Metode faktorizacije

Andrijević, Maja

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Maja Andrijević

Metode faktorizacije

Završni rad

Osijek, 2020.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Maja Andrijević

Metode faktorizacije

Završni rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2020.

Sažetak

U ovom radu upoznat ćemo se s nekim metodama faktorizacije prirodnih brojeva. Najprije ćemo ponoviti neke osnovne definicije i važne rezultate teorije brojeva kako bismo mogli razumijeti algoritme metoda kao što su Fermatova metoda, metoda faktorske baze, metoda verižnog razlomka, Pollardova ρ metoda, Pollardova $p-1$ metoda, metoda kvadratnog sita i metoda pomoću eliptičkih krivulja. Na kraju svakog poglavlja vidjet ćemo primjenu algoritama na nekoliko primjera.

Ključne riječi

faktorizacija, metode faktorizacije, prirodni brojevi, prosti brojevi, Euklidov algoritam, najveći zajednički djelitelj

Factorization methods

Summary

In this final paper, we will consider some methods of factorization of positive integers. In order to understand methods of algorithms such as Fermat method, factor bases method, the continued fraction method, Pollard's ρ method, Pollard's $p-1$ method, the quadratic sieve method and elliptic curve factorization method, we will mark some basic definitions and important results of number theory. At the end of each chapter, we will present couple of examples concerning presented methods.

Key words

factorization, methods of factorization, positive integers, prime numbers, Euclidean algorithm, greatest common divisor

Sadržaj

Uvod

Ako prirodan broj n ne prođe neki od testova prostosti, onda znamo da je n složen i da ga možemo zapisati kao produkt prostih faktora. No, takav način zapisivanja prirodnih brojeva nije uvijek jednostavan. Faktorizacija može biti vrlo složen problem i upravo zbog toga se koristi u različitim kriptosustavima. Primjerice, sigurnost RSA kriptosustava zasnovana je upravo na težini faktorizacije prirodnih brojeva.
Matematičari su se godinama bavili proučavanjem metoda za faktorizaciju, a neke metode se i dalje izučavaju.
U ovom radu ćemo prikazati algoritme nekoliko metoda faktorizacije prirodnih brojeva.
Metode faktorizacije dijelimo na opće i specijalne. U općim metodama broj operacija ovisi o veličini broja n, a kod specijalnih metoda ovisi i o svojstvima faktora od n.

Kako bismo lakše mogli pratiti sadržaj rada ponovimo neke osnovne definicije i rezultate, a ostalo možemo pronaći u [3].

Definicija 1. *Prirodan broj $p > 1$ zove se prost, ako p nema niti jednog djelitelja d sa svojstvom $1 < d < p$. Ako prirodan broj nije prost, onda kažemo da je složen.*

Definicija 2. *Neka su b i c cijeli brojevi. Cijeli broj a zovemo zajednički djelitelj od b i c ako $a|b$ i $a|c$. Ako je barem jedan od brojeva b i c različit od nule, onda postoji samo konačno mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se najveći zajednički djelitelj od b i c i označava se s $nzd(b,c)$, $gcd(d,c)$ ili (b,c). Analogno se definira najveći zajednički djelitelj cijelih brojeva $b_1, b_2, \ldots, b_n$, koji nisu svi jednaki nuli te se označava s $nzd(b_1, b_2, \ldots, b_n)$.*

Propozicija 1 (vidjeti [1, Fundamental property of prime number])**.** *Ako je p prost broj i ako $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 \ldots a_n$, onda p dijeli barem jedan faktor a_i.*

Teorem 1 (Teorem o dijeljenju s ostatkom, vidjeti [3, Teorem 2.2])**.** *Za proizvoljan prirodni broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je*

$$b = qa + r,\ 0 \leqslant r < a.$$

Teorem 2 (Euklidov algoritam, vidjeti [3, Teorem 2.7])**.** *Neka su b i c prirodni brojevi te neka je $b > c$. Pretpostavimo da je uzastopnom primjenom teorema o dijeljenju s ostatkom dobiven niz jednakosti*

$$\begin{aligned}
b &= cq_1 + r_1,\ 0 < r_1 < c,\\
c &= r_1q_2 + r_2,\ 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3,\ 0 < r_3 < r_2,\\
&\ldots\\
r_{j-2} &= r_{j-1}q_j + r_j,\ 0 < r_j < r_{j-1},\\
r_{j-1} &= r_jq_{j+1}.
\end{aligned}$$

Tada je (b,c) jednak r_j, posljednjem ostatku različitom od nule.

Teorem 3 (Osnovni teorem aritmetike, vidjeti [1, Unique factorization theorem]). *Svaki prirodan broj $n \geqslant 2$ možemo na jedinstven način zapisati u obliku*

$$n = p_1^{e_1} \dots p_k^{e_k},$$

gdje su $1 < p_1 < p_2 < \dots < p_k$ prosti brojevi, a $e_1, \dots, e_k$ pozitivni cijeli brojevi.

Dokaz: Moramo pokazati jedinstvenost faktorizacije. Stoga pretpostavimo suprotno, tj. neka $n > 1$ ima dvije moguće faktorizacije

$$n = p_1 p_2 \dots p_k \text{ i } n = q_1 q_2 \dots q_l,\ k, l \in \mathbb{N}.$$

Slijedi da je

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_l, \tag{1}$$

a od tu slijedi da $p_1 | q_1 q_2 \dots q_l$.
Sada prema Propoziciji 1 slijedi $p_1 | q_i$ za neki $i \in \{1, \dots, l\}$. Jer su p_1 i q_i prosti, a jedan dijeli drugoga, slijedi $p_1 = g_i$, permutacijom faktora q_1 do q_l možemo uzeti da je $i = 1$. Sada nakon dijeljenja jednakosti (1) s p_1 slijedi

$$p_2 p_3 \dots p_k = q_2 q_3 \dots q_l.$$

Potpuno analogno zaključujemo za $p_2 = q_2,\ p_3 = q_3,\ \dots,\ p_k = p_l$. □

Osnovni teorem aritmetike govori nam da svaki prirodan broj $n \geqslant 2$ možemo zapisati kao produkt potencija prostih brojeva i da je samo jedan mogući izbor prostih brojeva i eksponenata.
Primjerice, uzmimo broj 54000. Taj broj možemo faktorizirati na jednostavan način dijeljenjem s prostim brojevima. Tako dobijemo sljedeću faktorizaciju

$$54000 = 2^4 \cdot 3^3 \cdot 5^3.$$

U nastavku rada upoznat ćemo se s nekim metodama faktorizacije i njihovim primjenama.

1 Pokusno dijeljenje

Pokusno (probno) dijeljenje ili *Trial division* je najstarija metoda rastavljanja prirodnog broja n na proste faktore. Ova metoda predstavlja dijeljenje broja n sa svim prostim faktorima od 2 do $\sqrt{n}$ (vidjeti [6]).

Primjer 1. *Faktorizirajmo prirodan broj* $n = 450$.
Rješenje: Primjenom algoritma pokusnog dijeljenja na broj 450 *dolazimo do najmanjeg prostog faktora od* $n = 450$, *a to je* 2. *Podijelimo* 450 *s* 2. *Dobijemo* 225 *što je složen broj pa ponovno primjenimo algoritam pokusnog dijeljenja.*
Dobivamo $225 : 3 = 75$, $75 : 3 = 25$. *Dakle,* 3^2 *dijeli* 450. *Primjenimo algoritam još dva puta te dobijemo* 5^2 *dijeli* 25 *i ostaje* 1.
Dakle, pronašli smo faktorizaciju od 450, *to je* $450 = 2 \cdot 3^2 \cdot 5^2$.

Algoritam pokusnog dijeljenja vrlo je lagan za razumijeti, ali nije baš učinkovit. Budući da algoritam daje potpunu faktorizaciju prirodnog broja ponavljajući svaki put postupak, kod velikih brojeva on može trajati godinama. Na primjeru ćemo vidjeti koliko bi nam vremena trebalo da faktoriziramo 100 znamenkasti broj (vidjeti [1]).

Primjer 2. *Pretpostavimo da je dani broj* $n > 10^{100}$. *Tada je* $\sqrt{n} > 10^{50}$. *Prema tome, algoritam moramo ponoviti najmanje* 10^{50} *puta. Kako bismo odredili koliko nam je potrebno vremena za faktorizaciju takvog prirodnog broja, pretpostavimo da računalo računa* 10^{10} *dijeljenja u minuti. Znači da bi računalu trebalo* 10^{40} *sekundi samo da provjeri je li dani broj prost. Jednostavnim računom izračunamo da bi faktorizacija trajala otprilike* 10^{31} *godina.*

Stoga se postavlja pitanje je li metoda pokusnog dijeljenja uopće korisna. Naime, ova metoda je vrlo korisna kada je riječ od malim brojevima, točnije brojevima manjim od 10^6. U takvim slučajevima faktorizaciju prirodnog broja možemo dobiti vrlo brzo. No, kada je riječ o većim brojevima koristit ćemo druge metode koje će nam olakšati faktorizaciju (vidjeti [1]).

2 Fermatova metoda

Ako je n produkt dva broja koja su blizu jedan drugome onda postoji tzv. Fermatova metoda faktorizacije za dani broj n. Ta metoda se temelji na činjenici da n možemo zaspisati kao razliku dva kvadrata od kojih je jedan puno manji od drugoga (vidjeti [5]).

U sljedećoj propoziciji vidjet ćemo kakvi moraju biti faktori od n da bi postojala jedinstvena faktorizacija u obliku razlike dva kvadrata.

Propozicija 2 (vidjeti [5, Proposition V.3.1.]). *Neka je n pozitivan cijeli broj takav da je $n = a \cdot b$, gdje je $a \geqslant b > 0$. Tada postoji jedinstvena faktorizacija od n u obliku*

$$n = t^2 - s^2,$$

gdje su t i s nenegativni cijeli brojevi takvi da je

$$t = \frac{a+b}{2} \ i \ s = \frac{a-b}{2}.$$

Dokaz: Kako je $n = a \cdot b$, možemo pisati

$$n = a \cdot b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

pa smo n uspjeli napisati kao razliku dva kvadrata.
Neka je sada $n = t^2 - s^2$. Izraz na desnoj strani možemo zapisati kao $(t-s)(t+s)$ pa odatle slijedi da je

$$t = \frac{a+b}{2} \text{ i } s = \frac{a-b}{2}.$$

□

Ako su a i b jako blizu, tada je $s = \frac{a-b}{2}$ jako mali broj, a $t = \frac{a+b}{2}$ je malo veći od $\sqrt{n}$. Brojeve a i b pronalazimo tako da za vrijednost od t krenemo s $\lfloor\sqrt{n}\rfloor + 1$, sve dok ne pronađemo takav t za koji je $t^2 - n = s^2$ potpun kvadrat. Pri tome, $\lfloor . \rfloor$ je funkcija koja uzima najveće cijelo od $\sqrt{n}$, a definiramo ju na sljedeći način:

Definicija 3. *Neka je $x \in \mathbb{R}$. Tada broj $\lfloor x \rfloor = max\{m \in \mathbb{Z} : m \leqslant x\}$ zovemo najveći cijeli dio od x ili najveće cijelo od x.*

Pogledajmo sada kako funkcija najveće cijelo funkcionira na nekim od primjera:

Primjer 3. *Odredimo vrijednosti funkcije najveće cijelo za dane brojeve x:*

x	$\lfloor x \rfloor$
9.8	*9*
5.3	*5*
-4.7	*-5*

Primjer 4 (vidjeti [5, Example 1, str.144]). *Fermatovom metodom faktorizirajmo broj* $n = 200819$.
Rješenje: Imamo $t = \lfloor\sqrt{200819}\rfloor + 1 = 448 + 1 = 449$,
pa je

$$s^2 = 449^2 - 200819 = 782,$$

ali to nije potpun kvadrat pa za t *biramo sljedeći broj.*
Sada je $t = 450$, *pa je* $s^2 = 450^2 - 200819 = 1681 = 41^2$.
Dakle, $200819 = 450^2 - 41^2 = (450 + 41)(450 - 41) = 491 \cdot 409$.

Pogledajmo na još jednom primjeru primjenu Fermatove metode faktorizacije.

Primjer 5. *Faktorizirajmo prirodan broj* $n = 403$.
Rješenje: Imamo

$$t = \left\lfloor\sqrt{403}\right\rfloor + 1 = 20 + 1 = 21 \text{ i } s^2 = 21^2 - 403 = 38$$

što nije potpun kvadrat. Idemo dalje s

$$t = \left\lfloor\sqrt{403}\right\rfloor + 2 = 22 \text{ i } s^2 = 22^2 - 403 = 81 = 9^2.$$

Sada je $403 = 22^2 - 9^2 = (22 - 9)(22 + 9) = 13 \cdot 31$.

Napomena 1. *Ako* a *i* b *nisu bliski, tada će Fermatova metoda pronaći* a *i* b, *ali tek nakon što za* t *odaberemo brojeve puno veće od* $\lfloor\sqrt{n}\rfloor + 1, \lfloor\sqrt{n}\rfloor + 2, \ldots$ *Stoga postoji generalizacija Fermatove metode koja će u takvim slučajevima biti dobar izbor. Odaberemo mali* k, *zatim za* t *redom stavljamo* $t = \left\lfloor\sqrt{kn}\right\rfloor + 1, \left\lfloor\sqrt{kn}\right\rfloor + 2, \ldots$ *sve dok ne dobijemo da je* $s^2 = t^2 - kn$ *potpun kvadrat. Tada je* $(t+s)(t-s) = kn$ *pa* $t+s$ *ima netrivijalan zajednički faktor s* n, *a njega možemo dobiti tako da izračunamo najveći zajednički djelitelj od* $t+s$ *i* n, *tj.* $(t+s, n)$.

Primjer 6. *Primjenimo prethodno opisanu metodu na dane brojeve* n:

(1.) *(vidjeti [5, Example 2, str.144])* $n = 141467$.
Rješenje: Neka je $k = 3$.
Tada je

$$t = \left\lfloor\sqrt{3n}\right\rfloor + 1 = 652, \; s^2 = 652^2 - 3 \cdot 141467 = 703,$$

što nije potpun kvadrat.
Uzimamo sljedeći t, $t = \lfloor\sqrt{3n}\rfloor + 2 = 653$, *ali ni tada za* s^2 *nećemo dobiti potpun kvadrat. Tek ćemo za* $t = \lfloor\sqrt{3n}\rfloor + 4 = 655$ *dobiti*

$$s^2 = 655^2 - 3 \cdot 141467 = 4624 = 68^2.$$

Sada još pomoću Euklidovog algoritma izračunamo $(655 + 68, 141467) = 241$ *što je netrivijalan faktor od* n.
Dakle, $141467 = 241 \cdot 587$.

(2.) $n = 3827$

Rješenje: Neka je $k = 3$. *Tada je*

$$t = \left\lfloor \sqrt{3n} \right\rfloor + 1 = 107 + 1 = 108 \text{ } i \text{ } s^2 = 108^2 - 3 \cdot 3827 = 183,$$

ali to nije potpun kvadrat.

Probamo dalje s

$$t = \left\lfloor \sqrt{3n} \right\rfloor + 2 = 107 + 2 = 109 \text{ } i \text{ } s^2 = 109^2 - 3 \cdot 3827 = 400 = 20^2.$$

Ovdje je s^2 *potpun kvadrat pa je tada* $(109 + 20, 3827) = 43$ *netrivijalan faktor od* n. *Dakle,* $3827 = 43 \cdot 89$.

3 Faktorske baze

Ova metoda je vrlo efikasno poopćenje Fermatove metode. Naime, umjesto da tražimo t i s takve da je $n = t^2 - s^2$, sada pokušamo pronaći t i s takve da $n \mid t^2 - s^2$, tj. takve da je $s^2 \equiv t^2 (\text{mod } n)$. Ako je pritom $s \not\equiv t (\text{mod } n)$, onda su $(t+s, n)$ i $(t-s, n)$ netrivijalni faktori od n. Kako bismo opisali algoritam faktorske baze uvedimo iduću definiciju.

Definicija 4. *Faktorska baza je skup $\mathscr{B} = \{p_1, p_2, ..., p_k\}$ različitih prostih brojeva, s tim da može biti $p_1 = -1$. Reći ćemo da je kvadrat cijelog broja b $\mathscr{B}$-broj (za dani n) ako se najmanji ostatak po apsolutnoj vrijednosti od b^2 modulo n može napisati kao produkt brojeva iz $\mathscr{B}$.*

Algoritam faktorske baze: Želimo faktorizirati jako velik prirodan broj n. Odaberemo prirodan broj y. Neka se faktorska baza $\mathscr{B}$ sastoji od -1 i svih prostih faktora manjih od y, tj.

$$\mathscr{B} = \{p : p \text{ prost broj}, \ p \leqslant y\} \cup \{-1\}.$$

Na slučajan način odaberemo konačno mnogo b_i-ova i pokušamo izraz $b_i^2 (\text{mod } n)$ prikazati kao produkt elemetana iz $\mathscr{B}$.
Kada dobijemo dovoljan broj $\mathscr{B}$-brojeva, pronađemo njihovu netrivijalnu linearnu kombinaciju koja je jednaka nul-vektoru. Sada je

$$b = \prod_i b_i (\text{mod } n), \ c = \prod_i p_j^{\gamma_j} (\text{mod } n),$$

gdje je

$$b_i^2 (\text{mod } n) \text{ i } \gamma_j = \frac{1}{2} \sum_i \alpha_{ij}.$$

Tada je $b^2 \equiv c^2 (\text{mod } n)$.
Ako je $b \not\equiv \pm c \ (\text{mod } n)$, onda izračunamo $(b+c, n)$ što je netrivijalan faktor od n.
A ako je $b \equiv \pm c (\text{mod } n)$, onda odaberemo neki drugi podskup od $\mathscr{B}$, takav da linearna kombinacija elemenata iz tog podkupa bude jednaka nul-vektoru ili nađemo još $\mathscr{B}$-brojeva i ponovimo navedeni postupak.

Pokažimo kako algoritam faktorske baze funkcionira na primjerima.

Primjer 7 (vidjeti [5, Example 9, str.147])**.** *Faktorizirajmo $n = 1829$ pomoću algoritma faktorske baze.*
Rješenje: Za b_i-ove uzimamo brojeve oblika $\left\lfloor \sqrt{1829k} \right\rfloor$ i $\left\lfloor \sqrt{1829k} \right\rfloor + 1$, za $k = 1, 2, ...$ takve da je $b_i^2 (mod\ n)$ produkt prostih brojeva manjih od 20. Dakle, $y = 20$.
Za takve b_i pišemo $b_i^2 (mod\ n) = \prod_j p_j^{\alpha ij}$, α_{ij} unosimo u tablicu

b_i	-1	2	3	5	7	11	13
42	1	-	-	1	-	-	1
43	-	2	-	1	-	-	-
61	-	-	2	-	1	-	-
74	1	-	-	-	-	1	-
85	1	-	-	-	1	-	1
86	-	4	-	1	-	-	-

.

Tablica 1

Za $k = 1, 2, 3, 4$ *imamo sljedeće:*

$$42^2 (mod\ 1829) = -65 = (-1) \cdot 5 \cdot 13$$
$$43^2 (mod\ 1829) = 20 = 2^2 \cdot 5$$
$$60^2 (mod\ 1829) = -58 = (-1) \cdot 58$$
$$61^2 (mod\ 1829) = -63 = (-1) \cdot 3^2 \cdot 7$$
$$74^2 (mod\ 1829) = -11 = (-1) \cdot 11$$
$$75^2 (mod\ 1829) = 138 = 2 \cdot 3 \cdot 23$$
$$85^2 (mod\ 1829) = -91 = (-1) \cdot 7 \cdot 13$$
$$86^2 (mod\ 1829) = 80 = 2^4 \cdot 5.$$

U stupac b_i *Tablice 1 unosimo samo one* b_i *koji su napisani kao produkt brojeva iz* $\mathscr{B}$*, a ispod brojeva iz* $\mathscr{B}$ *unosimo* α_{ij}*.*

Sada u Tablici 1 tražimo podskup redaka u kojima je suma α_{ij} *paran broj u svakom stupcu. Vidimo da* 2. *i* 6. *redak daju upravo takvu sumu* $-6 - 2 - --$*, a to nam daje sljedeću kongruenciju*

$$(b_2 \cdot b_6)^2 \equiv (43 \cdot 86)^2 (mod\ 1829) \equiv 40^2 (mod\ 1829).$$

No, $43 \cdot 86 \equiv 40 (mod\ 1829)$ *pa imamo samo trivijalnu faktorizaciju i moramo birati drugi podskup redaka.*
Pogledajmo sada sumu 1.,2.,3. *i* 5. *retka, ona je jednaka* $2\ 2\ 2\ 2\ 2\ -\ 2$*, a to nam daje:*

$$(b_1 \cdot b_2 \cdot b_3 \cdot b_5)^2 \equiv (42 \cdot 43 \cdot 61 \cdot 85)^2 (mod\ 1829),$$

tj. $1459^2 \equiv 901^2 (mod\ 1829)$*.*
Sada zaključujemo da je faktor od $n = 1829$ *jednak* $(1459 + 901, 1829) = 59$*. Dakle,* $1829 = 59 \cdot 31$*.*

Primjer 8. *Algoritmom faktorske baze faktorizirajmo broj* $n = 7215$*.*
Rješenje: Za b_i*-ove uzmimo brojeve oblika* $\left\lfloor \sqrt{7215k} \right\rfloor$ *i* $\left\lfloor \sqrt{7215k} \right\rfloor + 1$*, za* $k = 1, 2, 3, \ldots$ *takve da je* $b_i^2 (mod\ n)$ *produkt prostih brojeva manjih od 30. Dakle* $y = 30$ *i*
$\mathscr{B} = \{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$*. Dobivamo tablicu:*

b_i	-1	2	3	5	7	11	13	17	19	23	29	
85	-	1	-	1	-	-	-	-	-	-	-	-
190	-	-	-	2	-	-	-	-	-	-	-	-
209	-	-	-	-	-	-	-	-	1	-	1	-
225	3	1	1	-	-	-	-	-	-	-	-	-
241	-	-	-	-	-	-	-	-	-	2	-	-

Tablica 2

Za $k = 1, \ldots, 8$ *imamo iduće kongruencije:*

$$\begin{aligned}
84^2 (mod\ 7215) &= -159 = (-1) \cdot 3 \cdot 53 \\
85^2 (mod\ 7215) &= 10 = 2 \cdot 5 \\
120^2 (mod\ 7215) &= 7185 = 3 \cdot 5 \cdot 479 \\
121^2 (mod\ 7215) &= 211 \\
147^2 (mod\ 7215) &= 7179 = 3 \cdot 2393 \\
148^2 (mod\ 7215) &= 259 = 7 \cdot 37 \\
189^2 (mod\ 7215) &= 6861 = 3 \cdot 2287 \\
190^2 (mod\ 7215) &= 25 = 5^2 \\
208^2 (mod\ 7215) &= 7189 = 7 \cdot 13 \cdot 79 \\
209^2 (mod\ 7215) &= 391 = 17 \cdot 23 \\
224^2 (mod\ 7215) &= 6886 = 2 \cdot 11 \cdot 313 \\
225^2 (mod\ 7215) &= 120 = 2^3 \cdot 3 \cdot 5 \\
240^2 (mod\ 7215) &= 7095 = 3 \cdot 5 \cdot 11 \cdot 43 \\
241^2 (mod\ 7215) &= 361 = 19^2.
\end{aligned}$$

Sada u Tablicu 2 unosimo samo one b_i *koje smo uspjeli zapisati kao produkt brojeva iz* $\mathscr{B}$*, a ispod brojeva iz* $\mathscr{B}$ *unosimo* α_{ij}*, tj. potencije brojeva iz* $\mathscr{B}$*.*
U Tablici 2 tražimo podskup redaka u kojima je suma α_{ij} *paran broj u svakom stupcu. Jednu takvu sumu daju nam* 2. *i* 5. *redak, a to nam daje kongruenciju:*

$$\begin{aligned}
(b_2 \cdot b_5)^2 &\equiv (190 \cdot 241)^2 (mod\ 7215) \equiv 2500^2 (mod\ 7215), \\
(45790)^2 &\equiv 2500^2 (mod\ 7215).
\end{aligned}$$

Sada je $(45790 + 2500, 7215) = 5$ *netrivijalan faktor od* n*. Dakle,* $n = 4 \cdot 1443$.

4 Metoda verižnog razlomka

U ovom poglavlju upoznat ćemo se s osnovnim pojmovima i rezultatima vezanim za verižne razlomke. Nakon toga ćemo se baviti algoritmom za faktorizaciju prirodnih brojeva i pogledat ćemo na primjerima kako taj algoritam funkcionira.

4.1 Verižni razlomci

Za početak uvedimo nekoliko definicija i rezultata kako bismo mogli razumjeti algoritam za faktorizaciju. Detaljnije o verižnim razlomcima možemo pronaći u [3].

Definicija 5. *Neka je $\alpha \in \mathbb{R}$. Stavimo $a_0 = \lfloor \alpha \rfloor$. Ako je $a_0 \neq \alpha$ stavimo $\alpha = a_0 + \frac{1}{\alpha_1}$, tj. $\alpha_1 = \frac{1}{\alpha - a_0} > 1$ i $a_1 = \lfloor \alpha_1 \rfloor$. Ako je $a_1 \neq \alpha_1$ stavimo $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, tj. $\alpha_2 = \frac{1}{\alpha_1 - a_1} > 1$ i $a_2 = \lfloor \alpha_2 \rfloor$. Taj postupak ponavljamo i on staje ako je za neki $m \in \mathbb{N}$ $a_m = \alpha_m$. Tada je*

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \cfrac{1}{a_m}}}}$$

i vrijedi $\alpha \in \mathbb{Q}$. Uočimo da je $a_0 \in \mathbb{Z}$ i $a_i \in \mathbb{N}$, za svaki $i = 1, \ldots, m$. Takav α pišemo u obliku $\alpha = [a_0, a_1, \ldots, a_m]$ i kažemo da je to razvoj broja α u jednostavan verižni razlomak . Ako je $\alpha_m \neq a_m$, za svaki m, onda je $\alpha \in \mathbb{I}$ i imamo razvoj oblika $\alpha = [a_0, a_1, \ldots]$.

Primjer 9. *Odredimo razvoj od $\alpha \in \mathbb{R}$ u jednostavan verižni razlomak ako je:*

(1.) $\alpha = \frac{193}{25}$
Rješenje: Primjenom Euklidovog algoritma lako dobijemo razvoj od α u jednostavan verižni razlomak.

$$\begin{aligned} 193 &= 7 \cdot 25 + 18 \\ 25 &= 1 \cdot 18 + 7 \\ 18 &= 2 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1. \end{aligned}$$

Dakle, $\alpha = \frac{193}{25} = [7, 1, 2, 1, 1, 3]$

(2.) $\alpha = \frac{53}{37}$
Rješenje: Analogno kao u prethodnom dobijemo sljedeći razvoj:

$$\alpha = \frac{53}{37} = [1, 2, 3, 5].$$

Definicija 6. *Ako je dan razvoj broja α u jednostavni verižni razlomak onda se racionalan broj*

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$$

zove n-ta konvergenta u razvoju broja α u jednostavni verižni razlomak.

Teorem 4 (vidjeti [3, Lema 8.13])**.** *Za $n \geqslant 2$ vrijedi*

$$p_n = a_n p_{n-1} + p_{n-2},\ p_0 = a_0,\ p_1 = a_0 a_1 + 1$$
$$q_n = a_n q_{n-1} + q_{n-2},\ q_0 = 1,\ q_1 = a_1.$$

Definicija 7. *Za beskonačni verižni razlomak $[a_0, a_1, a_2, \ldots]$ kažemo da je periodski ako postoje cijeli brojevi $k \geqslant 0$, $m \geqslant 1$ takvi da je $a_{m+n} = a_n$ za sve $n \geqslant k$. U tom slučaju verižni razlomak pišemo u obliku*

$$[a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+m-1}}],$$

gdje crta iznad brojeva $a_k, \ldots, a_{k+m-1}$ znači da se taj blok brojeva ponavlja unedogled. Broj m se naziva duljina perioda.

Teorem 5 (vidjeti [3, Teorem 8.41])**.** *Ako prirodni broj n nije potpun kvadrat, onda razvoj u jednostavan verižni razlomak od $\sqrt{n}$ ima oblik*

$$\sqrt{n} = [a_0, \overline{a_1, a_2, \ldots, a_{r-1}, 2a_0}],$$

gdje je $a_0 = \lfloor \sqrt{n} \rfloor$ te su $a_1, \ldots, a_{r-1}$ centralno simetrični, tj $a_1 = a_{r-1}, a_2 = a_{r-2}, \ldots$

Takav razvoj dobijemo po sljedećim formulama:

$$s_0 = 0,\ t_0 = 1,\ a_i = \left\lfloor \frac{s_i + \lfloor \sqrt{n} \rfloor}{t_i} \right\rfloor$$
$$s_{i+1} = a_i t_i - s_i,\ t_{i+1} = \frac{n - s_{i+1}^2}{t_i}, \quad i \in \mathbb{N}.$$

Primjer 10. *Neka je $\alpha = \sqrt{12}$. Pronađimo razvoj od α u verižni razlomak.*
Rješenje: Primjenom gore nevedenih formula dobijemo razvoj od α:

$$s_0 = 0,\ t_0 = 1,\ a_0 = \left\lfloor \frac{0 + \lfloor \sqrt{12} \rfloor}{1} \right\rfloor = 3,$$
$$s_1 = 3 \cdot 1 - 0 = 3,\ t_1 = \frac{12 - 3^2}{1} = 3,\ a_1 = \left\lfloor \frac{3 + \lfloor \sqrt{12} \rfloor}{3} \right\rfloor = 2,$$
$$s_2 = 2 \cdot 3 - 3 = 3,\ t_2 = \frac{12 - 3^2}{3} = 1,\ a_2 = \left\lfloor \frac{3 + \lfloor \sqrt{12} \rfloor}{1} \right\rfloor = 6.$$

Dakle, $\alpha = [3, \overline{2, 6}]$.

4.2 Algoritam verižnog razlomka

Metoda verižnog razlomka naziva se još i Brillhart-Morrisonova metoda jer su je oni iskoristili za faktorizaciju Fermatovog[1] broja $2^{2^7}+1$.
Neka je n složen broj. Možemo pretpostaviti da n nije potpun kvadrat. Tada je razvoj broja $\sqrt{n}$ u verižni razlomak periodičan. Neka je $\frac{p_i}{q_i}$ i-ta konvergenta tog verižnog razlomka. Za njih vrijedi

$$p_i^2 - nq_i^2 = (-1)^{n-1}t_{i+1}, \text{ za } i \geqslant 0 \text{ te } s_i < \sqrt{n},\ t_i \leqslant 2\sqrt{n},$$

odnosno

$$p_i^2 \equiv w_i (\text{mod } n),$$

gdje je $w_i = (-1)^i t_i$. Ako uspijemo pronaći neke w_i-ove čiji je produkt potpun kvadrat, tj. $w_{k_1}^2 \dots w_{k_m}^2 = w^2$, onda smo pronašli željenu kongruenciju

$$(p_{k_1} \dots p_{k_m})^2 \equiv w^2 (\text{mod } n),$$

odnosno

$$(p_{k_1} \dots p_{k_m})^2 - w^2 \equiv 0 (\text{mod } n),$$

tj.

$$(p_{k_1} \dots p_{k_m} + w)(p_{k_1} \dots p_{k_m} - w) \equiv 0 (\text{mod } n).$$

Sada računamo $(p_{k_1} \dots p_{k_m} + w)$ i $(p_{k_1} \dots p_{k_m} - w)$ i ako dobijemo brojeve različite od n ili 1 dobili smo netrivijalan faktor od n i faktorizirali smo n (vidjeti [2]).

Pogledajmo primjenu algoritma verižnog razlomka na nekoliko primjera.

Primjer 11 (vidjeti [2, Primjer 5.15, str.234])**.** *Metodom verižnog razlomka faktorizirajmo* $n = 9073$.
Rješenje: Najprije broj $\sqrt{9073}$ *razvijemo u verižni razlomak. U tablicu stavimo* s_i, t_i, a_i, p_i*:*

i	*0*	*1*	*2*	*3*	*4*	*5*
s_i	*0*	*95*	*49*	*90*	*92*	*82*
t_i	*1*	*48*	*139*	*7*	*87*	*27*
a_i	*95*	*3*	*1*	*26*	*2*	*6*
p_i	*95*	*286*	*381*	*1119*	*2619*	*16833*

.

$$\sqrt{9073} = [95; 3, 1, 26, 2, 6].$$

Sada tražimo takve w_i*-ove čiji će produkt biti potpun kvadrat. Očito je*

$$w_0 w_4 = (-1)^1 48 (-1)^5 27 = 1296 = 36^2.$$

[1] Brojevi $F_n = 2^{2^n}+1, n \in \mathbb{N}$ nazivaju se Fermatovi brojevi.

Dolazimo do kongruencije:

$$p_0^2 p_4^2 = (95 \cdot 2619)^2 \equiv 3834^2 \equiv 36^2 (mod\ 9073).$$

Sada izračunamo $(3834 + 36, 9073) = 43$ *i* $(3834 - 36, 9073)$ *i to su netrivijalni faktori od* n. *Dakle,* $9073 = 43 \cdot 211$.

Primjer 12. *Neka je* $n = 377$. *Metodom verižnog razlomka faktorizirajmo* n.
Rješenje: Najprije ćemo broj $\sqrt{377}$ *razviti u verižni razlomak i zapisati u tablicu* a_i, t_i, a_i *i* p_i. *Dobivamo:*

i	*0*	*1*	*2*	*3*	*4*
s_i	*0*	*19*	*13*	*13*	*19*
t_i	*1*	*16*	*13*	*16*	*1*
a_i	*19*	*2*	*2*	*2*	*38*
p_i	*19*	*39*	*97*	*233*	*8951*

.

Dakle, $\sqrt{377} = [19, 2, 2, 2, 38]$.
Tražimo takve w_i *čiji je produkt potpun kvadrat. Očito je*

$$w_1 w_3 = (-1)^2 16 (-1)^2 16 = 16^2.$$

Tako dolazimo do kongruencije:

$$p_1^2 p_3^2 = (39 \cdot 233)^2 \equiv (9087)^2 \equiv 39^2 (mod\ 377).$$

Sada pomoću Euklidovog algoritma izračunamo $(9087 + 39, 377) = 13$ *i dobijemo faktorizaciju od* n. *Dakle,* $377 = 13 \cdot 29$.

5 Pollardova ρ metoda

Pollardova ρ metoda je jedna od najjednostavnijih metoda faktorizacije. Ona generira niz brojeva koji su kandidati za faktore danog broja n, a logička struktura algoritma podsjeća na grčko slovo ρ.
Neka je n složen broj kojeg želimo faktorizirati.Ideja faktorizacije broja n je sljedeća:

(1.) Odaberemo polinom f stupnja većeg ili jednakog od 2. Obično radi jednostavnosti biramo $f(x) = x^2 + 1$.

(2.) Odaberemo sada neku početnu vrijednost x_0 i izračunamo iterativne vrijednosti od f: $x_1 = f(x_0),\ x_2 = f(x_1),\ \ldots\ , x_{j+1} = f(x_j),$ za $j = 0, 1, \ldots, B$, pri čemu B određujemo u 3. koraku

(3.) Pogledamo sve razlike $x_i - x_j$ modulo n sve dok ne odredimo onu za koju je $x_B \not\equiv x_j (\text{mod } n)$, ali $x_B \equiv x_j (\text{mod } n)$, za j za koji je $B > j > 1$. Tada je $(x_B - x_j, n)$ netrivijalan faktor od n.

Pogledajmo sada na nekoliko primjera primjenu Pollardove ρ metode.

Primjer 13. *Pollardovom ρ metodom faktorizirajmo broj:*

(1.) $n = 129$, *za* $x_0 = 1$ *i* $f(x) = x^2 + 1$.
Rješenje: Imamo:

$$x_1 = 2$$
$$x_2 = 5$$
$$x_3 = 26$$
$$x_4 = 677 (mod\ 129) = 32$$
$$x_5 = 1025 (mod\ 129) = 122$$
$$x_6 = 14885 (mod\ 129) = 50$$
$$x_7 = 2501 (mod\ 129) = 50.$$

Lako sada možemo izračunati $(x_4 - x_2, n) = (27, 129) = 3$ *što je netrivijalan faktor od* n.
Dakle, $129 = 3 \cdot 43$.

(2.) $n = 7827$ *za* $x_0 = 1$ *i* $f(x) = x^2 + 1$
Rješenje: Računamo iterativne vrijednosti od f *pa imamo:*

$$x_1 = 2$$
$$x_2 = 5$$
$$x_3 = 26$$
$$x_4 = 677.$$

Sada vidimo da je $(x_4 - x_2, n) = (672, 7827) = 3$ *što je netrivijalan faktor od* n *pa je* $7827 = 3 \cdot 2609$.

(3.) $n = 31861$ *za* $x_0 = 1$ *i* $f(x) = x^2 + 1$
Rješenje:

$$\begin{aligned} x_1 &= 2 \\ x_2 &= 5 \\ x_3 &= 26 \\ x_4 &= 677 \\ x_5 &= 458330 (mod\ 31861) = 12276 \\ x_6 &= 150700177 (mod\ 31861) = 29508 \\ x_7 &= 870722065 (mod\ 31861) = 24657 \\ x_8 &= 607967650 (mod\ 31861) = 27909 \\ x_9 &= 778912282 (mod\ 31861) = 6415 \\ x_{10} &= 41152226 (mod\ 31861) = 19675. \end{aligned}$$

Računamo redom najveće zajedničke djelitelje:

$$(x_2 - x_1) = (3, 31861) = 1,\ (x_4 - x_2) = (672, 31861) = 1, \ldots$$

te dolazimo do

$$(x_{10} - x_5, n) = (7389, 31861) = 151$$

što je faktor od n.
Dakle, $31861 = 151 \cdot 211$.

Objasnimo sada razlog zbog kojeg se ova metoda naziva Pollardova ρ metoda, tj. zašto logička struktura algoritma podsjeća na grčko slovo ρ (vidjeti [6]).

Uzmimo primjerice $n = 29$, $x_0 = 2$ i $f(x) = x^2 + 1$. Izračunajmo nekoliko članova niza $(f(x_j))$. Dobivamo sljedeće:

$$
\begin{aligned}
&x_9 = 442 \equiv 7 (\text{mod } 29) \\
&\uparrow \\
&x_8 = 50 \equiv 21 (\text{mod } 29) \\
&\uparrow \\
&x_7 = 65 \equiv 7 (\text{mod } 29) \\
&\uparrow \\
&x_6 = 530 \equiv 8 (\text{mod } 29) \\
&\uparrow \\
&x_5 = 226 \equiv 23 (\text{mod } 29) \\
&\uparrow \\
&x_4 = 3146 \equiv 14 (\text{mod } 29) \\
&\uparrow \\
&x_3 = 677 \equiv 10 (\text{mod } 29) \\
&\uparrow \\
&x_2 = 26 \\
&\uparrow \\
&x_1 = 5 \\
&\uparrow \\
&x_0 = 2.
\end{aligned}
$$

Iz ovog primjera možemo vidjeti da je $x_7 = x_9$, a računajući x_{10} dobili bismo vrijednost jednaku kao x_8. To znači da bismo se vrtili po krugu između x_7 i x_9. To nam govori da je niz vrijednosti od f periodičan krenuvši od nekog mjesta pa nadalje. Upravo od tu i dolazi naziv ρ metoda jer okrugli dio slova ρ označava periodični dio niza, a ravni dio slova označava pretperiod.

6 Pollardova $p-1$ metoda

Pollardova $p-1$ metoda spada u specijalne metode faktorizacije, a temelji se na Malom Fermatovom teoremu.

Teorem 6 (Mali Fermatov teorem, vidjeti [3, Teorem 3.10]). *Neka je p prost broj i a cijeli broj. Ako p ne dijeli a, onda vrijedu*

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

Napomena 2. *Mali Fermatov teorem predstavlja jedan način za ispitivanje prostosti. Naime, ako postoji prirodan broj $a < p-1$ takav da je $a^{p-1} \not\equiv (mod\ p)$, tada p nije prost broj. Ukoliko za prirodan broj p vrijedi $a^{p-1} \equiv 1 (mod\ p)$, za sve $a \in \{2, 3, \ldots, p-1\}$ to ne znači da je p prost. Prema tome, obrat ovog teorema ne vrijedi.*

Neka je n složen broj i p neki njegov prosti faktor. Prema Malom Fermatovom teoremu vrijedi $a^m \equiv 1 (\mathrm{mod}\, p)$ za svaki višekratnik od $p-1$. Ako bismo pronašli m, onda je $(a^m - 1, n)$ faktor od n. No, pitanje je kako pronaći višekratnike od $p-1$ ako ne znamo p. Kako bismo to objasnili za početak uvedimo novu definiciju.

Definicija 8. *Za prirodan broj kažemo da je B-gladak ako su mu svi prosti faktori $\leqslant B$.*

Primjerice, neka je $B = 8$. Tada je B-gladak broj broj 10 jer su prosti faktori od 10, 2 i 5, ali to može biti i broj 120 jer su njegovi prosti faktori 2, 3 i 5.
Ako je $B = 7$, tada su B-glatki brojevi primjerice 105 i 42.

Ako je $p-1$ B-gladak onda za m možemo uzeti najmanji zajednički višekratnik brojeva $1, 2, \ldots, B$.

Primjer 14. *Navedenom metodom faktorizirajmo sljedeće prirodne brojeve n:*

(1.) *(vidjeti [2, Primjer 5.12, str.230]) Neka je $n = 846631$, $B = 8$ i $a = 2$.*
Rješenje: $m = 2^3 \cdot 3 \cdot 5 \cdot 7 = 840$.
Tada imamo

$$2^{840} (mod\ 846631) = 346905 \ i\ (346905, 846631) = 421.$$

Zaista, $n = 421 \cdot 2011$.

(2.) *Neka je $n = 76$, $B = 5$ i $a = 2$.*
Rješenje: $m = 2 \cdot 3 \cdot 5 = 30$. Sada je

$$2^{30} (mod\ 76) = 68 \ i\ (68, 76) = 4.$$

Dakle, $n = 4 \cdot 19$.

(3.) *Neka je $n = 7173$, $B = 5$ i $a = 3$.*
Rješenje: $m = 2 \cdot 3 \cdot 5 = 30$ pa imamo:

$$3^{30} (mod\ 7173) = 855 \ i\ (855, 7173) = 9.$$

Sada je, $7173 = 9 \cdot 797$.

7 Metoda kvadratnog sita

U ovom poglavlju upoznat ćemo se s još jednom metodom faktorizacije. To je metoda kvadratnog sita, a prije same analize metode uvedimo sljedeću definiciju.

Definicija 9. *Neka je* $(a, n) = 1$. *Ako kongruencija* $x^2 \equiv a (mod\ n)$ *ima rješenja, onda kažemo da je* a *kvadratni ostatak modulo* n. *U protivnom kažemo da je* a *kvadratni neostatak modulo* n.

Primjer 15. *Kvadratni ostatci modulo* 5 *su* 1 *i* 4, *a kvadratni neostatci modulo* 5 *su* 2 *i* 3.

Metoda kvadratnog sita je varijanta metode faktorske baze. Ovdje za faktorsku bazu $\mathscr{B}$ uzimamo sljedeći skup

$$\mathscr{B} = \{p : p \text{ neparan prost broj},\ p \leqslant B,\ \left(\frac{n}{p}\right) = 1\} \cup \{2\},$$

pri čemu je B broj odabran na neki prikladan način, a $\left(\frac{n}{p}\right)$ Legendreov simbol definiran s

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & \text{ako je } n \text{ kvadratni ostatak modulo } p \\ 0, & \text{ako } p \text{ dijeli } n \\ -1, & \text{ako je } n \text{ kvadratni neostatak modulo } p \end{cases}.$$

Skup S u kojem tražimo $\mathscr{B}$-brojeve je skup

$$S = \{t^2 - n : \lfloor\sqrt{n}\rfloor + 1 \leqslant t \leqslant \lfloor\sqrt{n}\rfloor + A\}$$

za neki odabrani A.

Razlika ove i metode faktorske baze leži u tome da ćemo sada uzimati po jedan $p \in \mathscr{B}$ i provjeravati djeljivost p za sve $s \in S$. Upravo od tu i dolazi naziv sito.

Sada ćemo opisati korake za faktorizaciju složenog broja n (vidjeti [2]).

(1.) Odaberemo brojeve A i B. Obično se uzimaju takvi da je $B < A < B^2$.

(2.) Za $t = \lfloor\sqrt{n}\rfloor + 1, \lfloor\sqrt{n}\rfloor + 2, \ldots, \lfloor\sqrt{n}\rfloor + A$ napravimo listu brojeva i stavimo ih u jedan stupac tablice.

(3.) Za svaki prost broj $p \leqslant B$ provjerimo je li $\left(\frac{n}{p}\right) = 1$. Ako nije, izbacimo p iz faktorske baze.

(4.) Za neparan prost broj iz baze $\mathscr{B}$, rješavamo kongruenciju $t^2 \equiv n (\text{mod } p^\beta)$, za $\beta = 1, 2, \ldots$ Neka je β najveći prirodan broj za kojeg postoji t, $\lfloor\sqrt{n}\rfloor + 1 \leqslant t \leqslant \lfloor\sqrt{n}\rfloor + A$, takav da je $t^2 \equiv n (\text{mod} p^\beta)$. Neka su t_1 i t_2 dva rješenja od $t^2 \equiv n (\text{mod } p^\beta)$ takva da je $t_2 \equiv -t_1 (\text{mod} p^\beta)$, t_1 i t_2 nisu nužno oba iz S.

(5.) Za p iz (4.) koraka, pogledamo listu brojeva iz (2.) koraka. U stupcu ispod p stavimo 1 kod svih vrijednosti od $t^2 - n$ kod kojih p dijeli $t - t_1$; promijenimo 1 u 2 ako p^2 dijeli $t - t_1$; 2 u 3 ako p^3 dijeli $t - t_1$, itd. sve dok ne dođemo do p^β. Zatim postupak ponovimo s t_2. Najveći broj koji će se pojaviti u stupcu bit će β.

(6.) Svaki put kada u (5.) koraku stavimo 1, ili promjenimo 1 u 2, 2 u 3, itd. podijelimo odgovarajući $t^2 - n$ s p i zabilježimo rezultat.

(7.) U stupcu ispod $p = 2$, ako $n \not\equiv 1 (\text{mod } 8)$, onda stavimo 1 kod svih $t^2 - n$ u kojima je t neparan te podijelimo $t^2 - n$ s 2. Ako je $n \equiv 1 (\text{mod } 8)$, onda rješavamo kongruenciju $t^2 \equiv n (\text{mod } 2^2\beta)$ i radimo sve isto kao za neparne p.

(8.) Kada prođemo kroz sve proste brojeve p iz $\mathscr{B}$, odbacimo sve $t^2 - n$, osim onih koji su postali jednaki 1 nakon dijeljenja s potencijama prostih brojeva u prethodna dva koraka. Dobivamo tablicu u kojoj će jedan stupac sadržavati vrijednosti elemenata $t^2 - n$ iz S koji su $\mathscr{B}$-brojevi, a ostali stupci će sadržavati potencije od $p \in \mathscr{B}$ u rastavu brojeva $t^2 - n$ na proste faktore.

(9.) Ostatak algoritma je isti kao kod metode faktorske baze.

Pogledajmo sada kako ova metoda funkcionira na primjerima.

Primjer 16. *Metodom kvadratnog sita faktorizirajmo broj* $n = 93$.
Rješenje: Neka su $A = 30$ *i* $B = 20$.
Kandidati za faktorsku bazu $\mathscr{B}$ *su:* $2, 3, 5, 7, 11, 13, 17, 19$.
Za svaki $p \leqslant B$ *provjerimo je li* $\left(\frac{93}{p}\right) = 1$.
Laganim računom dobijemo da su sljedeći Legendreovi simboli jednaki 1*:*

$$\left(\frac{93}{2}\right), \left(\frac{93}{7}\right), \left(\frac{93}{11}\right), \left(\frac{93}{17}\right), \left(\frac{93}{19}\right).$$

Dakle, naša faktorska baza je $\mathscr{B} = \{2, 7, 11, 17, 19\}$.
Za $t = \lfloor\sqrt{n}\rfloor + 1, \ \ldots, \lfloor\sqrt{n}\rfloor + A$ *napravimo listu brojeva* $t^2 - n$ *koji se mogu napisati kao produkt brojeva iz* $\mathscr{B}$*. Dobivamo tablicu*

t	$t^2 - n$	2	7	11	17	19
10	7	-	1	-	-	-
11	28	2	1	-	-	-
13	76	2	-	-	-	1
17	196	2	2	-	-	1
25	532	2	1	-	-	1
29	748	2	-	1	1	-
32	931	-	2	-	-	1

.

Sada tražimo retke čija suma će biti paran broj u svakom stupcu. Primjer takvog je suma 1. *i* 2. *retka:* 2 2 $-$ $-$ $-$*. Tako dobivamo sljedeću kongruenciju:*

$$(10 \cdot 11)^2 \equiv (2 \cdot 7)^2 (mod\ 93),$$

tj.

$$17^2 \equiv 14^2 (mod\ 93),$$

odakle dobivamo netrivijalni faktor od n, $(17 - 14, 93) = 3$.
Dakle, $93 = 3 \cdot 31$.

Primjer 17 (vidjeti [5, Exercise 3.(a)])**.** *Neka je* $n = 1046603$. *Metodom kvadratnog sita faktorizirajmo* n.
Rješenje: Neka je $B = 50$ *i* $A = 500$.
Kandidati za faktorsku bazu su svi prosti brojevi p *manji od* $B = 50$. *Računanjem Legendreovih simbola* $\left(\frac{1046603}{p}\right)$ *dobijemo da je faktorska baza skup*

$$\mathscr{B} = \{2, 13, 17, 19, 29, 37, 41, 47\}.$$

Za $t = \lfloor \sqrt{n} \rfloor + 1,\ \ldots, \lfloor \sqrt{n} \rfloor + A$ *napravimo tablicu u koju unosimo samo one brojeve* $t^2 - n$ *koji se mogu napisati kao produkt brojeva iz* $\mathscr{B}$. *Dobivamo:*

t	$t^2 - n$	2	13	17	19	29	37	41	47
1030	14297	-	-	1	-	2	-	-	-
1319	693158	1	-	1	1	1	1	-	-
1370	830297	-	2	3	-	-	-	-	-
1493	1182446	1	-	-	1	2	1	-	-

.

1. *i* 3. *redak daju parnu sumu u svakom stupcu:*

$$-\ 2\ 4\ -\ 2\ -\ -\ -,$$

te tako dobivamo kongruenciju:

$$(1030 \cdot 1370)^2 \equiv (13 \cdot 17^2 \cdot 29)^2 (mod\ 1046603),$$

tj.

$$364497^2 \equiv 108953^2 (mod\ 1046603).$$

Sada je $(364497 - 108953, 1046603) = 1879$ *netrivijalan faktor od* $n = 1046603$ *pa je* $1046603 = 1879 \cdot 557$.

8 Faktorizacija pomoću eliptičkih krivulja

Najvažnija modifikacija Pollardove $p-1$ metode je Lenstrina metoda faktorizacije pomoću liptičkih krivulja. Danas je ova metoda jedna od najefikasnijih poznatih algoritama za faktorizaciju i detaljnije je opisana u [2, 3].

Za početak, upoznajmo se s osnovnim pojmovima vezanim za eliptičke krivulje, a više o njima može se pronaći u [7].

Neka je $\mathbb{K}$ polje. Općenito, eliptička krivulja nad $\mathbb{K}$ je nesingularna projektivna kubna krivulja nad $\mathbb{K}$ s barem jednom točkom. Njezina jednadžba je oblika

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$

gdje su koeficijenti $a, b, c, \ldots, j \in \mathbb{K}$, a nesingularnost znači da je u svakoj točki na krivulji barem jedna parcijalna derivacija funkcije F različita od 0. Svaka takva jednadžba može se biracionalnim [2] transformacijama svesti na oblik

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

koji nazivamo Weierstassova forma.

Definicija 10. *Neka je $\mathbb{K}$ polje. Karakteristika polja $\mathbb{K}$ je najmanji prirodni broj n takav da je $n \cdot 1 = 0$, gdje su 0 i 1 neutralni elementi za zbrajanje, odnosno množenje u $\mathbb{K}$.*

Ako je $n \cdot 1 \neq 0$ za svaki prirodan broj n, onda kažemo da je $\mathbb{K}$ polje karakteristike 0.
Polja $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su polja karakteristike 0, dok je $\mathbb{F}_q$ polje karakteristike p, gdje je p prost broj i $q = p^m$ za neki prirodan broj m. Karakteristika polja je ili 0 ili prost broj.

Ako je karakteristika polja $\mathbb{K}$ različita od 2 ili 3, onda se jednadžba (2) transformira u oblik

$$y^2 = x^3 + ax + b$$

koji nazivamo kratka Weierstrassova forma (vidjeti [2]).

Ovdje ćemo promatrati eliptičke krivulje nad prstenom $\mathbb{Z}_n$. Pretpostavit ćemo da je $(n, 6) = 1$ te ćemo promatrati eliptičke krivulje oblika

$$E_{a,b} : y^2 = x^3 + ax + b,$$

gdje je

$$(4a^3 + 27b^2, n) = 1.$$

Jedno od najvažnijih svojstava eliptičkih krivulja je da se na njima može definirati operacija uz koju one postaju Abelove grupe.
Neka je $\mathbb{K} = \mathbb{R}$ polje realnih brojeva. Tada eliptičke krivulje možemo prikazati kao podskup ravnine. Definirat ćemo operaciju zbrajanja na eliptičkoj krivulji E. Neka su P i Q dvije

[2] Biracionalne transformacije su racionalne transformacije čiji je inverz također racionalna transformacija.

točke na krivulji E. Povucimo pravac kroz točke P i Q. On siječe krivulju E u tri točke P, Q i treću točku označimo s $P * Q$. Sada označimo osnosimtričnu točku točki $P * Q$ obrizom na os x, s $P + Q$. Dakle, operacija zbrajanja se uvodi "geometrijski". Ovaj geometrijski zakon može se opisati i eksplicitnim formulama za zbrajanje točaka. Tako dobivene formule mogu poslužiti za definiciju zbrajanja točaka na eliptičkoj krivulji nad proizvoljnim poljem. Navedimo te formule.
Neka je $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Tada je:

$$
\begin{aligned}
&1) -\mathscr{O} = \mathscr{O},\\
&2) -P = (x_1, -y_1),\\
&3) \mathscr{O} + P = P,\\
&4) \text{ ako je } Q = -P, \text{ onda je } P + Q = \mathscr{O},\\
&5) \text{ ako je } Q \neq -P, \text{ onda je } P + Q = (x_3, y_3), \text{ gdje je}\\
&\quad x_3 = \lambda^2 - x_1 - x_2,\ y_3 = -y_1 + \lambda(x_1 - x_3),\\
&\quad \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1,\\ \frac{3x_1^2 + a}{2y_1}, & \text{ako je } x_2 \neq x_1. \end{cases}
\end{aligned}
$$

Po definiciji stavljamo da je $P + \mathscr{O} = \mathscr{O} + P = P$, za svaki $P \in E$, pri čemu je $\mathscr{O}$ neutralni element. Pokazuje se da je skup E uz ovako definiranu operaciju Abelova grupa. Sva svojstva Abelove grupe, osim svojstva asocijativnosti, lako se pokazuju dok je dokaz asocijativnosti nešto složeniji.

U primjenama eliptičkih krivulja često je potrebno izračunati višekratnik neke točke P, tj. točku

$$[k]P = \underbrace{P + P + \cdots + P}_{k \text{ pribrojnika}}$$

Opišimo sada osnovne korake u Lenstrinu algoritmu za faktorizaciju broja n (vidjeti [2]).

(1.) Izbor elipričke krivulje.
Primjerice, slučajno izaberemo elemente $a, x, y \in \mathbb{Z}_n$, pa izračunamo $b = (y^2 - x^3 - ax) \bmod n$. Neka je $g = (4a^3 + 27b^2, n)$. Ako je $1 < g < n$, onda smo našli netrivijalni faktor od n. Ako je $g = n$, onda biramo nove a, x, y. Ako je $g = 1$, onda smo našli eliptičku krivulju $E_{a,b}$ nad $\mathbb{Z}_n$ i točku $P = (x, y)$ na njoj.

(2.) Neka je k najmanji zajednički višekratnik brojeva $1, 2, 3, \ldots, B$, za prikladno odabranu granicu B. U praksi se obično uzima $B = 10000$, a zatim se granica po potrebi povećava.

(3.) Računamo $[k]P \in E_{a,b}(\mathbb{Z}_n)$ koristeći formule za zbrajanje točaka na eliptičkim krivuljama:

$$(x_3, y_3) = (\lambda^2 - x_1 - x_2 (\bmod\ n), \lambda(x_1 - x_3) - y_1 (\bmod\ n)),$$

gdje je $\lambda = (3x_1^2 + a)(2y_1)^{-1} \bmod n$ ako su točke jednake, a $\lambda = (y_1 - y_2)(x_1 - x_2)^{-1} \bmod n$ inače.

(4.) Ako se u računanju $[k]P$ dogodi da neki zbroj točaka ne možemo izračunati zato što za neki broj, nazovimo ga d, ne možemo izračunati d^{-1} jer d nema inverz modulo n, onda izračunamo $g = (d, n)$. Ako je $g \neq n$, onda smo našli netrivijalan faktor od n.

(5.) U slučaju neuspjeha, možemo izabrati novu eliptičku krivulju ili povećati granicu za B.

Pogledajmo na primjeru kako funkcionira Lenstrin algoritam za faktorizaciju prirodnih brojeva.

Primjer 18 (vidjeti [2, Primjer 5.13, str.232]). *Neka je* $n = 209$. *Pomoću eliptičkih krivulja faktorizirajmo* n.
Rješenje: Neka je $B = 3$ *pa je* $k = 6$.
Računamo $[k]P = [6]P = [2](P + [2]P)$. *Najprije ćemo izračunati* $[2]P$, *a zatim* $[3]P = P + [2]P$. *Pripadni* λ *za točku* $[2]P$ *je* $4 \cdot 6^{-1} = 140 (mod\ 209)$ *pa dobivamo* $[2]P = (163, 169) = 1$. *Sada računamo* $[3]P = P + [2]P$. *Pripadni* λ *za ovu točku je* $166 \cdot 163^{-1} = 60 (mod\ 209)$, *pa je* $[3]P = (148, 143) = 1$.
Konačno, računamo $[6]P = [2]([3]P)$. *Pripadni* λ *je* $90 \cdot 77^{-1}$. *Inverz od* 77 *modulo* 209 *ne postoji jer je* $(77, 209) = 11$, *pa zaključujemo da je* 11 *faktor od* 209. *Zaista,* $209 = 11 \cdot 19$.

Literatura

[1] S. C. Coutinho, *The Mathematics of Ciphers-Number Theory and RSA Cryptography*, A. K. Peters, Rio de Janeiro, 1998.

[2] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[3] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[4] G. Everest, T. Ward, *An Introduction to Number Theory*, Springer, Norwich, 2005.

[5] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1994.

[6] R. A. Mollin, *An Introduction to Cqyptography*, Chapman i Hall/CRC, Boca Raton, 2007.

[7] J. H. Silverman, J. Tate, *Rational points on Eliptic Curves*, Springer, New York, 1992.