 5 \cdot 2 = 0$$

Jednačina prave koja prolazi kroz tačke G i $2G$ je $y = 5x$.

$$x_g = 5^2 - 1 - 2 = 9$$
$$y_g = 5 \cdot 9 = 6$$
$$3G = (9, -6) = (9, 7)$$

- $4G = (x_g, y_g) = 2G + 2G$

$$k = \frac{3 \cdot 2^2 + 3}{2 \cdot 10} = 2 \cdot 7^{-1} = 2 \cdot 2 = 4$$
$$n = 10 - 4 \cdot 2 = 2$$

Jednačina tangete koja prolazi kroz tačku $2G$ je $y = 4x + 2$.

$$x_g = 4^2 - 2 \cdot 2 = 3 - 4 = 12$$
$$y_g = 4 \cdot 12 + 2 = 9 + 2 = 11$$
$$4G = (12, -11) = (12, 2)$$

- $5G = (x_g, y_g) = 4G + G$

$$k = \frac{2 - 5}{12 - 1} = -3 \cdot 11^{-1} = -3 \cdot 6 = 8$$
$$n = 5 - 8 \cdot 1 = -3 = 10$$

Jednačina prave koja prolazi kroz tačke G i $4G$ je $y = 8x + 10$.

$$x_g = 8^2 - 1 - 12 = 12$$
$$y_g = 8 \cdot 12 + 10 = 2$$
$$5G = (12, -2) = (12, 11)$$

- $6G = (x_g, y_g) = 3G + 3G$

$$k = \frac{3 \cdot 9^2 + 3}{2 \cdot 7} = 12$$
$$n = 7 - 12 \cdot 9 = 3$$

Jednačina tangete koja prolazi kroz tačku $3G$ je $y = 12x + 3$.

$$x_g = 12^2 - 2 \cdot 9 = 1 - 5 = 9$$
$$y_g = 12 \cdot 9 + 3 = -9 + 3 = 7$$
$$6G = (9, -7) = (9, 6)$$

- $7G = (x_g, y_g) = 4G + 3G$

$$k = \frac{2 - 7}{12 - 9} = -5 \cdot 3^{-1} = -5 \cdot (-4) = 7$$
$$n = 2 - 7 \cdot 12 = 2 + 7 = 9$$

Jednačina prave koja prolazi kroz tačke $3G$ i $4G$ je $y = 7x + 9$.

$$x_g = 7^2 - 9 - 12 = 2$$
$$y_g = 7 \cdot 2 + 9 = 10$$
$$7G = (2, -10) = (12, 3)$$

- $8G = (x_g, y_g) = 4G + 4G$

$$k = \frac{3 \cdot 12^2 + 3}{2 \cdot 2} = 6 \cdot 4^{-1} = 6 \cdot (-3) = 8$$
$$n = 2 - 8 \cdot 12 = 2 + 8 = 10$$

Jednačina tangete koja prolazi kroz tačku $4G$ je $y = 8x + 10$.

$$x_g = 8^2 - 2 \cdot 12 = 12 + 2 = 1$$
$$y_g = 8 \cdot 1 + 10 = 5$$
$$8G = (1, -5) = (1, 8)$$

Dobili smo sve tačke iz skupa pa zaključujemo da tačka $G = (1, 5)$ jeste generator. Ostaje još da napravimo tabelu umnožaka:

n	0	1	2	3	4	5	6	7	8
nG	∅	(1,5)	(2, 10)	(9, 7)	(12, 2)	(12,11)	(9, 6)	(2, 3)	(1,8)

b) Na osnovu tabele sve tačke mogu da se predstava kao umnožak tačke G koja predstavlja generator skupa. Skup čini cikličnu grupu koja ima 9 tačaka pa ćemo umnoške generatora svoditi po modulu 9.

- (12,11)+(2,3) = 5G + 7G = 3G = (9, 7)
- (12,2)+(9,6) = 4G + 6G = G = (1,5)
- 25(9,7) = 25· 3G = 3G = (9, 7)

Zadatak 8.3 *Dokazati da eliptička kriva nad poljem $\mathbb{F}_p$ ima najviše $2p + 1$ tačku.*

Rešenje: Sve tačke krive su oblika $(x, y), x, y \in \mathbb{F}_p$. Zbog toga, za koordinatu x postoji najviše p mogućih vrednosti. Jednoj x koordinati odgovaraju najviše dve vrednosti za y (jednake po apsolutnoj vrednosti). To nam daje najviše $2p$ tačaka. Kada tome dodamo beskonačno udaljenu tačku dobijamo najviše $2p + 1$ tačku.

■

Zadatak 8.4 *Eliptička kriva koja se koristi za problem usaglašavanja ključeva Diffie-Helman protokola je $E : y^2 = x^3 + 3x + 8$ nad poljem $\mathbb{F}_{13}$. Ako se koristi generator $G = (2, 3)$, tajni ključevi $e_A = 4$, $e_B = 5$, odrediti tačku koja se dobija kao rezultat usaglašavanja.*

Rešenje: Javni podaci su $G = (2, 3)$ i $n = 13$. Radi lakšeg računa G ćemo predstaviti kao $7(1, 5)$ i koristićemo tabelu umnožaka koju smo napravili u zadatku 8.2.

Osoba A generiše svoj javni ključ G^{e_A}:

$$G^{e_A} = e_A \cdot G = 4(2, 3) = 28(1, 5) = (1, 5)$$

Osoba B generiše svoj javni ključ G^{e_B}:

$$G^{e_B} = e_B \cdot G = 5(2, 3) = 35(1, 5) = 8(1, 5) = (1, 8)$$

Kako bi se usaglasili, osoba A računa $(G^{e_B})^{e_A}$, a osoba B računa $(G^{e_A})^{e_B}$:

$$(G^{e_B})^{e_A} = 4 \cdot (1, 8) = 32(1, 5) = 5(1, 5) = (12, 11)$$
$$(G^{e_A})^{e_B} = 5 \cdot (1, 5) = (12, 11)$$

Zadatak 8.5 *Za sistem El Gamal koristi se eliptička kriva* $E : y^2 = x^3 + 3x + 8$ *nad poljem* $\mathbb{F}_{13}$. *Generator je* $G = (2, 3)$. *Ako su tajni ključevi* $e_A = 5$ *i* $e_B = 3$, *prikazati postupak šifrovanja poruke* $M = (12, 11)$ *(koristi se slučajan broj* $k = 4$*), a zatim postupak dešifrovanja šifrata.*

Rešenje: Javni parametri su $G = (2, 3)$ i $n = 13$. Osobe A i B generišu svoje javne ključeve:

$$G^{e_A} = e_A \cdot G = 5(2, 3) = 35(1, 5) = 8(1, 5) = (1, 8)$$
$$G^{e_B} = e_B \cdot G = 3(2, 3) = 21(1, 5) = 3(1, 5) = (9, 7)$$

Osoba A određuje vrednost maskirajućeg ključa G^k:

$$G^k = k \cdot G = 4(2, 3) = 28(1, 5) = (1, 5)$$

Zatim, osoba A šifruje poruku M pomoću maskirajućeg ključa i javnog ključa učesnika B:

$$G^{e_B k} = 4G^{e_B} = 4(9, 7) = 12(1, 5) = 3(1, 5) = (9, 7)$$
$$MG^{e_B k} = (12, 11) + (9, 7) = 5(1, 5) + 3(1, 5) = 8(1, 5) = (1, 8)$$

Osoba A šalje osobi B par $(MG^{e_B k}, G^k)$. Da bi osoba B dešifrovala poruku, prvo mora izračunati $G^{e_B k}$, a zatim $(G^{e_B k})^{-1}$. Dobijene vrednost primenjuje u formuli $MG^{e_B k}(G^{e_B k})^{-1}$ čime dobija M.

$$G^{e_B k} = 3G^k = 3(1, 5) = (9, 7)$$
$$(G^{e_B k})^{-1} = -(9, 7) = -3(1, 5) = 6(1, 5) = (9, 6)$$
$$MG^{e_B k}(G^{e_B k})^{-1} = (1, 8) + (9, 6) = 8(1, 5) + 6(1, 5) = 14(1, 5) = 5(1, 5) = (12, 11)$$

8.1 Programi

Zadatak 8.6 *Napisati Python klasu koja opisuje tačku na eliptičkoj krivoj oblika* $y^2 = x^3 + Ax + B$ *i implementira sabiranje dve tačke, dupliranje tačke, negiranje tačke i višesturko sabiranje tačke.*

Rešenje:

```
class Tacka:
    def __init__(self, x, y, p, a):
        self.x = x
        self.y = y
        self.p = p
        self.a = a


    def __str__(self):
        return f'({self.x}, {self.y})'


    def saberi(self, p):
        if p.x == 0 and p.y == 0:
            return self

        if self.x == 0 and self.y == 0:
            return p

        if self.x == p.x and self.y == p.y:
```

```
            return self.dupliraj()

        try:
            k = (p.y - self.y) * mod_inv(p.x - self.x, self.p) % self.p
            n = (self.y - k * self.x) % self.p
        except:
            return Tacka(0, 0, self.p, self.a)

        x = (mod_pow(k, 2, self.p) - p.x - self.x) % self.p
        y = (k * x + n) % self.p
        y = -y % self.p

        return Tacka(x, y, self.p, self.a)


    def dupliraj(self):
        if self.x == 0 and self.y == 0:
            return Tacka(0, 0, self.p, self.a)


        k = (3 * mod_pow(self.x, 2, self.p) + self.a) * mod_inv(2 * self.y, self.p) %
    ↪ self.p
        n = (self.y - k * self.x) % self.p

        x = (mod_pow(k, 2, self.p) - 2 * self.x) % self.p
        y = (k * x + n) % self.p
        y = -y % self.p

        return Tacka(x, y, self.p, self.a)


    def negiraj(self):
        return Tacka(self.x, -self.y % self.p, self.p, self.a)


    def pomnozi_skalarom(self, n):
        if n == 0:
            return Tacka(0, 0, self.p, self.a)

        if n == 1:
            return self

        if n % 2 == 1:
            return self.pomnozi_skalarom(n-1).saberi(self)

        else:
            return self.pomnozi_skalarom(n // 2).dupliraj()
```

Zadatak 8.7 *Napisati Python klasu koja opisuje eliptičku krivu oblika* $y^2 = x^3 + Ax + B$.

Rešenje: Implementacija se oslanja na klasu `Tacka`.

```
class Elipticka_kriva:
    def __init__(self, a, b, p, G):
        self.a = a
        self.b = b
        self.p = p
        self.G = G


    def tacka(self, x, y):
        return Tacka(x, y, self.p, self.a)
```

Zadatak 8.8 *Napisati Python program koji implementira protokol usaglašavanja ključeva Diffie-Helman korišćenjem eliptičke krive.*

Rešenje: Implementacija se sastoji iz klase `EK_DH` i glavnog dela programa koji koristi funkcionalnosti pomenute klase i prati protokol usaglašavanja ključeva.

```
class EK_DH(Elipticka_kriva):
    def __init__(self, a, b, p, G, pr = None):
        super().__init__(a, b, p, G)

        if pr == None:
            pr = random.randrange(2, p)

        self.pr = pr
        self.jav = G.pomnozi_skalarom(self.pr)


    def izracunaj_kljuc(self, jav):
        return jav.pomnozi_skalarom(self.pr)
```

```
def main():
    a = 3
    b = 8
    p = 13
    G = Tacka(2, 3, p, a)

    A = EK_DH(a, b, p, G, 4)
    B = EK_DH(a, b, p, G, 5)

    print(A.izracunaj_kljuc(B.jav))
    print(B.izracunaj_kljuc(A.jav))
```

Zadatak 8.9 *Napisati Python program koji implementira El Gamal protokol nad eliptičkom krivom.*

Rešenje: Implementacija se sastoji iz klase `EK_EG` i glavnog dela programa koji koristi funkcionalnosti pomenute klase i prati protokol za razmenu poruka.

```
class EK_EG(Elipticka_kriva):
    def __init__(self, a, b, p, G, pr = None, k = None):
        super().__init__(a, b, p, G)

        if pr == None:
            pr = random.randrange(2, p)

        self.pr = pr
        self.jav = G.pomnozi_skalarom(self.pr)

        if k == None:
            k = random.randrange(2, p)

        self.k = k
        self.kG = G.pomnozi_skalarom(self.k)


    def sifruj(self, M, jav):
        return M.saberi(jav.pomnozi_skalarom(self.k))


    def desifruj(self, kG, Me):
        return Me.saberi(kG.pomnozi_skalarom(self.pr).negiraj())
```

```
def main():
    a = 3
    b = 8
    p = 13
    G = Tacka(2, 3, p, a)

    A = EK_EG(a, b, p, G, 5, 4)
    B = EK_EG(a, b, p, G, 3)

    M = Tacka(12, 11, p, a)

    Me = A.sifruj(M, B.jav)
    Md = B.desifruj(A.kG, Me)

    print("Sifrovano:", Me)
    print("Desifrovano:", Md)
```

9 Digitalni potpis

Zadatak 9.1 *U sistemu autentikacije zasnovanom na RSA korisnik A je izabrao javni ključ $e = 7$ i $n = 77$. Ako je on od korisnika B dobio broj $M = 23$, kako treba da glasi njegov odgovor da bi sagovornika ubedio u svoj identitet?*

Rešenje: Javni podaci su n i e, dok se p, q i d čuvaju u tajnosti. Da bi korisnik B bio siguran da mu je korisnik A poslao poruku, korisnik A poslaće M^d, a B onda može da odredi $(M^d)^e$ jer je e javno.

Prvo ćemo odrediti d, a onda i M^d algoritmom stepenovanje kvadriranjem:

$$\begin{aligned}
\varphi(n) &= \varphi(77) = \varphi(7) \cdot \varphi(11) = 60 \\
d &= e^{-1}(mod\ \varphi(n)) = 7^{-1}(mod\ 60) = -17(mod\ 60) = 43(mod\ 60) \\
M^d &= 23^{43}(mod\ 77) = 23^{32} \cdot 23^8 \cdot 23^2 \cdot 23^1(mod\ 77) \\
& 23^2 \equiv 67 \\
& 23^8 \equiv (23^2)^4 \equiv (67^2)^2 \equiv 23^2 \equiv 67 \\
& 23^{32} \equiv (23^8)^4 \equiv (67^2)^2 \equiv 23^2 \equiv 67 \\
M^d &= 23^{32} \cdot 23^8 \cdot 23^2 \cdot 23^1(mod\ 77) = 67 \cdot 67 \cdot 67 \cdot 23(mod\ 77) = 23(mod\ 77)
\end{aligned}$$

Dakle, učesnik A odgovoriće brojem 23 kako bi uverila učesnika B u svoj identitet.

Zadatak 9.2 *Za digitalne potpise zasnovane na sistemu RSA korisnici A i B imaju javne ključeve $e_A = 3$, $n_A = 15$ i $e_B = 7$, $n_B = 77$. Korisnik B želi da pošalje poruku $M = 4$ kao potpis nekog teksta. Koji ceo broj on treba da pošalje?*

Rešenje: Prvo ćemo odrediti d_B, a onda i M^{d_B} algoritmom stepenovanje kvadriranjem:

$$\begin{aligned}
\varphi(n_B) &= \varphi(77) = \varphi(7) \cdot \varphi(11) = 60 \\
d_B &= e_B^{-1}(mod\ \varphi(n)) = 7^{-1}(mod\ 60) = -17(mod\ 60) = 43(mod\ 60) \\
M^d &= 4^{43}(mod\ 77) = 4^{32} \cdot 4^8 \cdot 4^2 \cdot 4^1(mod\ 77) \\
& 4^2 \equiv 16 \\
& 4^8 \equiv (4^2)^4 \equiv (16^2)^2 \equiv 25^2 \equiv 9 \\
& 4^{32} \equiv (4^8)^4 \equiv (9^2)^2 \equiv 4^2 \equiv 16 \\
M^d &= 4^{32} \cdot 4^8 \cdot 4^2 \cdot 4^1(mod\ 77) = 16 \cdot 9 \cdot 16 \cdot 4(mod\ 77) = 53(mod\ 77)
\end{aligned}$$

Dakle, učesnik B poslaće broj 53 kao potpis učesniku A.

Zadatak 9.3 *Dokazati da za digitalne potpise zasnovane na RSA važi sledeće tvrdjenje: Ako je S_1 potpis poruke m_1, a S_2 potpis poruke m_2, onda je S_1S_2 potpis poruke m_1m_2.*

Rešenje: Neka je $M = m_1m_2$ poruka koja predstavlja konkatenaciju poruka m_1 i m_2. Pošto je u pitanju RSA, važi

$$S_1 = m_1^d \ \text{ i } \ S_2 = m_2^d$$

Sada možemo razviti poruku koja se šifruje:

$$S = M^d = (m_1m_2)^d = m_1^d m_2^d = S_1S_2$$

■

Zadatak 9.4 *Opisati algoritam potpisivanja El Gamal za* $p = 677$, $g = 2$, $S = 316$, $e_A = 307$, $k = 401$.

Rešenje: Učesnik A čuva u tajnosti svoj privatni ključ e_A, a javni ključ g^{e_A} objavljuje:

$$\begin{aligned}
g^{e_A} = \; & 2^{307}(mod\ 677) = 2^{256} \cdot 2^{32} \cdot 2^{16} \cdot 2^2 \cdot 2^1(mod\ 677) \\
& 2^{16} \equiv (2^8)^2 \equiv 256^2 \equiv 544 \\
& 2^{32} \equiv (2^{16})^2 \equiv 544^2 \equiv 87 \\
& 2^{256} \equiv (2^{32})^8 \equiv (87^2)^4 \equiv (122^2)^2 \equiv 667^2 \equiv 100 \\
g^{e_A} = \; & 2^{256} \cdot 2^{32} \cdot 2^{16} \cdot 2^2 \cdot 2^1(mod\ 677) = 100 \cdot 87 \cdot 544 \cdot 4 \cdot 2(mod\ 677) = 498
\end{aligned}$$

Učesnik A računa vrednosti r i x i dobijene vrednosti zajedno sa S šalje učesniku B.

$$\begin{aligned}
r &= g^k(mod\ p) = 2^{401}(mod\ 677) \\
&= 2^{256} \cdot 2^{128} \cdot 2^{16} \cdot 2^1(mod\ 677) \\
&= 100 \cdot 667 \cdot 544 \cdot 2(mod\ 677) = 616
\end{aligned}$$

$$\begin{aligned}
x &= k^{-1}(S - e_A r)(mod\ \varphi(p)) \\
&= 401^{-1}(316 - 307 \cdot 616)(mod\ 676) \\
&= -59 \cdot (-192)(mod\ 676) = 512(mod\ 676)
\end{aligned}$$

Dakle, učesnik A šalje trojku $(616, 512, 316)$. Da bi se uverio daje A poslao poruku, učesnik B računa vrednosti g^S i $(g^{e_A})^r r^x$. Ukoliko su vrednosti jednake, onda B može biti siguran da je poruka stigla od učesnika A.

$$\begin{aligned}
g^S &= 2^{316}(mod\ 677) = 2^{256} \cdot 2^{32} \cdot 2^{16} \cdot 2^8 \cdot 2^4(mod\ 677) \\
&= 100 \cdot 87 \cdot 544 \cdot 256 \cdot 16(mod\ 677) = \underline{424(mod\ 677)}
\end{aligned}$$

$$\begin{aligned}
(g^{e_A})^r = \; & 498^{616}(mod\ 677) = 498^{512} \cdot 498^{64} \cdot 498^{32} \cdot 498^8(mod\ 677) \\
& 498^8 \equiv (498^2)^4 \equiv (222^2)^2 \equiv 540^2 \equiv 490 \\
& 498^{32} \equiv (498^8)^4 \equiv (490^2)^2 \equiv 442^2 \equiv 388 \\
& 498^{64} \equiv (498^{32})^2 \equiv 388^2 \equiv 250 \\
& 498^{512} \equiv (498^{64})^8 \equiv (250^2)^4 \equiv (216^2)^2 \equiv 620^2 \equiv 541 \\
(g^{e_A})^r = \; & 498^{512} \cdot 498^{64} \cdot 498^{32} \cdot 498^8(mod\ 677) = 541 \cdot 250 \cdot 388 \cdot 490 = 625
\end{aligned}$$

$$\begin{aligned}
r^x = \; & 616^{512}(mod\ 677) = (616^2)^{256}(mod\ 677) = (336^2)^{128}(mod\ 677) = (514^2)^{64}(mod\ 677) \\
& = (166^2)^{32}(mod\ 677) = (476^2)^{16}(mod\ 677) = (458^2)^8(mod\ 677) = (571^2)^4(mod\ 677) \\
& = (404^2)^2(mod\ 677) = 59^2(mod\ 677) = 96(mod\ 677)
\end{aligned}$$

$$(g^{e_A})^r r^x = 625 \cdot 96(mod\ 677) = \underline{424(mod\ 677)}$$

10 Verižni razlomci

Verižni razlomak je oblika:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

gde su a_i celi nenegativni brojevi i važi $a_i > 0$ za $i > 0$. Uobičajeno se verižni razlomci predstavljaju u zapisu $[a_0, a_1, a_2, \ldots, a_n]$. Racionalnim brojevima odgovaraju konačni verižni razlomci, dok iracionalnim brojevima odgovaraju beskonačni verižni razlomci oblika

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}}$$

Racionalni brojevi $a_0, a_0 + \dfrac{1}{a_1}, a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, \ldots$ su *konvergenti* odnosno *parcijalni razlomci* broja α.
Konvergente možemo odrediti po sledećim formulama:

$$\begin{array}{ll} P_{-1} = 1 & Q_{-1} = 0 \\ P_0 = a_0 & Q_0 = 1 \\ P_n = a_n P_{n-1} + P_{n-2} & Q_n = a_n Q_{n-1} + Q_{n-2} \end{array}$$

i-ti parcijalni razlomak ima vrednost: $\dfrac{P_i}{Q_i}$.

Zadatak 10.1 *Odrediti verižni razvoj datih brojeva i prvih 8 parcijalnih razlomaka:*

a) $\dfrac{107}{19}$

b) $\dfrac{7}{23}$

c) $\sqrt{3}$

d) $\sqrt{5}$

e) 1.625

f) π

Rešenje:

a) U pitanju je racionalan broj pa ćemo primeniti Euklidov algoritam:

$$\begin{aligned} 107 &= 5 \cdot 19 + 12 \\ 19 &= 1 \cdot 12 + 7 \\ 12 &= 1 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Svaka od jednakosti poslužiće za određivanje jednog a_i. Iz prve jednačine izvodimo:

$$\frac{107}{19} = 5 + \frac{12}{19}$$

Kako bismo dobili oblik verižnog razlomka, razlomak $\frac{12}{19}$ zapisujemo kao $\frac{1}{\frac{19}{12}}$. Za brojeve 19 i 12 koristimo drugu jednačinu dobijenu Euklidovim algoritmom. Isti postupak ćemo primeniti za ostale vrednosti pa dobijamo:

$$\frac{107}{19} = 5 + \frac{12}{19} = 3 + \frac{1}{\frac{19}{12}} = 5 + \frac{1}{1 + \frac{7}{12}} = 5 + \frac{1}{1 + \frac{1}{\frac{12}{7}}} = 5 + \frac{1}{1 + \frac{1}{1 + \frac{5}{7}}}$$

$$= 5 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{7}{5}}}} = 5 + \frac{1}{1 + \frac{1}{1 + \frac{2}{5}}} = \underline{5} + \frac{1}{\underline{1} + \frac{1}{\underline{1} + \frac{1}{\underline{2} + \frac{1}{\underline{2}}}}}$$

Dakle, traženi verižni razvoj je $[5, 1, 1, 1, 2, 2]$. Primetimo da su to količnici dobijeni Euklidovim algoritmom. Odredimo i konvergente:

n	-1	0	1	2	3	4	5
a_n		5	1	1	1	2	2
P_n	1	5	6	11	17	45	107
Q_n	0	1	1	2	3	8	19
$\frac{P_n}{Q_n}$		5	6	5.5	5.666...	5.625	5.6315...

b) $\frac{7}{23}$ je racionalan broj pa možemo primeniti Euklidov algoritam:

$$\begin{aligned} 7 &= \underline{0} \cdot 23 + 7 \\ 23 &= \underline{3} \cdot 7 + 2 \\ 7 &= \underline{3} \cdot 2 + 1 \\ 2 &= \underline{2} \cdot 1 + 0 \end{aligned}$$

Iz ovoga dobijamo da je verižni razvoj:

$$\frac{7}{23} = 0 + \frac{1}{\frac{23}{7}} = 0 + \frac{1}{3 + \frac{1}{\frac{7}{2}}} = 0 + \frac{1}{3 + \frac{1}{3 + \frac{1}{2}}}$$

odnosno $[0, 3, 3, 2]$. Odredimo i konvergente:

n	-1	0	1	2	3
a_n		0	3	3	2
P_n	1	0	1	3	7
Q_n	0	1	3	10	23
$\frac{P_n}{Q_n}$		0	0.333...	0.3	0.304...

c) Kako je broj $\sqrt{3}$ iracionalan broj, nećemo moći da primenimo Euklidov algoritam. Zato ćemo se poslužiti jednim trikom. Odredićemo najbliži ceo broj broju $\sqrt{3}$ koji je manji od $\sqrt{3}$. Kako važi $1 < \sqrt{3} < 2$, biramo broj 1. Broju $\sqrt{3}$ dodajemo i oduzimamo broj 1, čime dobijamo $a_0 = 1$:

$$\sqrt{3} = \sqrt{3} + 1 - 1 = 1 + (\sqrt{3} - 1) = 1 + \cfrac{1}{\cfrac{1}{\sqrt{3}-1}}$$

Postupak nastavljamo za $\cfrac{1}{\sqrt{3}-1}$. Ovaj razlomak možemo racionalizovati množenjem sa $\cfrac{\sqrt{3}+1}{\sqrt{3}+1}$.

$$\frac{1}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1} = \frac{\sqrt{3}+1}{3-1} = \frac{\sqrt{3}+1}{2}$$

Ponovo ćemo se poslužiti trikom dodavanja i oduzimanja najbližeg manjeg celog broja. Sada posmatramo broj $\cfrac{\sqrt{3}+1}{2}$. Važi $2 < \sqrt{3}+1 < 3$. Dakle, broj koji bismo dodali je 2. Međutim, pošto sad imamo razlomak, treba nam da se u brojiocu pojavi broj koji će biti deljiv imeniocem pa dodajemo 2-1=1.

$$\frac{\sqrt{3}+1}{2} = \frac{\sqrt{3}+1+1-1}{2} = 1 + \frac{\sqrt{3}-1}{2} = 1 + \cfrac{1}{\cfrac{2}{\sqrt{3}-1}}$$

Ponovićemo istu stvar za $\cfrac{2}{\sqrt{3}-1}$:

$$\frac{2}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1} = \frac{2(\sqrt{3}+1)}{3-1} = \sqrt{3}+1+2-2 = 2 + \cfrac{1}{\cfrac{1}{\sqrt{3}-1}}$$

Dalje se nastavlja postupak za $\cfrac{1}{\cfrac{1}{\sqrt{3}-1}}$. Međutim, tu vrednost smo već izračunali i nema potrebe da ponavljamo. Iz toga znamo da će se beskonačno ponavljati brojevi 1 i 2 pa je verižni razvoj

$$1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}}$$

odnosno $[1, 1, 2, \overline{1, 2}, \ldots]$. Odredimo i konvergente:

n	-1	0	1	2	3	4	5	6	7
a_n		1	1	2	1	2	1	2	1
P_n	1	1	2	5	7	19	26	71	97
Q_n	0	1	1	3	4	11	15	41	56
$\frac{P_n}{Q_n}$		1	2	1.666...	1.75	1.727...	1.733...	1.731...	1.732...

d) $\sqrt{5}$ je iracionalan broj pa se služimo trikom iz dela pod c). Važi $2 < \sqrt{5} < 3$.

$$\sqrt{5} = 2 + \sqrt{5} - 2 = 2 + \cfrac{1}{\cfrac{1}{\sqrt{5}-2}}$$

$$\frac{1}{\sqrt{5}-2} \cdot \frac{\sqrt{5}+2}{\sqrt{5}+2} = \frac{\sqrt{5}+2}{5-4} = \sqrt{5}+2+2-2 = 4 + \cfrac{1}{\cfrac{1}{\sqrt{5}-2}}$$

U ovom slučaju ponavlja se $\dfrac{1}{\sqrt{5}-2}$ pa je verižni razvoj:

$$2 + \cfrac{1}{4 + \cfrac{1}{4 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}}$$

odnosno $[2, 4, \overline{4}, \ldots]$. Odredimo i konvergente:

n	-1	0	1	2	3	4	5	6	7
a_n		2	4	4	4	4	4	4	4
P_n	1	2	9	38	161	682	2889	12238	51841
Q_n	0	1	4	17	72	305	1292	5473	23184
$\frac{P_n}{Q_n}$		2	2.25	2.235...	2.2361...	2.236065...	2.236068...	2.236067...	2.23602...

e) Ukoliko broj nije zadat kao razlomak već u decimalnom zapisu, možemo primeniti sledeći postupak. Prvo računamo $a_0 = \lfloor x \rfloor$ (najveći ceo broj koji je manji od x). U ovom slučaju, $a_0 = 1$. Dalje, određujemo vrednost x_1:

$$x_1 = \frac{1}{x - a_0} = 1.6$$

Sledeće a_i dobijamo zaokruživanjem vrednosti x_1 odnosno $a_1 = \lfloor x_1 \rfloor = 1$. Postupak nastavljamo računanjem vrednosti x_2:

$$x_2 = \frac{1}{x_1 - a_1} \approx 1.666...$$

i određivanjem a_2 na isti način. Dakle, $a_2 = 1$. Odredimo i ostale vrednosti:

$$x_3 = \frac{1}{x_2 - a_2} = 1.5 \qquad a_3 = 1$$

$$x_4 = \frac{1}{x_3 - a_3} = 2 \qquad a_4 = 2$$

Možemo da stanemo kad x_i postane ceo broj. Napravimo tabelu konvergenata:

n	-1	0	1	2	3	4
a_n		1	1	1	1	2
P_n	1	1	2	3	5	13
Q_n	0	1	1	2	3	8
$\frac{P_n}{Q_n}$		1	2	1.5	1.666...	1.625

f) Primenićemo isti postupak kao u delu pod e):

$$
\begin{aligned}
a_0 &= \lfloor \pi \rfloor = 3 \\
x_1 &= \frac{1}{x - a_0} \approx 7.06251... \\
a_1 &= 7 \\
x_2 &= \frac{1}{x_1 - a_1} \approx 15.9965... \\
a_2 &= 15 \\
x_3 &= \frac{1}{x_2 - a_2} \approx 1.0034... \\
a_3 &= 1 \\
x_4 &= \frac{1}{x_3 - a_3} \approx 292.63459... \\
a_4 &= 292 \\
x_5 &= \frac{1}{x_4 - a_4} \approx 1.57581... \\
a_5 &= 1 \\
x_6 &= \frac{1}{x_5 - a_5} \approx 1.73665... \\
a_6 &= 1 \\
x_7 &= \frac{1}{x_6 - a_6} \approx 1.35747... \\
a_7 &= 1
\end{aligned}
$$

Napravimo tabelu konvergenata:

n	-1	0	1	2	3	4	5	6	7
a_n		3	7	15	1	292	1	1	1
P_n	1	3	22	333	355	103993	104348	208341	312689
Q_n	0	1	7	106	113	33102	33215	66317	99532
$\frac{P_n}{Q_n}$		3	3.142..	3.14150..	3.1415929..	3.1415926530..	3.1415926539..	3.1415926534..	3.1415926536..

Zadatak 10.2 *Dokazati da za svaki prirodan broj n važi* $P_n \cdot Q_{n-1} - P_{n-1}Q_n = (-1)^{n-1}$.

Rešenje: Dokaz ćemo izvesti matematičkom indukcijom. Dokaz ćemo izvesti matematičkom indukcijom.

Baza indukcije: Za n = 0 važi $P_0 \cdot Q_{-1} - P_{-1}Q_0 = a_0 \cdot 0 - 1 \cdot 1 = -1 = (-1)^{-1}$.

Induktivna hipoteza: Pretpostavimo da za $n \geq 1$ važi $P_n \cdot Q_{n-1} - P_{n-1}Q_n = (-1)^{n-1}$.

Induktivni korak: Treba dokazati da važi $P_{n+1} \cdot Q_n - P_nQ_{n+1} = (-1)^n$.

$$
\begin{aligned}
P_{n+1} \cdot Q_n - P_nQ_{n+1} &= (a_nP_n + P_{n-1})Q_n - P_n(a_nQ_n + Q_{n-1}) \\
&= \cancel{a_nP_nQ_n} + P_{n-1}Q_n \cancel{- a_nP_nQ_n} - P_nQ_{n-1} \\
&= -(P_nQ_{n-1} - P_{n-1}Q_n) = -(-1)^{n-1} = (-1)^n
\end{aligned}
$$

■

10.1 Programi

Zadatak 10.3 *Napisati Python funkciju za određivanje verižnog razvoja zadatog broja.*

Rešenje:

```
import math

def verizni_razlomak(x, bk = 8):
    a = math.floor(x)

    razlomak = [a]

    for i in range(bk-1):
        if x == a:
            break

        x = 1 / (x - a)
        a = math.floor(x)
        razlomak.append(a)

    return razlomak
```

Zadatak 10.4 *Napisati Python funkciju za određivanje vrednosti parcijalnog razlomka na osnovu verižnog razvoja.*

Rešenje:

```
def konvergenti(a):
    n = len(a)

    p = [1, a[0]]
    q = [0, 1]

    for i in range(2, n+1):
        p.append(a[i-1] * p[i-1] + p[i-2])
        q.append(a[i-1] * q[i-1] + q[i-2])

    return p, q
```

10.2 Zadaci za vežbu

Zadatak 10.1 *Odrediti verižni razvoj i prvih 10 parcijalnih razlomaka sledećih brojeva:* $\frac{27}{8}$, 0.7241, e, $\frac{13}{57}$, $\sqrt{7}$.

11 Linearni pomerački registar

Zadatak 11.1 *Odrediti orbite za* $n = 3$, $(b_0, b_1, b_2) = (1, 1, 0)$, $(k_0, k_1, k_2) = (0, 1, 1)$.

Rešenje: Znamo da je polinom $g(x) = 1 + x + x^3$ nesvodljiv u $\mathbb{F}_2$ i važi da je x generator[8] $\mathbb{F}_{2^n}^* = \mathbb{F}[x]/(g(x))$ pa znamo da ćemo dobiti orbitu maksimalne dužine. Početno stanje je $(0, 1, 1)$, a funkcija kojom se dobija poslednji bit narednog stanja je

$$f(s_0, s_1, s_2) = 1 \cdot s_0 + 1 \cdot s_1 + 0 \cdot s_2 = s_0 + s_1$$

Orbita veličine $2^3 - 1$ izgleda ovako:

s_0	s_1	s_2
0	1	1
1	1	1
1	1	0
1	0	0
0	0	1
0	1	0
1	0	1
0	1	1

Zadatak 11.2 *Odrediti orbite za* $n = 4$, $(b_0, b_1, b_2, b_3) = (1, 0, 1, 0)$, $(k_0, k_1, k_2, k_3) = (0, 1, 1, 1)$.

Rešenje: Znamo da je polinom $g(x) = 1+x^2+x^4$ nije nesvodljiv u $\mathbb{F}_2$ jer je jednak polinomu $(1+x+x^2)^2$ pa znamo da nećemo dobiti orbitu maksimalne dužine. Početno stanje je $(0, 1, 1, 1)$, a funkcija kojom se dobija poslednji bit narednog stanja je

$$f(s_0, s_1, s_2, s_3) = 1 \cdot s_0 + 0 \cdot s_1 + 1 \cdot s_2 + 0 \cdot s_3 = s_0 + s_2$$

Orbite izgledaju ovako:

s_0	s_1	s_2	s_3
0	1	1	1
1	1	1	1
1	1	1	0
1	1	0	0
1	0	0	1
0	0	1	1
0	1	1	1

s_0	s_1	s_2	s_3
0	0	0	1
0	0	1	0
0	1	0	1
1	0	1	0
0	1	0	0
1	0	0	0
0	0	0	1

s_0	s_1	s_2	s_3
0	1	1	0
1	1	0	1
1	0	1	1
0	1	1	0

Dakle, dobijene su 3 orbite dužune, redom, 6, 6 i 3.

Zadatak 11.3 *Odrediti orbite za* $n = 4$, $(b_0, b_1, b_2, b_3) = (1, 0, 0, 1)$, $(k_0, k_1, k_2, k_3) = (0, 1, 1, 1)$.

Rešenje: Polinom $g(x) = 1 + x^3 + x^4$ je nesvodljiv u $\mathbb{F}_2$ i važi da je x generator[9] $\mathbb{F}_{2^n}^* = \mathbb{F}[x]/(g(x))$ pa znamo da postoji jedna orbita maksimalne dužine.

[8] Proveriti za vežbu.
[9] Proveriti za vežbu.

Zadatak 11.4 *Odrediti orbite za polinome:*

a) $1 + x^2 + x^3 + x^4$

b) $1 + x + x^5$

c) $1 + x + x^6$

d) $1 + x^3 + x^5$

Rešenje:

a) Polinom $g(x) = 1 + x^2 + x^3 + x^4$ može se rastaviti na proizvod polinoma $(x^3 + x + 1)$ i $(x + 1)$. Na osnovu polinoma $g(x)$ dobijamo informacije $n = 4$ i $(b_0, b_1, b_2, b_3) = (1, 0, 1, 1)$. Iz toga zaključujemo da ima $2^4 - 1 = 15$ stanja, a funkcija kojom se dobija poslednji bit narednog stanja je

$$f(s_0, s_1, s_2, s_3) = s_0 + s_2 + s_3$$

Pošto polinom $g(x)$ nije svodljiv, nema maksimalne orbite pa je potrebno da ih odredimo. Za svaku orbitu uzećemo proizvoljnu kombinaciju koja do tada nije iskorišćena.

s_0	s_1	s_2	s_3
0	0	0	1
0	0	1	1
0	1	1	0
1	1	0	1
1	0	1	0
0	1	0	0
1	0	0	0
0	0	0	1

s_0	s_1	s_2	s_3
0	0	1	0
0	1	0	1
1	0	1	1
0	1	1	1
1	1	1	0
1	1	0	0
1	0	0	1
0	0	1	0

s_0	s_1	s_2	s_3
1	1	1	1
1	1	1	1

Dakle, dobijene su 3 orbite dužune, redom, 7, 7, 1.

b) Polinom $g(x) = 1+x+x^5$ nije nesvodljiv jer predstavlja proizvod polinoma (x^3+x^2+1) i (x^2+x+1). Na osnovu polinoma $g(x)$ dobijamo informacije $n = 5$ i $(b_0, b_1, b_2, b_3, b_4) = (1, 1, 0, 0, 0)$. Iz toga zaključujemo da ima $2^5 - 1 = 31$ stanje, a funkcija kojom se dobija poslednji bit narednog stanja je

$$f(s_0, s_1, s_2, s_3, s_4) = s_0 + s_1$$

Pošto polinom $g(x)$ nije svodljiv, nema maksimalne orbite pa je potrebno da ih odredimo. Za svaku orbitu uzećemo proizvoljnu kombinaciju koja do tada nije iskorišćena.

s_0	s_1	s_2	s_3	s_4
0	0	0	0	1
0	0	0	1	0
0	0	1	0	0
0	1	0	0	0
1	0	0	0	1
0	0	0	1	1
0	0	1	1	0
0	1	1	0	0
1	1	0	0	1
1	0	0	1	0
0	0	1	0	1
0	1	0	1	0
1	0	1	0	1
0	1	0	1	1
1	0	1	1	1
0	1	1	1	1
1	1	1	1	1
1	1	1	1	0
1	1	1	0	0
1	1	0	0	0
1	0	0	0	0
0	0	0	0	1

s_0	s_1	s_2	s_3	s_4
1	1	1	0	1
1	1	0	1	0
1	0	1	0	0
0	1	0	0	1
1	0	0	1	1
0	0	1	1	1
0	1	1	1	0
1	1	1	0	1

s_0	s_1	s_2	s_3	s_4
1	1	0	1	1
1	0	1	1	0
0	1	1	0	1
1	1	0	1	1

Dakle, dobijene su 3 orbite dužune, redom, 21, 7 i 3.

c) Polinom $g(x) = 1+x+x^6$ je nesvodljiv[10] u $\mathbb{F}_2$. Da bismo dobili orbitu maksimalne dužine potrebno je i da x bude generator. To možemo proveriti računanjem vrednosti x^k za $k \in [0, 63]$ i proverom da li su generisani svi članovi skupa. Međutim, postoji i lakši način. Dovoljno je da proverimo da li je $x^{63} = 1$ i da li neki delilac broja 63 generiše cikličnu grupu, odnosno treba da proverimo da li $x^k \neq 1 \ \forall k \mid 63$. U ovom slučaju, $k \in \{3, 7, 9, 21\}$ pa ćemo odrediti x^k za te vrednosti. Vodimo računa da je $x^6 = x + 1$.

$$
\begin{aligned}
x^3 &= x^3 \neq 1 \\
x^7 &= x^6 \cdot x = x^2 + x \neq 1 \\
x^9 &= x^7 \cdot x^2 = x^4 + x^2 \neq 1 \\
x^{21} &= (x^2 + x)^3 = (x^4 + x^2)(x^2 + x) = x^5 + x^4 + x^3 + x + 1 \neq 1
\end{aligned}
$$

Nijedan delilac broja 63 ne pravi cikličnu grupu, što znači da ima nade da je x generator. Moramo proveriti i da li je x^{63}. To najbrže određujemo algoritmom stepenovanje kvadriranje pri čemu znamo da je $63 = 32 + 16 + 8 + 4 + 2 + 1$.

$$
\begin{aligned}
x^8 &= x^6 \cdot x^2 = x^3 + x^2 \\
x^{16} &= (x^8)^2 = (x^3 + x^2)^2 = x^6 + x^5 + x^5 + x^4 = x^4 + x + 1 \\
x^{32} &= (x^{16})^2 = (x^4 + x + 1)^2 = x^8 + \cancel{x^5} + \cancel{x^4} + \cancel{x^5} + x^2 + \cancel{x} + \cancel{x^4} + \cancel{x} + 1 = x^3 + 1
\end{aligned}
$$

[10] Proveriti za vežbu. Dovoljno je proveriti da li je deljiv nesvodljivim polinomima stepena 1, 2 i 3.

Sada se lako izračunava x^{63}:

$$\begin{aligned}
x^{63} &= x^{32} \cdot x^{16} \cdot x^8 \cdot x^4 \cdot x^2 \cdot x \\
&= (x^3+1)(x^4+x+1)(x^3+x^2)(x^2+x) \\
&= (x^7 + \cancel{x^4} + x^3 + \cancel{x^4} + x + 1)(x^5 + \cancel{x^4} + \cancel{x^4} + x^3) \\
&= (x^2 + \cancel{x} + x^3 + \cancel{x} + 1)(x^5 + x^3) \\
&= (x^3 + x^2 + 1)(x^5 + x^3) \\
&= x^8 + x^6 + x^7 + \cancel{x^5} + \cancel{x^5} + x^3 \\
&= \cancel{x^3} + \cancel{x^2} + \cancel{x} + 1 + \cancel{x^2} + \cancel{x} + \cancel{x^3} \\
&= 1
\end{aligned}$$

Sve provere su prošle, možemo zaključiti da je x generator i da je orbita maksimalne dužine.

d) Polinom $g(x) = 1 + x^3 + x^5$ je nesvodljiv[11] u $\mathbb{F}_2$ i važi da je x generator[12] $\mathbb{F}_{2^n}^* = \mathbb{F}[x]/(g(x))$ pa znamo da postoji jedna orbita maksimalne dužine $(2^5 - 1)$.

Zadatak 11.5 *Odrediti povratne sprege i linearne pomeračke registre na osnovu otvorenog teksta* $OT = [4, 0] = [00100, 00000]$ *i šifrovanog teksta* $ST = [17, 30] = [10001, 11110]$.

Rešenje:

OT	0	0	1	0	0	0	0	0	0	0
ST	1	0	0	0	1	1	1	1	1	0
niz ključa	1	0	1	0	1	1	1	1	1	0
	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9

$$\begin{aligned}
k_5 &= f(k_0, k_1, k_2, k_3, k_4) = b_0k_0 + b_1k_1 + b_2k_2 + b_3k_3 + b_4k_4 = b_0 + b_2 + b_4 = 1 \\
k_6 &= f(k_1, k_2, k_3, k_4, k_5) = b_1 + b_3 + b_4 = 1 \\
k_7 &= f(k_2, k_3, k_4, k_5, k_6) = b_0 + b_2 + b_3 + b_4 = 1 \\
k_8 &= f(k_3, k_4, k_5, k_6, k_7) = b_1 + b_2 + b_3 + b_4 = 1 \\
k_9 &= f(k_4, k_5, k_6, k_7, k_8) = b_0 + b_1 + b_2 + b_3 + b_4 = 0
\end{aligned}$$

[11] Proveriti za vežbu. Dovoljno je proveriti da li je deljiv nesvodljivim polinomima stepena 1 i 2.
[12] Proveriti za vežbu. Dovoljno je proveriti da li je $x^{31} = 1$ pošto je broj 31 prost.

Iz ovoga dobijamo sistem jedačina:

$$
\begin{array}{cccccccccc}
b_0 & & & + & b_2 & & & + & b_4 & = 1 \\
 & & b_1 & & & + & b_3 & + & b_4 & = 1 \\
b_0 & & & + & b_2 & + & b_3 & + & b_4 & = 1 \\
 & & b_1 & + & b_2 & + & b_3 & + & b_4 & = 1 \\
b_0 & + & b_1 & + & b_2 & + & b_3 & + & b_4 & = 0 \\
\hline
b_0 & = & 1 & & & & & & & \\
 & & b_2 & & & + & b_4 & = 0 & & \\
b_1 & & & + & b_3 & + & b_4 & = 1 & & \\
 & & b_2 & + & b_3 & + & b_4 & = 0 & & \\
b_1 & + & b_2 & + & b_3 & + & b_4 & = 1 & & \\
\hline
b_0 & = & 1 & & & & & & & \\
b_1 & = & 1 & & & & & & & \\
b_2 & & & + & b_4 & = 0 & & & & \\
 & & b_3 & + & b_4 & = 0 & & & & \\
b_2 & + & b_3 & + & b_4 & = 0 & & & & \\
\hline
b_0 & = & 1 & & & & & & & \\
b_1 & = & 1 & & & & & & & \\
b_2 & = & 0 & & & & & & & \\
b_3 & = & 0 & & & & & & & \\
b_4 & = & 0 & & & & & & &
\end{array}
$$

Rešavanjem sistema dobili smo povratnu spregu $(b_0, b_1, b_2, b_3, b_4) = (1, 1, 0, 0, 0)$, odnosno $g(x) = 1 + x + x^5$.

11.1 Programi

Zadatak 11.6 *Napisati Python funkciju za određivanje* $\boldsymbol{d}$ *bitova ključa koji se dobija linearnim pomeračkim registrom sa povratnom spregom* $\boldsymbol{b}$ *počevši iz stanja* $\boldsymbol{s}$.

Rešenje:

```
def lpr(b, s, d):
    stanje_registra = [i for i in s]
    kljuc = []
    n = len(b)

    for j in range(d):
        novi_bit = 0
        for i in range(n):
            novi_bit = novi_bit ^ b[i] * stanje_registra[i]

        kljuc.append(stanje_registra[0])
        stanje_registra = stanje_registra[1:] + [novi_bit]

    return kljuc
```

12 Slučajno lutanje

U toku slučajnog lutanja po skupu od n elemenata, posle otprilike $1.2\sqrt{n}$ koraka očekuje se nailazak na već ranije pregledani element. Polardov ρ-metod koristi upravo tu činjenicu. Očekivani broj koraka povratka u neki već viđenu tačku je $O(\sqrt{n})$.

12.1 Faktorizacija algoritmom slučajnog lutanja

Da bi smo rastavili broj n na činioce, iteriramo funkciju $f(x)(mod\ n)$ polazeći od vrednosti a_0 i time dobijamo slučajno lutanje kroz $\mathbb{Z}/n\mathbb{Z}$. Vrednost a_i dobija se primenom funkcija na prethodu vrednost a_{i-1}, odnosno $a_i = f(a_{i-1})(mod\ n)$. Vrednosti a_i računamo dok važi $NZD(a_{2j} - a_j, n) = 1$. U trenutku kada pronađemo dva broja koja nisu uzajamno prosti odnosno $NZD(a_{2j} - a_j, n) = p \neq 1$, dobili smo jedan faktor p. Drugi se dobija kao količnik pri deljenju n sa p odnosno $q = \frac{n}{p}$.

Zadatak 12.1 *Algoritmom slučajnog lutanja faktorisati sledeće brojeve ako se koristi* $f(x) = x^2 + 1(mod\ n)$ *i* $a_0 = 0$*:*

a) 1357

b) 14873

c) 957

Rešenje:

a) Potrebno je da odredimo vrednosti za a_i $i \geq 0$ dok ne naiđemo na vrednosti a_{2i} i a_i koje nisu uzajamno proste.

i	0	1	2	3	4	5	6	7	8	9	10	11	12
a_i	0	1	2	5	26	677	1021	266	193	611	146	1255	906

$NZD(2-1, 1357) = 1$
$NZD(26-2, 1357) = 1$
$NZD(1021-5, 1357) = 1$
$NZD(193-26, 1357) = 1$
$NZD(146-677, 1357) = NZD(827, 1357) = 1$
$NZD(906-1021, 1357) = NZD(1242, 1357) = 23 = p$

Za $i = 6$ dolazimo do brojeva koji nisu uzajamno prosti. Njihov NZD predstavlja jedan od faktora broja n. Na osnovu toga lako dolazimo i do drugih:

$$q = \frac{n}{p} = \frac{1357}{23} = 59.$$

Vrednosti p i q su prosti brojevi pa se postupak ovde završava. Dakle, $n = 1357 = 23 \cdot 59$

b)

i	0	1	2	3	4	5	6	7	8
a_i	0	1	2	5	26	677	12140	3044	58
i		9	10	11	12	13	14	15	16
a_i		3365	4873	8822	12149	13423	5408	6147	8190

$NZD(2-1, 1357) = 1$
$NZD(26-2, 1357) = 1$
$NZD(12140-5, 1357) = 1$
$NZD(58-26, 1357) = 1$
$NZD(4873-677, 1357) = 1$
$NZD(12149-12140, 1357) = 1$
$NZD(8190-58, 1357) = 107 = p$

Za $i = 8$ dolazimo do brojeva koji nisu uzajamno prosti. Upravo njihov NZD predstavlja jedan od faktora broja n. Na osnovu toga lako dolazimo i do drugih:

$$q = \frac{n}{p} = \frac{14873}{107} = 139.$$

Vrednosti p i q su prosti brojevi pa se postupak ovde završava. Dakle, $n = 14873 = 107 \cdot 139$

Primena slučajnog lutanja na problem diskretnog logaritma sa eliptičkim krivama

Zadata je eliptička kriva $E : y^2 = x^3 + Ax + B$ nad F_q. Generator krive je tačka G i važi $mG = \varnothing$ (zbog čega se tačke množe celim brojevima po modulu m). Zadata je tačka $Q = (x, y) = nG$ i potrebno je odrediti broj n. To se može odrediti slučajnim lutanjem kroz $E(F_q)$. Neka je $P_0 = \varnothing$ i $v_0 = [0, 0]$. Vektoru $v_i = [a_i, b_i]$ odgovara tačka $P_i = a_iQ + b_iG$, gde su a_i i b_i ostaci po modulu m. Algoritam se primenjuje na sledeći način[13]:

- $P_i = \varnothing \ \vee \ x(P_i) \leq 33 \quad \Rightarrow \quad P_i = Q + P, v_{i+1} = v_i + [1, 0],$
- $33 < x(P_i) < 68 \quad \Rightarrow \quad P_i = 2P_i, v_{i+1} = 2v_i,$
- $x(P_i) \geq 68 \quad \Rightarrow \quad P_i = G + P_i, v_{i+1} = v_i + [0, 1]$

Računanje se ponavlja dok se ne pronađu dve tačke tako da važi $P_{2j} = P_j$. Tada određujemo broj n izvođenjem ove jednakosti:

$$\begin{aligned}
&P_{2j} = P_j \\
&a_{2j}Q + b_{2j}G = a_jQ + b_jG \\
&(a_{2j} - a_j)Q = (b_j - b_{2j})G \\
&Q = (a_{2j} - a_j)^{-1}(b_j - b_{2j})G = nG \\
&n = (a_{2j} - a_j)^{-1}(b_j - b_{2j})
\end{aligned}$$

pri čemu se račun vrši po modulu m.

[13] $x(P_i)$ označava x koordinatu tačke P_i

Zadatak 12.2 *Odrediti n tako da je $Q(5,98) = n \cdot G$ algoritmom slučajnog lutanja, ako je data eliptička kriva $E : y^2 = x^3 + 17x + 1$ u polju F_{101}, gde je $G(0,1)$ generator i važi $103 \cdot G = \varnothing$.*

Rešenje:

$$
\begin{aligned}
P_0 &= \varnothing & v_0 &= [0,0] \\
P_1 &= P_0 + Q = (5,98) & v_1 &= [1,0] \\
P_2 &= P_1 + Q = (68,60) & v_2 &= [2,0] \\
P_3 &= P_2 + G = (63,29) & v_3 &= [2,1] \\
P_4 &= 2P_3 = (12,32) & v_4 &= [4,2] \\
P_5 &= P_4 + Q = (8,89) & v_5 &= [5,2] \\
P_6 &= P_5 + Q = (97,77) & v_6 &= [6,2] \\
P_7 &= P_6 + G = (62,66) & v_7 &= [6,3] \\
P_8 &= 2P_7 = (53,81) & v_8 &= [12,6] \\
P_9 &= 2P_8 = (97,77) & v_9 &= [24,12] \\
P_{10} &= P_9 + G = (62,66) & v_{10} &= [24,13] \\
P_{11} &= 2P_{10} = (53,81) & v_{11} &= [48,26] \\
P_{12} &= 2P_{11} = (97,77) & v_{12} &= [96,52]
\end{aligned}
$$

Dobijamo dve jedanke tačke za $j = 6$ ($P_6 = P_{12}$). Primetimo da važi i $P_6 = P_9$, ali $2 \cdot 6 \neq 9$ (slično za $P_7 = P_{10}$ i $P_8 = P_{11}$) pa smo morali da nastavimo sa računom. Sada možemo da odredimo broj n:

$$n = (96-6)^{-1}(2-52) = 90^{-1}(-50) = (-8)(-50) = 91$$

Dakle, $Q = 91G$.

Primena slučajnog lutanja na problem diskretnog u konačnom polju

Dato je konačno polje F_q, generator g i broj $y = g^x$. Potrebno je odrediti broj x. Definišemo slučajno lutanje kroz F_{101}^*. Neka je $c_0 = 1$ i $v_0 = [0,0]$. Vektoru $v_i = [a_i, b_i]$ odgovara $c_i = y^{a_i} g^{b_i}$, pri čemu su brojevi a_i i b_i ostaci po modulu $\varphi(q)$ tj. $q-1$. Algoritam se primenjuje na sledeći način:

- $c_i \leq 33 \;\Rightarrow\; c_{i+1} = c_i y, v_{i+1} = v_i + [1,0]$,
- $33 < c_i < 68 \;\Rightarrow\; c_{i+1} = c_i^3, v_{i+1} = 3v_i$,
- $c_i \geq 68 \;\Rightarrow\; c_{i+1} = c_i g, v_{i+1} = v_i + [0,1]$,

Računanje se ponavlja dok se ne pronađu dva broja tako da važi $c_{2j} = c_j$. Tada određujemo broj x izvođenjem ove jednakosti:

$$
\begin{aligned}
& c_{2j} = c_j \\
& y^{a_{2j}} g^{b_{2j}} = y^{a_j} g^{b_j} \\
& y^{a_{2j} - a_j} = g^{b_j - b_{2j}} \\
& y = g^{(b_j - b_{2j})(a_{2j} - a_j)} = g^x \\
& x = (b_j - b_{2j})(a_{2j} - a_j)
\end{aligned}
$$

pri čemu se račun vrši po modulu $q-1$.

Zadatak 12.3 *Ako se zna da je $g = 2$ generator za F_{101}, odrediti x tako da je $y = 86 = g^x$ primenom algoritma lutanja kroz F_{101}.*

Rešenje:

$$\begin{aligned} c_0 &= 0 & v_0 &= [0,0] \\ c_1 &= c_0 y = 86 & v_1 &= [1,0] \\ c_2 &= c_1 g = 71 & v_2 &= [1,1] \\ c_3 &= c_2 g = 41 & v_3 &= [1,2] \\ c_4 &= c_3^3 = 39 & v_4 &= [3,6] \\ c_5 &= c_4^3 = 32 & v_5 &= [9,18] \\ c_6 &= c_5 y = 25 & v_6 &= [10,18] \\ c_7 &= c_6 y = 29 & v_7 &= [11,18] \\ c_8 &= c_7 y = 70 & v_8 &= [12,18] \\ c_9 &= c_8 g = 39 & v_9 &= [12,19] \\ c_{10} &= c_9^3 = 32 & v_{10} &= [36,57] \end{aligned}$$

Dobijamo jednakost za $j = 5$ ($c_5 = c_{10}$). Primetimo da važi i $c_4 = c_9$, ali $2 \cdot 4 \neq 8$ pa smo morali da nastavimo sa računom. Sada možemo da odredimo broj x:

$$x = (18 - 57)(36 - 9)^{-1} = -39 \cdot 27^{-1} = 43$$

12.2 Programi

Zadatak 12.4 *Napisati Python funkciju za faktorizaciju broja $\boldsymbol{n}$ algoritmom slučajnog lutanja.*

Rešenje:

```
def f(x, n):
    return (x*x + 1) % n

def slucajno_lutanje(n):
    a = [0]
    i = 1

    while True:
        a.append(f(a[i-1], n))

        if i % 2 == 0:
            p = nzd(a[i] - a[i // 2], n)

            if p > 1 and p != n:
                return (p, n // p)

        i += 1
```

13 Faktorizacija

U ovom delu pozabavićemo se različim metodama faktorizacije brojeva.

13.1 Fermaova faktorizacija

Neka je dat broj n koji je potrebno faktorisati. Najpre je potrebno izračunati broj $x = \lceil \sqrt{n} + i \rceil$ (za $i \geq 0$) , a onda i $\sqrt{x^2 - n}$ sve dok ne dobijemo ceo broj. Kada smo dobili celobrojnu vrednost (obeležimo je sa z), onda važi:

$$n = (x - z)(x + z)$$

Zadatak 13.1 *Primeniti Fermaovu faktorizaciju na sledeće brojeve:*

a) $n = 3229799$

b) $n = 1357$

c) $n = 21079$

Rešenje:

a) $n = 3229799 \rightarrow x = \lceil \sqrt{n} \rceil = 1798$

$$\sqrt{1798^2 - 3229799} = \sqrt{3232804 - 3229799} = \sqrt{3005} \notin \mathbb{Z}$$
$$\sqrt{1799^2 - 3229799} = \sqrt{3236401 - 3229799} = \sqrt{6602} \notin \mathbb{Z}$$
$$\sqrt{1800^2 - 3229799} = \sqrt{3240000 - 3229799} = \sqrt{10201} = 101$$

Dobili smo ceo broj za $i = 2$, pa se broj n faktoriše na sledeći način:

$$n = (1800 - 101)(1800 + 101) = 1699 \cdot 1901$$

b) $n = 1357 \rightarrow x = \lceil \sqrt{n} \rceil = 37$

$$\sqrt{37^2 - 1357} = \sqrt{12} \notin \mathbb{Z}$$
$$\sqrt{38^2 - 1357} = \sqrt{87} \notin \mathbb{Z}$$
$$\sqrt{39^2 - 1357} = \sqrt{164} \notin \mathbb{Z}$$
$$\sqrt{40^2 - 1357} = \sqrt{243} \notin \mathbb{Z}$$
$$\sqrt{41^2 - 1357} = \sqrt{324} = 18$$

Dobili smo ceo broj za $i = 4$, pa se broj n faktoriše na sledeći način:

$$n = (41 - 18)(41 + 18) = 23 \cdot 59$$

c) $n = 21079 \rightarrow x = \lceil \sqrt{n} \rceil = 146$

$$\sqrt{146^2 - 21079} = \sqrt{237} \notin \mathbb{Z}$$
$$\sqrt{147^2 - 21079} = \sqrt{530} \notin \mathbb{Z}$$
$$\sqrt{148^2 - 21079} = \sqrt{825} \notin \mathbb{Z}$$
$$\sqrt{149^2 - 21079} = \sqrt{1122} \notin \mathbb{Z}$$
$$\sqrt{150^2 - 21079} = \sqrt{1421} \notin \mathbb{Z}$$
$$\sqrt{151^2 - 21079} = \sqrt{1722} \notin \mathbb{Z}$$
$$\sqrt{152^2 - 21079} = \sqrt{2025} = 45$$

Dobili smo ceo broj za $i = 5$, pa se broj n faktoriše na sledeći način:

$$n = (152 - 45)(152 + 45) = 107 \cdot 197$$

13.2 Baze faktora

Neka je zadata broj n koji treba faktorisati i broj b koji predstavlja granicu glatkosti. Cilj je pronaći vrednosti x takve da važi da je $x^2(mod\ n)$ gladak broj. Kada pronađemo takve vrednosti, pokušavamo da pronađemo kombinaciju takvu da proizvod brojeva bude potpuni kvadrat po modulu n. Vrednosti za x biraju se tako da budu bliski umnošku broja n koji se faktoriše. Kreira se baza faktora koja se sastoji od prostih brojeva $\leq b$. U bazu faktora dodajemo i broj -1.

Za svako x za koje je $x \approx kn$ izračunava se ostatak $r \equiv x^2(mod\ n)$. Ako je r blizak broju n onda se umesto njega koristi $-1 \cdot (n - r)$. Ostatak se dalje rastavlja na faktore koriste bazu faktora i niz deljenja. Neće svaka vrednost moći da se faktoriše pomoću baze faktora pa se postupak ponavlja za više vrednosti koje su bliske broju kn i za različite vrednosti k, $k \geq 1$. Postupak ponavljamo sve dok se ne dođe do toga da je proizvod neke kombinacije ostataka potpuni kvadrat. Tada proveravamo uslove:

$$x^2 \equiv y^2(mod\ n)\ \wedge\ x \not\equiv \pm y(mod\ n)$$

pri čemu je y faktorizacija broja x koju dobijamo na osnovu baze faktora. Ukoliko su oba uslova ispunjena, onda je jedan faktor broja n

$$p = NZD(x + y, n)$$

Ukoliko nisu ispunjena oba uslova, potrebno je da pronađemo novu kombinaciju ostataka koja je potpuni kvadrat i ponovo proveriti uslov.

Zadatak 13.2 *Faktorisati broj $n = 89893$ pomoću baza faktora ako je $b = 20$.*

Rešenje: Sa primenom algoritma krećemo za $k = 1$ pa računamo $\sqrt{n} \approx 299$. Tražimo vrednosti za x bliske broju 299 čiji su ostaci po modulu n glatki brojevi:

$$299^2 \equiv -492 \text{ (nije gladak)}$$
$$300^2 \equiv 107 \text{ (nije gladak)}$$
$$301^2 \equiv 708 \text{ (nije gladak)}$$
$$298^2 \equiv 88804 \equiv -1098 \equiv (-1) = 3^2 \cdot 11^2$$

Postupak ćemo ponoviti za $k = 2$, $\sqrt{2n} \approx 424$:

$$424^2 \equiv 8983 \equiv -10 = (-1) \cdot 2 \cdot 5$$
$$423^2 \equiv 89036 \equiv -857 \text{ (nije gladak)}$$
$$425^2 \equiv 839 \text{ (nije gladak)}$$
$$426^2 \equiv 1690 = 2 \cdot 5 \cdot 13^2$$

Predstavićemo ostatke preko baze faktora u narednoj tabeli:

	-1	2	3	5	7	11	13	17	19
298^2	1	0	2	0	0	2	0	0	0
424^2	1	1	0	1	0	0	0	0	0
426^2	0	1	0	1	0	0	2	0	0
$298^2 \cdot 424^2 \cdot 426^2$	2	2	2	2	0	2	2	0	0

Proizvod ova tri ostatka daje pun kvadrat pa je

$$x^2 = 298^2 \cdot 424^2 \cdot 426^2 = 65928$$
$$y^2 = (-1)^2 \cdot 2^2 \cdot 3^2 \cdot 5^2 \cdot 11^2 \cdot 13^2 = 65928$$

Jasno je da važi $x^2 \equiv y^2 (mod\ n)$. Ono što treba da proverimo jeste drugi uslov:

$$x \equiv 298 \cdot 424 \cdot 426 (mod\ 89893) \equiv 69938 (mod\ 89893)$$
$$y \equiv (-1) \cdot 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 (mod\ 89893) \equiv -4290 (mod\ 89893) \equiv 85603 (mod\ 89893)$$

Pošto je ispunjen i drugi uslov, na korak smo od pronalaženja jednog faktora broja 89893:

$$p = NZD(x + y, n) = NZD(65648, 89893) = 373$$

Sada lako nalazimo i drugi faktor:

$$q = \frac{n}{p} = \frac{89893}{373} = 241$$

Dakle, $89893 = 373 \cdot 241$.

13.3 Verižni razlomci

Algoritam zasnovan na verižnim razlomcima sličan je prethodnom. Potrebno je da x^2 bude približno umnošku broja n. Prvi korak je odrediti verižni razvoj broja $\sqrt{n}$. Neka je $\frac{P}{Q}$ neki parcijalni razlomak dobijen polazeći od tog razvoja. Tada važi da je $\frac{P^2}{Q^2} \approx n$, odnosno $P^2 \approx Q^2 n$ odakle vidimo da je P^2 blisko umnošku broja n. Broj $P^2 (mod\ n)$ je broj koji ćemo pokušati da rastavimo na činioce pomoću baze faktora i postupak je dalje sličan kao u prethodnom algoritmu. Tražimo brojeve $P^2 (mod\ n)$ koji su glatki i postupak ponavljamo sve dok se ne dođe do toga da je proizvod neke kombinacije ovih brojeva potpuni kvadrat. Tada proveravamo uslove:

$$x^2 \equiv y^2 (mod\ n)\ \wedge\ x \not\equiv \pm y (mod\ n)$$

pri čemu je y faktorizacija broja x koju dobijamo na osnovu baze faktora. Ukoliko su oba uslova ispunjena, onda je jedan faktor broja n

$$p = NZD(x - y, n)$$

Ukoliko nisu ispunjena oba uslova, potrebno je da pronađemo novu kombinaciju brojeva koja je potpuni kvadrat i ponovo proveriti uslov.

Zadatak 13.3 *Faktorisati broj $n = 17873$ pomoću verižnih razlomaka ako je granica glatkosti $b = 30$.*

Rešenje: Prvo određujemo verižni razvoj[14] broja $\sqrt{17873}$. Dobija se tablica konvergenata:

n	-1	0	1	2	3	4	5	6	7	8
a_n		133	1	2	4	2	3	1	2	1
P_n	1	133	134	401	1738	3877	13369	17246	47861	65107
Q_n	0	1	1	3	13	29	100	129	358	487

[14] Ovaj deo zadatka odraditi za vežbu.

Sada tražimo glatke brojeve među P_i^2:

$$P_0^2 = 133^2 \equiv 17689 \equiv -184 = (-1) \cdot 2^3 \cdot 23$$
$$P_1^2 = 134^2 \equiv 83 \text{ (nije gladak)}$$
$$P_2^2 = 401^2 \equiv 17817 \equiv -56 = (-1) \cdot 2^3 \cdot 7$$
$$P_3^2 = 1738^2 \equiv 107 \text{ (nije gladak)}$$
$$P_4^2 = 3877^2 \equiv 17809 \equiv -64 = (-1) \cdot 2^6$$
$$P_5^2 = 13369^2 \equiv 161 = 7 \cdot 23$$

Predstavimo to tabelom:

	-1	2	3	5	7	11	13	17	19	23	29
133^2	1	3	0	0	0	0	0	0	0	1	0
401^2	1	3	0	0	1	0	0	0	0	0	0
3877^2	1	6	0	0	0	0	0	0	0	0	0
13369^2	0	0	0	0	1	0	0	0	0	1	0
$133^2 \cdot 401^2 \cdot 13369^2$	2	6	0	0	2	0	0	0	0	2	0

Proizvod ovih brojeva daje pun kvadrat pa je

$$x^2 = 133^2 \cdot 401^2 \cdot 13369^2 = 14628$$
$$y^2 = (-1)^2 \cdot 2^6 \cdot 7^2 \cdot 23^2 = 14628$$

Jasno je da važi $x^2 \equiv y^2 (mod\ n)$. Ono što treba da proverimo jeste drugi uslov:

$$x \equiv 133 \cdot 401 \cdot 13369 (mod\ 17873) \equiv 1288 (mod\ 17873)$$
$$y \equiv (-1) \cdot 2^3 \cdot 7 \cdot 23 (mod\ 17873) \equiv -1288 (mod\ 17873)$$

Drugi uslov nije ispunjen pa nastavljamo potragu za glatkim brojevima među P_i^2:

$$P_6^2 = 17246^2 \equiv 17796 \equiv -77 = (-1) \cdot 7 \cdot 11$$
$$P_7^2 = 47861^2 \equiv 12115^2 \equiv 149 \text{ (nije gladak)}$$
$$P_8^2 = 65107^2 \equiv 11488^2 \equiv 17785 \equiv -88 = (-1) \cdot 2^3 \cdot 11$$

Dopunimo prethodnu tabelu:

	-1	2	3	5	7	11	13	17	19	23	29
133^2	1	3	0	0	0	0	0	0	0	1	0
401^2	1	3	0	0	1	0	0	0	0	0	0
3877^2	1	6	0	0	0	0	0	0	0	0	0
13369^2	0	0	0	0	1	0	0	0	0	1	0
17246^2	1	0	0	0	1	1	0	0	0	0	0
65107^2	1	3	0	0	0	1	0	0	0	0	0
$401^2 \cdot 3877^2 \cdot 17246^2 \cdot 65107^2$	4	12	0	0	2	2	0	0	0	0	0

Proizvod ovih brojeva daje pun kvadrat pa je

$$x^2 = 401^2 \cdot 3877^2 \cdot 17246^2 \cdot 65107^2 = 13650$$
$$y^2 = (-1)^4 \cdot 2^{12} \cdot 7^2 \cdot 11^2 = 13650$$

Jasno je da važi $x^2 \equiv y^2 (mod\ n)$. Ono što treba da proverimo jeste drugi uslov:

$$x \equiv 401 \cdot 3877 \cdot 17246 \cdot 65107 (mod\ 17873) \equiv 7272 (mod\ 17873)$$
$$y \equiv (-1)^2 \cdot 2^6 \cdot 7 \cdot 11 (mod\ 17873) \equiv 4928 (mod\ 17873) \equiv -12945 (mod\ 17873)$$

Pošto je ispunjen i drugi uslov, možemo odrediti jedan faktor broja 17873:

$$p = NZD(x - y, n) = NZD(2344, 17873) = 293$$

Sada lako nalazimo i drugi faktor:

$$q = \frac{n}{p} = \frac{17873}{293} = 61$$

Dakle, $17873 = 293 \cdot 61$.

13.4 Eliptičke krive

Zadata je eliptička kriva $E : y^2 = x^3 + Ax + B$ i tačka R koja se nalazi na zadatoj krivoj. Ideja je da se određuju tačke mR za $m \geq 2$ dokle to može. Kada se dođe do vrednosti za m takve da koeficijent pravca nije moguće odrediti (jer ne može da se odredi inverz imenioca po modulu n) tada dobijamo jedan od faktora broja n. Zaista, inverz nije moguće odrediti ukoliko brojevi nisu uzajamno prosti, a kako se određuje NZD nekog broja i broja n, dobijeni NZD (koji nije jednak broju 1) jeste jedan delilac broja n. Drugi se dobija jednostavnim deljenjem broja n dobijenim NZD-om.

Zadatak 13.4 *Faktorisati broj $n = 221$ pomoću eliptičke krive $E : y^2 = x^3 + x + 1$ i tačke $R = (0, 1)$ na toj krivoj.*

Rešenje:
2R $= R + R$:

$$k = \frac{3 \cdot 0 + 1}{2 \cdot 1} = 1 \cdot 2^{-1} = 111 \qquad n = 1 - 0 \cdot 111 = 1$$
$$x_3 = 111^2 = 166 \qquad y_3 = 111 \cdot 166 + 1 = 84$$

$2R = (166, -84) = (166, 137)$

3R $= 2R + R$:

$$k = \frac{137 - 1}{166} = 136 \cdot 166^{-1} = 136 \cdot 4 = 102 \qquad n = 137 - 166 \cdot 102 = 1$$
$$x_3 = 102^2 - 166 - 0 = 72 \qquad y_3 = 102 \cdot 72 + 1 = 52$$

$3R = (72, -52) = (72, 169)$

4R $= 2R + 2R$:

$$k = \frac{169 - 1}{72 - 0} = 168 \cdot 72^{-1} = 168 \cdot 132 = 76 \qquad n = 1 - 76 \cdot 0 = 1$$
$$x_3 = 76^2 - 72 - 0 = 179 \qquad y_3 = 76 \cdot 179 + 1 = 124$$

$4R = (179, -124) = (179, 97)$

5R $= 4R + R$:

$$k = \frac{97 - 1}{179 - 0} = 96 \cdot 179^{-1} = 96 \cdot 121 = 124 \qquad n = 1 - 124 \cdot 0 = 1$$
$$x_3 = 124^2 - 179 - 0 = 127 + 42 = 169 \qquad y_3 = 169 \cdot 124 + 1 = 183$$

$2R = (169, -183) = (169, 38)$

6R $= 3R + 3R$:

$$k = \frac{3 \cdot 72^2 + 1}{2 \cdot 169} = 102 \cdot 117^{-1}$$

Nailazimo na tačku koju ne možemo da odredimo jer važi $NZD(117, 221) = 13 = p$. Time smo dobili jedan faktor. Vrednost drugog faktora dobijamo deljenjem broja n brojem p:

$$q = \frac{n}{p} = \frac{221}{13} = 17$$

Dakle, $221 = 13 \cdot 17$.

13.5 Programi

Zadatak 13.5 *Napisati Python funkciju za faktorizaciju broja* $\boldsymbol{n}$ *primenom postupka Fermaove faktorizacije.*

Rešenje:

```
import math

def fermaova_faktorizacija(n):
    a = math.ceil(math.sqrt(n))

    while True:
        b = math.sqrt(a*a - n)

        if b == math.trunc(b):
            return (int(a - b), int(a + b))

        a += 1
```

14 Polje brojeva

Skup $\mathbb{Q}(\alpha)$ je polje brojeva i važi $\mathbb{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$. Ovo polje sastoji se od svih brojeva dobijenih kombinovanjem racionalnih brojeva i α korišćenjem operacija $+, -, \times$ i $/$.

Definicija 14.1 *Ako je koeficijent uz najveći stepen minimalnog polinoma jednak 1 onda je α algebarski ceo broj.*

Definicija 14.2 $\beta \mid \alpha \Leftrightarrow \exists\gamma : \alpha = \beta\gamma, \quad \alpha, \beta, \gamma$ *su celi algebarski brojevi*

Definicija 14.3 α *je prost broj* $\Leftrightarrow \alpha \mid \beta\gamma \Rightarrow \alpha \mid \beta \veebar \alpha \mid \gamma, \ \forall\beta, \gamma$

Polje $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. Algebarski celi brojevi u $\mathbb{Q}(i)$ su oblika $a + bi$ za $a, b \in \mathbb{Z}$, a polje obično označavamo kao $\mathbb{Z}(i)$. Jedinice ovog polja su ± 1 i $\pm i$. U njemu važi da ako je $p \in \mathbb{Z}_{>0}$ prost broj i $p \equiv 3(mod\ 4)$ onda je broj prost i u $\mathbb{Z}(i)$. Ukoliko važi $p \equiv 1(mod\ 4)$, onda se p može predstaviti u obliku $a^2 + b^2$, $a, b \in \mathbb{Z}$ pa je $p = (a + bi)(a - bi)$ pri čemu su $a + bi$ i $a - bi$ nepridruženi prosti brojevima. Na primer, $4 + i$ i $1 - 4i$ su pridruženi brojevi što obeležavamo kao $4 + i \sim 1 - 4i$. Uvek biramo brojeve oblika $a \pm bi$ za koje važi $a \geq b \geq 0$, pa bismo između $4 + i$ i $1 - 4i$ odabrali $4 + i$.

Definišemo preslikavanje $N : \mathbb{Q}(i) \to \mathbb{Q}$ kao $N(a+bi) = a^2+b^2$ i nazivamo ga *norma*. Ako je $a+bi \in \mathbb{Z}(i)$, p prost broj u $\mathbb{Z}$ i $p \mid N(a + bi)$ onda neki prosti delilac p deli $a + bi$.

Zadatak 14.1 *Pokazati da je $f(x) = x^2 - 2$ minimalni polinom polja koje je zatvoreno za operacije $+, -, \times$ i $/$.*

Rešenje: Minimalni polinom možemo rastaviti na činioce:

$$f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

Odatle je $\alpha = \sqrt{2}$, a polje je $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Jasno je da je skup zatvoren za sabiranje i oduzimanje. Proverimo za množenje i deljenje:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

$$\begin{aligned}\frac{a + b\sqrt{2}}{c + d\sqrt{2}} &= \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{(ac - 2bd) + (-ad + bc)\sqrt{2}}{c^2 - 2d^2} \\ &= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})\end{aligned}$$

Zadatak 14.2 *Odrediti minimalni polinom broja $\alpha = 2^{\frac{1}{3}} + 1$.*

Rešenje:

$$\begin{aligned}\alpha &= 2^{\frac{1}{3}} + 1 \\ 2 &= (\alpha - 1)^3 \\ 2 &= \alpha^3 - 3\alpha^2 + 3\alpha - 1 \\ 0 &= \alpha^3 - 3\alpha^2 + 3\alpha - 3\end{aligned}$$

Pošto je α koren minimalnog polinoma, iz poslednje jednačine dobijamo da je minimalni polinom $f(x) = x^3 - 3x^2 + 3x - 3$.

Zadatak 14.3 *Dokazati da su u polju $\mathbb{Q}(\sqrt{-5})$ svi algebarski celi brojevi oblika $a+b\sqrt{-5}$, gde su a i b celi brojevi.*

Rešenje: Neka je $f(x)$ minimalni polinom broja α. Onda važi $(x-\alpha) \mid f(x)$. Pošto je $\alpha \in \mathbb{Q}(\sqrt{-5})$ onda je $\alpha = a+b\sqrt{-5}$, i pretpostavimo suprotno, odnosno da su $a, b \in \mathbb{Q}$. Njegov konjugovani element je $\overline{\alpha} = a-b\sqrt{-5}$. Za njega takođe važi $(x-\overline{\alpha}) \mid f(x)$. Onda važi i $(x-\alpha)(x-\overline{\alpha}) \mid f(x)$. Taj proizvod možemo izvesti:

$$\begin{aligned}(x-\alpha)(x-\overline{\alpha}) &= (x-a-b\sqrt{-5})(x-a+b\sqrt{-5}) \\ &= x^2 - ax + \cancel{bx\sqrt{-5}} - ax \cancel{-ab\sqrt{-5}} + a^2 \cancel{-bx\sqrt{-5}} + \cancel{ab\sqrt{-5}} + 5b^2 \\ &= x^2 - 2ax + a^2 + 5b^2\end{aligned}$$

Dakle, važi $(x^2-2ax+a^2+5b^2) \mid f(x)$. Kako koeficijenti minimalnog polinoma moraju biti celi brojevi, ukoliko su brojevi a i b racionalni brojevi onda će koeficijent uz najveći stepen ovog polinoma biti različit od 1 (a onda broj nije algebarski ceo) što je kontradikcija. Time smo pokazali da su algebarski celi brojevi oblika $a+b\sqrt{-5}$ za $a, b \in \mathbb{Z}$.

■

Zadatak 14.4 *Dokazati da se u polju $\mathbb{Q}(\sqrt{-5})$ broj 2 ne može rastaviti u netrivijalni proizvod algebarskih celih brojeva.*

Rešenje: Prvi pokušaj bi bio rastavljanje na proizvod brojeva -1 i -2. Međutim, to je trivijalan proizvod. Potrebni su nam brojevi oblika $a+b\sqrt{-5}, b \neq 0$, odnosno:

$$2 = (a+b\sqrt{-5})(c+d\sqrt{-5}) = ac-5bd+(ad+bc)\sqrt{-5} \quad \text{za} \quad a,b,c,d \in \mathbb{Z}$$

Proizvod nije trivijalan za $b \neq 0 \ \wedge \ d \neq 0$ Pretpostavimo suprotno:

$$\begin{aligned} ac - 5bd &= 2 \\ ad + bc &= 0 \end{aligned}$$

Ovo možemo podeliti na 3 slučaja, u zavisnosti od vrednosti koje uzimaju brojevi b i d:

I) $b = 0$

$$\begin{aligned} ac &= 2 \\ ad &= 0 \end{aligned}$$

Iz ovog sistema saznajemo da $d = 0$ i $a \neq 0$, što daje trivijalan proizvod. $\lightning$

II) $b \neq 0 \wedge d = 0$

$$\begin{aligned} ac = 2 &\rightarrow c \neq 0 \\ bc = 0 &\rightarrow c = 0 \ \lightning \end{aligned}$$

U ovom slučaju dolazi do kontradikcije jer zbog prve jednačine c ne sme biti jednako 0, a zbog druge mora biti jednako 0 (jer je b različito od 0).

III) $b \neq 0 \wedge d \neq 0$

$$
\begin{aligned}
& ac - 5bd = 2 \\
& ad + bc = 0 \\
& \text{---------} \\
& bc = -ad \\
& \frac{c}{d} = -\frac{a}{b} = t \\
& a = -tb, c = td \\
& \text{---------} \\
& -t^2bd - 5bd = 2 \\
& -bd(t^2 + 5) = 2 \ \lightning
\end{aligned}
$$

I u ovom slučaju dolazimo do kontradikcije jer važi da je $t^2 + 5$ sigurno veće od 5, što je svakako veće od 2, pa množenjem celim brojem ne može dati broj 2. Kako smo u svim slučajevima naišli na kontradikciju možemo zaključiti da se 2 ne može predstaviti kao netrivijalan proizvod.

■

Zadatak 14.5 *Dokazati da 2 nije prost u* $Q(\sqrt{-5})$.

Rešenje: Pretpostavimo suprotno: broj 2 je prost broj. Znamo da broj 2 deli broj 6. Broj 6 možemo predstaviti kao $(1 - \sqrt{-5})(1 + \sqrt{-5})$. Primenom definicije 14.3 znamo da broj 2 deli jedan od ova dva broja. Proverimo da li je to ispunjeno tako što ćemo odrediti minimalni polinom brojeva $\frac{1-\sqrt{-5}}{2}$ i $\frac{1+\sqrt{-5}}{2}$:

$$
\begin{aligned}
x &= \frac{1 - \sqrt{-5}}{2} / \cdot 2 \\
2x &= 1 - \sqrt{-5} \\
\sqrt{-5} &= 1 - 2x /^2 \\
-5 &= 1 - 4x + 4x^2 \\
4x^2 - 4x + 6 &= 0 / : 2 \\
2x^2 - 2x + 3 &= 0
\end{aligned}
$$

Dobijeni polinom nije moničan[15] što znači da x nije algebarski ceo broj. Iz toga zaključujemo da broj 2 ne deli $(1 - \sqrt{-5})$. Pokušajmo sa $(1 + \sqrt{-5})$:

$$
\begin{aligned}
x &= \frac{1 + \sqrt{-5}}{2} / \cdot 2 \\
2x &= 1 + \sqrt{-5} \\
\sqrt{-5} &= 2x - 1 /^2 \\
-5 &= 4x^2 - 4x + 1 \\
4x^2 - 4x + 6 &= 0 / : 2 \\
2x^2 - 2x + 3 &= 0
\end{aligned}
$$

Dobijeni polinom nije moničan što znači da x nije algebarski ceo broj. Iz toga zaključujemo da broj 2 ne deli ni $(1 + \sqrt{-5})$. Ovde nailazimo na kontradikciju jer broj 2 ne odgovara definiciji prostog broja.

[15] Moničan polinom je polinom čiji je najstariji koeficijent jednak 1.

■

Zadatak 14.6 *Odrediti proste brojeve u $\mathbb{Z}(i)$ koji su manji od 30.*

Rešenje: Brojevi manji od 30 koji su prosti u $\mathbb{Z}$ pripadaju skupu $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$. Svaki od njih ćemo rastaviti ukoliko važi da po modulu 4 daju 1, odnosno obeležiti kao prost (obeležićemo ih zvezdicom) ukoliko daju ostatak 3 po modulu 4:

$$2 = 1 + 1 = (1 - i)(\underbrace{1 + i}_{=(1-i)i}) = (\underbrace{1 - i}_{=(1+i)i})^2 i = (1 + i)^2 i^3$$

3^*

$5 = 4 + 1 = (2 + i)(2 - i)$

7^*

11^*

$13 = 9 + 4 = (3 + 2i)(3 - 2i)$

$17 = 16 + 1 = (4 + i)(4 - i)$

19^*

23^*

$29 = 25 + 4 = (5 + 2i)(5 - 2i)$

Dakle, prosti brojevi manji od 30 u $\mathbb{Z}(i)$ su $\{3, 7, 11, 19, 23\}$.

Zadatak 14.7 *U skupu $\mathbb{Z}(i)$ rastaviti na činioce:*

a) $5 + 3i$

b) $11 - 3i$

c) $7 + i$

Rešenje:

a) $N(5 + 3i) = 25 + 9 = 34 = 2 \cdot 17$
Na osnovu norme možemo da zaključimo da su kandidati za faktore: $(1 + i), i^3$ i $(4 \pm i)$. Krenimo redom sa proverom:

$$\frac{5 + 3i}{1 + i} = \frac{(5 + 3i)(1 - i)}{(1 + i)(1 - i)} = \frac{5 + 3i - 5i - 3i^2}{1 - i^2} = \frac{8 - 2i}{2} = 4 - i$$

Nakon prvog pokušaja našli smo faktore

$$5 + 3i = (1 + i)(4 - i)$$

b) $N(11 - 3i) = 121 + 9 = 130 = 2 \cdot 5 \cdot 13$
Na osnovu norme možemo da zaključimo da su kandidati za faktore: $(1 + i), i^3, (2 \pm i)$ i $(3 \pm 2i)$. Krenimo redom sa proverom:

$$\frac{11 - 3i}{1 + i} = \frac{(11 - 3i)(1 - i)}{(1 + i)(1 - i)} = \frac{8 - 14i}{2} = 4 - 7i$$

Broj $11 - 3i$ jeste deljiv brojem $1 + i$. Dalje, razlažemo $4 - 7i$. Kako bismo dodatno ubrzali faktorizaciju, možemo odrediti normu ovog broja i nastaviti račun sa redukovanim skupom kandidata.

Pošto važi da je $N(4-7i) = 16+49 = 65 = 5 \cdot 13$ biramo neki od faktora brojeva 5 i 13, na primer $2+i$:

$$\frac{4-7i}{2+i} = \frac{(4-7i)(2-i)}{(2+i)(2-i)} = \frac{1-18i}{5}$$

Ispostavilo se da $2+i$ ne deli $4-7i$ pa pokušavamo sa nekim drugim kandidatom, na primer $2-i$:

$$\frac{4-7i}{2-i} = \frac{(4-7i)(2+i)}{(2-i)(2+i)} = \frac{15-10i}{5} = 3-2i$$

Dakle, $11-3i = (1+i)(2-i)(3-2i)$.

c) $N(7+i) = 49+1 = 50 = 2 \cdot 5^2$. Na osnovu norme možemo da zaključimo da su kandidati za faktore: $(1+i), i^3$ i $(2 \pm i)$. Krenimo redom sa proverom[16]:

$$\frac{7+i}{i^3} = \frac{(7+i)\cdot i}{i^3 \cdot i} = \frac{-1+7i}{i^4} = -1+7i$$

$$\frac{7+i}{2+i} = \frac{(7+i)(2-i)}{(2+i)(2-i)} = \frac{5+15i}{5} = 1+3i$$

$N(1+3i) = 1+9 = 10 = 2 \cdot 5$ pa se skup kandidata ne menja. Možemo još jednom pokušati sa $2+i$:

$$\frac{1+3i}{2+i} = \frac{(1+3i)(2-i)}{(2+i)(2-i)} = \frac{5+5i}{5} = 1+i$$

Dakle, $7+i = i^3(1+i)(2+i)^2$

[16] Napomena: Na času je broj $7+i$ prvo podeljen brojem $1+i$ i dobijen je rezultat $4-3i$. U narednom koraku, umesto da se faktorizacija nastavi rastavljanjem rezultata, greškom je ponovo podeljen broj $7+i$ brojem i^3. Zbog toga ćemo u ovom rešenju preskočiti prvo deljenje iz rešenja zadatka sa časa i započeti deljenjem brojem i^3.