View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Repository of Faculty of Science, University of Zagreb

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Kristina Kralj

PRIMJENA VERIŽNIH RAZLOMAKA U FAKTORIZACIJI I TESTIRANJU PROSTOSTI

Diplomski rad

Voditelj rada:
akad. Andrej Dujella

Zagreb, studeni, 2017.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Prirodan broj p je prost ako nema niti jednog djelitelja osim broja 1 i samog sebe. Ako broj nije prost, tada kažemo da je složen. Postavlja se pitanje o tome je li skup prostih brojeva konačan te postoji li najveći prosti broj. Na to pitanje odgovor je dao Euklid dokazavši da prostih brojeva ima beskonačno mnogo.

Prosti brojevi su zanimljivi zbog toga što svaki prirodan broj možemo napisati kao umnožak prostih brojeva. Osnovni teorem aritmetike govori da je faktorizacija svakog prirodnog broja jedinstvena. No, nije uvijek jednostavan zadatak pronaći faktorizaciju, pogotovo ako taj određeni broj ima puno znamenaka. Zapravo je puno lakše pomnožiti dva velika prosta broja nego faktorizirati njihov produkt. Na toj ideji temelje se neki kriptosustavi pa je zbog toga zanimljivo istraživati različite metode faktorizacije. U ovom radu bavit ćemo se metodom faktorizacije velikih prirodnih brojeva pomoću verižnih razlomaka. Za faktorizaciju broja n koristit će se razvoj broja $\sqrt{n}$ u verižni razlomak te njegove konvergente. Prije opisivanja same metode, reći ćemo nešto o verižnim razlomcima te njihovim svojstvima i primjeni. Osnovna literatura je knjiga *Prime Numbers and Computer Methods for Factorization*, koju je napisao H. Riesel [6].

Također ćemo se baviti pitanjem je li neki prirodni broj prost ili složen. Za mali prirodni broj n možemo odrediti je li on prost ili složen jednostavnim dijeljenjem svim prostim brojevima manjim od $\sqrt{n}$. No, za velike prirodne brojeve potrebna je efikasnija metoda testiranja prostosti. Jedna metoda bit će opisana u ovom radu, a to je metoda verižnog razlomka. Pokazat ćemo da konvergente verižnog razlomka dobivenog razvojem broja $\sqrt{3}$ imaju neka zanimljiva svojstva pomoću kojih možemo testirati prostost prirodnih brojeva. Osim općenitog testa, bit će opisan i slučaj testiranja prostosti Mersennovih brojeva. Mersennovi brojevi imaju jedno posebno svojstvo pomoću kojeg možemo test prostosti provesti na jednostavniji način. Vidjet ćemo da za Mersennov broj možemo efikasno odrediti je li on prost ili složen. Ovaj dio napisan je prema knjizi *Factorization and Primality Testing*, čiji je autor D.M. Bressoud [1].

U radu će biti navedene neke tvrdnje i teoremi iz teorije brojeva, čiji dokazi se mogu naći u [3]. Svi izračuni u radu dobiveni su pomoću programa napisanih u programskom jeziku Python.

Poglavlje 1

Verižni razlomci

U ovom poglavlju definirat ćemo verižne razlomke te navesti njihova osnovna svojstva i primjene.

1.1 Jednostavni verižni razlomci

Definicija 1.1.1. *Verižni razlomak je izraz oblika*

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \ddots}}}. \tag{1.1}$$

Brojevi a_i nazivaju se parcijalni kvocijenti verižnog razlomka.

Ukoliko su svi djelomični brojnici b_i jednaki 1, tada se radi o jednostavnom verižnom razlomku i on je oblika

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}. \tag{1.2}$$

Jednostavne verižne razlomke još zapisujemo u obliku $[a_0; a_1, a_2, a_3, \ldots]$, odnosno u obliku $[a_0; a_1, a_2, a_3, \ldots, a_n]$, ako je verižni razlomak konačan. U tom slučaju $a_0, a_1, a_2, \ldots$ su *elementi* verižnog razlomka te mogu biti realni ili kompleksni. Mi ćemo se baviti slučajevima

kada su $a_1, a_2, \ldots \in \mathbb{N}$, a $a_0 \in \mathbb{Z}$. U ovom radu će se koristiti samo jednostavni verižni razlomci pa ćemo ih kraće nazivati "verižni razlomci". Broj elemenata verižnog razlomka može biti konačan ili beskonačan. Prema tome, izraz (1.2) predstavlja beskonačni verižni razlomak, dok izraz oblika

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \; + \cfrac{1}{a_n}}}} \tag{1.3}$$

predstavlja konačni verižni razlomak. U slučaju da su mu elementi racionalni brojevi, možemo točno odrediti vrijednost tog verižnog razlomka što znači da se zapravo radi o racionalnom broju. Može se pokazati da se svaki racionalni broj može zapisati u obliku konačnog verižnog razlomka. S druge strane, vrijednost beskonačnog verižnog razlomka ne možemo tako jednostavno odrediti.

1.2 Euklidov algoritam i konačni verižni razlomci

Euklidov algoritam je efikasan algoritam za nalaženje najvećeg zajedničkog djelitelja dvaju prirodnih brojeva. Neka su a i b dva broja kojima tražimo najveći zajednički djelitelj. Raspišimo Euklidov algoritam kao niz koraka:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Ovdje je najveći zajednički djelitelj brojeva a i b posljednji ne-nul ostatak u algoritmu, odnosno $nzd\ (a, b) = r_n$. Budući da je konačni verižni razlomak zapravo racionalni broj, svaki racionalni broj može se razviti u jednostavni verižni razlomak pomoću Euklidovog algoritma. Primjenom Euklidovog algoritma na brojnik i nazivnik racionalnog broja $\frac{a}{b}$

dobivamo

$$\begin{aligned}
\frac{a}{b} &= q_1 + \cfrac{1}{\cfrac{b}{r_1}}, \\
\frac{a}{b} &= q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cfrac{r_1}{r_2}}}, \\
&\vdots \\
\frac{a}{b} &= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ddots \; + \cfrac{1}{q_n}}}}.
\end{aligned}$$

Posljednji izraz naziva se *razvoj broja $\frac{a}{b}$ u jednostavni verižni razlomak*. Primijetimo da za svaki razlomak $\frac{a}{b}$ kojem je brojnik manji od nazivnika dobivamo $q_1 = 0$. To znači da će razvoj svakog "pravog" razlomka u verižni razlomak biti oblika $[0; q_2, q_3, q_4, \ldots, q_n]$.

1.3 Beskonačni verižni razlomci

Iracionalni brojevi mogu se također razviti u verižni razlomak, samo što će u tom slučaju verižni razlomak biti beskonačan. Naravno, postupak razvoja je drugačiji nego za racionalne brojeve. Ako je razvoj realnog broja β u jednostavni verižni razlomak oblika kao u (1.2), parcijalni kvocijenti $a_0, a_1, a_2, \ldots$ dobivaju se na sljedeći način:

$$a_0 = \lfloor \beta \rfloor, \quad \beta = a_0 + \frac{1}{\beta_1}, \quad a_1 = \lfloor \beta_1 \rfloor, \quad \beta_1 = a_1 + \frac{1}{\beta_2}, \quad a_2 = \lfloor \beta_2 \rfloor, \ \ldots. \tag{1.4}$$

Postupak se nastavlja sve dok je $a_k \neq \beta_k$.

Ukoliko je verižni razlomak konačan, možemo odrediti njegovu vrijednost i zapisati ga kao racionalni broj. No, kako bismo odredili vrijednost beskonačnog verižnog razlomka? Njegovu vrijednost možemo samo aproksimirati pomoću *konvergenti* tog verižnog razlomka. Konvergente predstavljaju jedan dio verižnog razlomka, pri čemu konačni verižni razlomci imaju konačan broj konvergenti, a beskonačni imaju beskonačno mnogo konvergenti.

Definicija 1.3.1. *Racionalne brojeve*

$$\frac{A_n}{B_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n}}}} = [a_0; a_1, a_2, \ldots, a_n] \tag{1.5}$$

nazivamo konvergente verižnog razlomka $\beta = [a_0; a_1, a_2, a_3, \ldots]$.

Konvergente beskonačnog verižnog razlomka bit će nam važne u nastavku, kao i sljedeći teorem koji govori o vezi između uzastopnih konvergenti verižnog razlomka.

Teorem 1.3.2. *Brojnici i nazivnici konvergenti* $\frac{A_n}{B_n}$ *zadovoljavaju sljedeće rekurzije:*

$$A_0 = a_0, \quad A_1 = a_0a_1 + 1, \quad A_n = a_nA_{n-1} + A_{n-2},$$
$$B_0 = 1, \quad B_1 = a_1, \quad B_n = a_nB_{n-1} + B_{n-2}.$$

Dokaz. Neka je verižni razlomak oblika $[a_0; a_1, a_2, a_3, \ldots]$. Njegova prva konvergenta je $\frac{A_1}{B_1} = a_0 + \frac{1}{a_1} = \frac{a_0a_1+1}{a_1}$ pa formule za A_1 i B_1 očito vrijede. Rekurzije za A_n i B_n dokazujemo matematičkom indukcijom. Najprije za $n = 2$ računamo konvergentu $\frac{A_2}{B_2}$:

$$\frac{A_2}{B_2} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} = a_0 + \frac{a_2}{a_1a_2 + 1} = \frac{a_0a_1a_2 + a_0 + a_2}{a_1a_2 + 1} = \frac{a_2(a_0a_1 + 1) + a_0}{a_1a_2 + 1}$$
$$= \frac{a_2A_1 + A_0}{a_2B_1 + B_0}.$$

Dakle, rekurzivne formule su istinite za $n = 2$. Ako pretpostavimo da one vrijede za neki prirodan broj $n \geq 2$, tada trebamo pokazati da vrijede i za $n + 1$. Uočimo da konvergentu $\frac{A_{n+1}}{B_{n+1}}$ možemo dobiti iz konvergente $\frac{A_n}{B_n}$:

$$\frac{A_{n+1}}{B_{n+1}} = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_n + \cfrac{1}{a_{n+1}}}}$$

tako da umjesto zadnjeg parcijalnog kvocijenta a_n napišemo $a_n + \frac{1}{a_{n+1}}$. Stoga, ako navedene rekurzivne formule vrijede za broj n tada vrijedi:

$$\frac{A_{n+1}}{B_{n+1}} = \frac{(a_n + \frac{1}{a_{n+1}})A_{n-1} + A_{n-2}}{(a_n + \frac{1}{a_{n+1}})B_{n-1} + B_{n-2}} = \frac{a_nA_{n-1} + A_{n-2} + \frac{A_{n-1}}{a_{n+1}}}{a_nB_{n-1} + B_{n-2} + \frac{B_{n-1}}{a_{n+1}}} = \frac{A_n + \frac{A_{n-1}}{a_{n+1}}}{B_n + \frac{A_{n-1}}{a_{n+1}}} = \frac{a_{n+1}A_n + A_{n-1}}{a_{n+1}B_n + B_{n-1}}.$$

Stavljanjem broja $n+1$ umjesto n u rekurzivne formule iz teorema 1.3.2 dobivamo isti izraz pa je time teorem dokazan. □

Koristeći rekurzivni postupak iz ovog teorema, možemo računati konvergente verižnog razlomka te na taj način aproksimirati njegovu vrijednost. Konvergente verižnog razlomka daju jako dobru racionalnu aproksimaciju realnih brojeva.

Još jedan način na koji možemo promatrati konvergentu $\frac{A_n}{B_n}$ verižnog razlomka je kao linearnu funkciju koja ovisi o a_n. Zapišimo je u obliku:

$$\frac{A(t)}{B(t)} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{t}}}}, \tag{1.6}$$

pri čemu t označava a_n iz izraza (1.5). Tada je

$$R(t) = \frac{A(t)}{B(t)} = \frac{a + bt}{c + dt}, \tag{1.7}$$

za neke konstante a, b, c i d. U izrazu (1.6), ako $t \to \infty$, onda je $R(\infty) = \frac{A_{n-1}}{B_{n-1}}$, a ako $t \to 0$, tada slijedi

$$\frac{1}{a_{n-1} + \frac{1}{t}} \to \frac{1}{a_{n-1} + \infty} = 0.$$

Zbog toga je

$$R(0) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{0}}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-2} + 0}}},$$

odnosno $R(0) = \frac{A_{n-2}}{B_{n-2}}$ Uočimo da za neku konstantu k mora vrijediti

$$\frac{A(t)}{B(t)} = \frac{A_{n-2} + kA_{n-1}t}{B_{n-2} + kB_{n-1}t}$$

da bi $R(0)$ i $R(\infty)$ poprimali točne vrijednosti. Vraćanjem zamjene $t = a_n$ imamo $R(a_n) = \frac{A_n}{B_n}$ i iz toga slijedi

$$\frac{A_n}{B_n} = \frac{A_{n-2} + kA_{n-1}a_n}{B_{n-2} + kB_{n-1}a_n}.$$

Primijetimo da je konstanta $k = 1$ zbog rekurzije iz teorema 1.3.2 te dobivamo da je vrijednost verižnog razlomka $\frac{A(t)}{B(t)}$ jednaka

$$\frac{A(t)}{B(t)} = \frac{A_{n-2} + A_{n-1}t}{B_{n-2} + B_{n-1}t}. \tag{1.8}$$

Važan je i sljedeći teorem koji daje još jednu vezu brojnika i nazivnika konvergente verižnog razlomka.

Teorem 1.3.3. *Brojnici i nazivnici konvergenti A_n i B_n zadovoljavaju sljedeću jednakost*

$$A_{n-1}B_n - A_nB_{n-1} = (-1)^n.$$

Dokaz. Teorem dokazujemo matematičkom indukcijom. Za $n = 1$ imamo $A_0B_1 - A_1B_0 = (-1)^1$, odnosno $a_0a_1 - (a_0a_1 + 1) \cdot 1 = -1$ pa u tom slučaju jednakost vrijedi. Pretpostavimo da jednakost vrijedi za neki prirodan broj n. Tada za $n + 1$ imamo:

$$\begin{aligned} A_nB_{n+1} - A_{n+1}B_n &= A_n(a_{n+1}B_n + B_{n-1}) - (a_{n+1}A_n + A_{n-1})B_n \\ &= a_{n+1}(A_nB_n - A_nB_n) + A_nB_{n-1} - A_{n-1}B_n \\ &= -(A_{n-1}B_n - A_nB_{n-1}) = -(-1)^n \\ &= (-1)^{n+1}. \end{aligned}$$

□

Prema ovom teoremu, brojnik i nazivnik konvergente verižnog razlomka su prosti brojevi. Kad bi A_n i B_n imali zajednički faktor veći od 1 tada bi se on pojavio kao djelitelj od $A_{n-1}B_n - A_nB_{n-1}$. Međutim, jedini mogući djelitelji su 1 i -1 pa su A_n i B_n relativno prosti.

1.4 Periodični verižni razlomci

Iracionalni brojevi imaju beskonačni razvoj u verižni razlomak. Zbog toga primjenom algoritma (1.4) nećemo dobiti sve točne parcijalne kvocijente. No, za iracionalne brojeve

oblika $\sqrt{N}$, pri čemu N nije kvadrat nekog cijelog broja, možemo dobiti točan razvoj u verižni razlomak. To je zbog toga što je njegov razvoj periodičan, što ćemo pokazati u nastavku.

Definicija 1.4.1. *Neka je N prirodan broj koji nije potpuni kvadrat. Parcijalni kvocijenti a_i iz razvoja broja $\sqrt{N}$ u verižni razlomak definirani su na sljedeći način:*

$$x_0 = \sqrt{N}, \quad a_i = \lfloor x_i \rfloor, \quad x_{i+1} = \frac{1}{x_i - a_i}.$$

Prema ovoj definiciji razvoj u verižni razlomak je oblika:

$$\sqrt{N} = [a_0; a_1, a_2, a_3, \ldots, a_n, \ldots],$$

pri čemu su a_i prirodni brojevi. Koristeći oznake iz definicije 1.4.1, zapišimo račun u sljedećem obliku:

$$x_0 = \sqrt{N} = \frac{0 + \sqrt{N}}{1}, \tag{1.9}$$

$$x_1 = \frac{1}{\sqrt{N} - a_0} = \frac{\sqrt{N} + a_0}{N - a_0^2} = \frac{P_1 + \sqrt{N}}{Q_1}, \tag{1.10}$$

$$\begin{aligned} x_2 &= \frac{1}{\frac{P_1+\sqrt{N}}{Q_1} - a_1} = \frac{1}{\frac{\sqrt{N}+P_1-Q_1a_1}{Q_1}} = \frac{Q_1}{\sqrt{N} - (Q_1a_1 - P_1)} = \frac{Q_1}{\sqrt{N} - P_2} \\ &= \frac{Q_1(\sqrt{N} + P_2)}{N - P_2^2} = \frac{\sqrt{N} + P_2}{\frac{N-P_2^2}{Q_1}} = \frac{P_2 + \sqrt{N}}{Q_2} \end{aligned} \tag{1.11}$$

$$\vdots$$

Pritom smo označili: $P_1 = a_0$ i $Q_1 = N - P_1^2$ te $P_2 = Q_1a_1 - P_1$ i $Q_2 = \frac{N-P_2^2}{Q_1}$ i to su cijeli brojevi. Također, primijetimo da smo uzeli $P_0 = 0$ i $Q_0 = 1$. Zapišimo sada taj račun u općenitom obliku:

$$\begin{aligned} x_i &= \frac{1}{x_{i-1} - a_{i-1}} = \frac{1}{\frac{P_{i-1}+\sqrt{N}}{Q_{i-1}} - a_{i-1}} = \frac{1}{\frac{\sqrt{N}+P_{i-1}-Q_{i-1}a_{i-1}}{Q_{i-1}}} = \frac{Q_{i-1}}{\sqrt{N} - (Q_{i-1}a_{i-1} - P_{i-1})} = \frac{Q_{i-1}}{\sqrt{N} - P_i} \\ &= \frac{Q_{i-1}(\sqrt{N} + P_i)}{N - P_i^2} = \frac{\sqrt{N} + P_i}{\frac{N-P_i^2}{Q_{i-1}}} = \frac{P_i + \sqrt{N}}{Q_i}, \end{aligned} \tag{1.12}$$

pri čemu je

$$P_i = Q_{i-1}a_{i-1} - P_{i-1}, \; Q_i = \frac{N - P_i^2}{Q_{i-1}}. \tag{1.13}$$

Dakle, parcijalni kvocijenti razvoja broja $\beta = \sqrt{N}$ u jednostavni verižni razlomak su $a_i = \lfloor x_i \rfloor = \left\lfloor \frac{P_i + \sqrt{N}}{Q_i} \right\rfloor$.

Drugim riječima, razvoj broja $\sqrt{N}$ u verižni razlomak može se dobiti sljedećim algoritmom:

$$\begin{aligned} \sqrt{N} &= [a_0; a_1, a_2, a_3, \ldots], \\ a_0 &= \lfloor \sqrt{N} \rfloor, \quad P_0 = 0, \quad Q_0 = 1, \\ P_{i+1} &= Q_i a_i - P_i, \quad Q_{i+1} = \frac{N - P_{i+1}^2}{Q_i}, \quad a_{i+1} = \left\lfloor \frac{P_{i+1} + \sqrt{N}}{Q_{i+1}} \right\rfloor. \end{aligned} \tag{1.14}$$

Na ovaj način možemo izračunati proizvoljan broj parcijalnih kvocijenata, odnosno odrediti točan razvoj broja $\sqrt{N}$ u verižni razlomak. O tome nam govori i sljedeći teorem.

Propozicija 1.4.2. *Neka je $\beta = \sqrt{N}$ iracionalan broj. Njegov razvoj u jednostavni verižni razlomak je periodičan.*

Dokaz. Trebamo pokazati da su brojevi P_i i Q_i ograničeni te da parova (P_i, Q_i) ima konačan broj. To znači da će se parcijalni kvocijenti početi ponavljati u nekom trenutku. Iz jednakosti (1.12) vidimo da se izraz

$$x_i = \frac{Q_{i-1}}{\sqrt{N} - P_i} = \frac{Q_{i-1}(\sqrt{N} + P_i)}{N - P_i^2} \tag{1.15}$$

uvijek može skratiti do oblika $\frac{P_i + \sqrt{N}}{Q_i}$, što znači da $Q_i = \frac{N - P_i^2}{Q_{i-1}}$ mora biti cijeli broj. To dokazujemo matematičkom indukcijom. Za $i = 1$, prema izrazu (1.10) imamo da je $x_1 = \frac{P_1 + \sqrt{N}}{Q_1}$, gdje je $Q_1 = N - P_1^2$. S obzirom na to da je $P_1 = a_0$, a a_0 je cijeli broj, tada je i P_1 cijeli broj što znači da je i Q_1 cijeli broj. Sada pretpostavimo da je $x_i = \frac{P_i + \sqrt{N}}{Q_i}$ te da vrijedi $Q_i | (N - P_i^2)$. Tada je

$$x_i = \frac{P_i + \sqrt{N}}{Q_i} = \frac{Q_i a_i - P_{i+1} + \sqrt{N}}{Q_i} = a_i + \frac{\sqrt{N} - P_{i+1}}{Q_i}, \tag{1.16}$$

$$x_{i+1} = \frac{1}{x_i - a_i} = \frac{1}{\frac{\sqrt{N} - P_{i+1}}{Q_i}} = \frac{Q_i(\sqrt{N} + P_{i+1})}{N - P_{i+1}^2}.$$

Budući da je $\frac{N - P_i^2}{Q_i}$ cijeli broj, tada je

$$Q_{i+1} = \frac{N - P_{i+1}^2}{Q_i} = \frac{N - (a_i Q_i - P_i)^2}{Q_i} = \frac{N - P_i^2}{Q_i} - a_i^2 Q_i + 2 a_i P_i$$

također cijeli broj. To znači da je Q_i uvijek cijeli broj. Prema definiciji je parcijalni kvocijent $a_{i-1} = \left\lfloor \frac{P_{i-1}+\sqrt{N}}{Q_{i-1}} \right\rfloor$ pa iz svojstva funkcije "najveće cijelo" slijedi

$$a_{i-1} < \frac{P_{i-1} + \sqrt{N}}{Q_{i-1}},$$

odnosno $a_{i-1}Q_{i-1} - P_{i-1} < \sqrt{N}$. Sada je lijeva strana nejednakosti jednaka P_i pa dobivamo $P_i < \sqrt{N}$. Iz jednakosti $P_{i+1} = a_iQ_i - P_i$ izrazimo Q_i i dobivamo

$$Q_i = \frac{P_i + P_{i+1}}{a_i} < 2\sqrt{N}.$$

Iz toga slijedi da je ukupan broj različitih razlomaka $\frac{\sqrt{N}+P_i}{Q_i}$, odnosno parova (P_i, Q_i) u razvoju najviše $\lfloor \sqrt{N} \rfloor \cdot 2\lfloor \sqrt{N} \rfloor < 2N$. Dakle, nakon najviše $2N$ koraka doći ćemo do razlomka $\frac{\sqrt{N}+P_k}{Q_k}$ koji se je već ranije pojavio u razvoju. Zato razvoj mora biti periodičan s periodom duljine najviše $2N - 1$. □

1.5 Neke primjene

Ranije smo vidjeli da beskonačni periodični verižni razlomci predstavljaju iracionalne brojeve oblika $\sqrt{N}$, $N \in \mathbb{N}$. Pomoću konvergenti tih verižnih razlomaka možemo dobiti jako dobre racionalne aproksimacije iracionalnih brojeva. Osim korijena, pomoću verižnih razlomaka mogu se dobiti i racionalne aproksimacije realnih brojeva kao što su π i e.

$$\pi = [3; 7, 15, 1, 292, 1, 1, \ldots] \quad e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots].$$

Neke konvergente verižnog razlomka koje daju aproksimaciju broja π su: $\frac{22}{7}$, $\frac{333}{106}$, $\frac{355}{113}$, a broj e aproksimiraju brojevi: $\frac{8}{3}$, $\frac{11}{4}$, $\frac{19}{7}$.

Verižni razlomci koriste se pri rješavanju linearnih diofantskih jednadžbi. One su oblika $ax + by = c$, pri čemu su koeficijenti a, b, c i rješenja cijeli brojevi. Takve jednadžbe ili nemaju rješenja ili ih imaju beskonačno mnogo. Sva rješenja mogu se dobiti ako se pronađe parcijalno rješenje, a njega možemo dobiti pomoću verižnih razlomaka.

Verižni razlomci poznati su još od doba Euklida (oko 300 god.pr.n.e) te imaju široku primjenu u različitim područjima. Također je važna njihova primjena u kriptografiji gdje se koriste pri faktorizaciji velikih prirodnih brojeva. Ta će njihova primjena biti opisana u sljedećem poglavlju.

Poglavlje 2

Faktorizacija metodom verižnih razlomaka

2.1 Metoda verižnog razlomka

Metodu verižnog razlomka (CFRAC - *continued fration factorization method*) za faktorizaciju velikih prirodnih brojeva razvili su Michael A. Morrison i John Brillhart 1975. godine. Osnovne ideje za ovu metodu dali su D. H. Lehmer and R.E. Powers već 1931. godine, a Brillhart i Morrison su istražujući te ideje napravili algoritam za faktorizaciju. Metoda verižnog razlomka jedna je od najučinkovitijih metoda faktorizacije velikih prirodnih brojeva. To je bila prva metoda sa subeksponencijalnim vremenom izvođenja i tada je bila najbrža metoda faktorizacije. Zasniva se na traženju netrivijalnog rješenja kongruencije $x^2 \equiv y^2 \pmod{N}$, kada je N broj koji želimo faktorizirati.

Definicija 2.1.1. *Neka je $m \neq 0$ cijeli broj. Ako $m|(a-b)$ tada kažemo da je a kongruentan b modulo m i pišemo*

$$a \equiv b \pmod{m}.$$

Nakon što smo pronašli par (x, y) koji zadovoljava kongruenciju $x^2 \equiv y^2 \pmod{N}$, prema gornjoj definiciji znamo da broj N dijeli

$$(x^2 - y^2) = (x - y)(x + y).$$

Zbog toga postoji barem 50% šanse da će najveći zajednički djelitelj brojeva $x - y$ i N biti netrivijalni faktor od N. Primjenom Euklidovog algoritma na brojeve $(x - y,\ N)$ trebali bismo dobiti faktor od N. Kod metode verižnog razlomka brojeve x i y dobivamo iz razvoja broja $\sqrt{N}$ u verižni razlomak. Za detaljniji opis te metode bit će nam potrebna sljedeća tvrdnja.

Teorem 2.1.2. *Neka je $\frac{A_n}{B_n}$ n-ta konvergenta razvoja broja $\sqrt{N}$ u verižni razlomak, P_n i Q_n definirani kao u (1.14). Za sve $n \geq 0$ vrijedi sljedeća formula:*

$$A_{n-1}^2 - NB_{n-1}^2 = (-1)^n Q_n.$$

Dokaz. Prisjetimo se jednakosti (1.8). Uvođenjem zamjene $t = x_n$ u tu jednakost dobivamo:

$$\sqrt{N} = \frac{A_{n-2} + A_{n-1}x_n}{B_{n-2} + B_{n-1}x_n}.$$

Nadalje, uvrstimo $x_n = \frac{\sqrt{N}+P_n}{Q_n}$ (kao u (1.16)). Time dobivamo

$$\sqrt{N} = \frac{Q_n A_{n-2} + P_n A_{n-1} + A_{n-1}\sqrt{N}}{Q_n B_{n-2} + P_n B_{n-1} + B_{n-1}\sqrt{N}},$$

odnosno

$$(Q_n B_{n-2} + P_n B_{n-1})\sqrt{N} + NB_{n-1} = Q_n A_{n-2} + P_n A_{n-1} + A_{n-1}\sqrt{N}.$$

Uz pretpostavku da N nije potpuni kvadrat, $\sqrt{N}$ je iracionalan broj. Tada možemo izjednačiti racionalni dio s lijeve strane jednakosti s racionalnim dijelom s desne strane. Isto tako izjednačimo iracionalne dijelove s obje strane te dobivamo

$$\begin{aligned} Q_n A_{n-2} + P_n A_{n-1} &= NB_{n-1} \\ Q_n B_{n-2} + P_n B_{n-1} &= A_{n-1}. \end{aligned} \tag{2.1}$$

Sada iz prve jednakosti možemo izraziti P_n te uvrstimo u drugu jednakost:

$$Q_n B_{n-2} + \frac{NB_{n-1} - Q_n A_{n-2}}{A_{n-1}} B_{n-1} = A_{n-1}.$$

Sređivanjem dobivamo

$$(A_{n-2}B_{n-1} - A_{n-1}B_{n-2})Q_n = NB_{n-1}^2 - A_{n-1}^2.$$

Prema teoremu 1.3.3, lijeva strana jednakosti je jednaka $(-1)^{n-1}Q_n$ pa vrijedi

$$(-1)^{n-1}Q_n = NB_{n-1}^2 - A_{n-1}^2.$$

Množenjem te jednakosti brojem -1 dobivamo početnu formulu. □

Iz početne formule slijedi i

$$A_{i-1}^2 \equiv (-1)^i Q_i \pmod{N},$$

što znači da je $(-1)^i Q_i$ *kvadratni ostatak modulo* N.

Definicija 2.1.3. *Neka su a i m relativno prosti brojevi. Ako kongruencija* $x^2 \equiv a \pmod{m}$ *ima rješenja, onda kažemo da je a kvadratni ostatak modulo m. U protivnom kažemo da je a kvadratni neostatak modulo m.*

Opišimo sada detaljnije metodu verižnog razlomka. Neka je N broj koji želimo faktorizirati. Uz pretpostavku da N nije potpuni kvadrat, prema propoziciji 1.4.2, razvoj broja $\sqrt{N}$ u verižni razlomak je periodičan. Neka je $\frac{A_i}{B_i} = [a_0; a_1, a_2, \ldots, a_i]$ i-ta konvergenta tog verižnog razlomka te neka su brojevi P_i i Q_i definirani kao u (1.14). Uz teorem 2.1.2 vrijedi

$$A_{i-1}^2 - NB_{i-1}^2 = (-1)^i Q_i,$$

odnosno

$$A_{i-1}^2 \equiv (-1)^i Q_i \pmod{N}.$$

Uz to vrijedi i $Q_i < 2\sqrt{N}$, što smo pokazali u dokazu propozicije 1.4.2. Radi jednostavnosti, označimo $(-1)^i Q_i = t_i$. Nakon što smo odredili brojeve A_i i Q_i iz razvoja $\sqrt{N}$ u verižni razlomak, želimo pronaći neki broj t_j koji je potpuni kvadrat ili neku kombinaciju brojeva t_i čiji produkt će biti potpuni kvadrat. Ukoliko smo pronašli takve brojeve, imamo da je neki produkt $t_{k_1} \cdot t_{k_2} \cdot \ldots \cdot t_{k_m}$ potpuni kvadrat te ga označimo s z^2. Sada koristeći gornje formule, imamo kongruenciju

$$A_{k_1-1}^2 \cdot A_{k_2-1}^2 \cdot \ldots \cdot A_{k_m-1}^2 \equiv z^2 \pmod{N}, \tag{2.2}$$

odnosno

$$(A_{k_1-1} \cdot A_{k_2-1} \cdot \ldots \cdot A_{k_m-1})^2 \equiv z^2 \pmod{N}.$$

Umnožak na lijevoj strani možemo zamijeniti njegovim najmanjim pozitivnim ostatkom modulo N. Zapišimo kongruenciju u obliku

$$(A_{k_1-1} \cdot A_{k_2-1} \cdot \ldots \cdot A_{k_m-1})^2 - z^2 \equiv 0 \pmod{N},$$

$$(A_{k_1-1} \cdot A_{k_2-1} \cdot \ldots \cdot A_{k_m-1} + z) \cdot (A_{k_1-1} \cdot A_{k_2-1} \cdot \ldots \cdot A_{k_m-1} - z) \equiv 0 \pmod{N}.$$

Sljedeći korak je primjena Euklidovog algoritma na brojeve $(A_{k_1-1} \cdot A_{k_2-1} \cdot \ldots \cdot A_{k_m-1} + z, N)$ te $(A_{k_1-1} \cdot A_{k_2-1} \cdot \ldots \cdot A_{k_m-1} - z, N)$. Ako dobijemo barem jedan broj koji je različit od N ili 1, imamo jedan faktor od N i gotovi smo. Ukoliko nismo dobili nijedan faktor, tražimo neku drugu kombinaciju brojeva t_i te ponavljamo postupak. Zbog periodičnosti razvoja broja $\sqrt{N}$ u verižni razlomak, u nekom trenutku će se brojevi Q_i, odnosno t_i početi ponavljati.

Pokažimo sada na jednostavnom primjeru opisanu metodu faktorizacije:

Primjer 2.1.4. *Želimo faktorizirati broj 16463. Razvoj broja* $\sqrt{16463}$ *u verižni razlomak dobiven postupkom kao u (1.14) je*

$$\sqrt{16463} = [128; \overline{3, 4, 10, 1, 12, 1, 1, 2, 7, 1, 7, 2, 1, 1, 12, 1, 10, 4, 3, 256}].$$

Brojnici konvergenti razvoja tog broja u verižni razlomak A_i te brojevi Q_i koji su nam potrebni, prikazani su u sljedećoj tablici:

i	P_i	Q_i	a_i	$A_i \pmod N$
0	0	1	128	128
1	128	79	3	385
2	109	58	4	1668
3	123	23	10	602
4	107	218	1	2270
5	111	19	12	11379
6	117	146	1	13649
7	29	107	1	**8565**
8	78	**97**	2	14316
9	116	31	7	9999
10	101	202	1	7852
11	101	31	7	**15574**
12	116	**97**	2	6074

Tablica 2.1: Koeficijenti iz razvoja broja $\sqrt{16463}$ u verižni razlomak

Iz trećeg stupca tablice vidljivo je da je umnožak

$$(-1)^8 Q_8 \cdot (-1)^{12} Q_{12} = 97 \cdot 97 = 97^2$$

potpun kvadrat. Uzimajući sada A_7 i A_{11}, dobivamo kongruenciju kao u (2.2):

$$8565^2 \cdot 15574^2 = 97^2.$$

Tada je

$$(8565 \cdot 15574)^2 = 133391310^2 \equiv 8084^2 \equiv 97^2 \pmod{16463}.$$

Sada računamo najveći zajednički djelitelj brojeva $8084 + 97$ *i* 16463 *te brojeva* $8084 - 97$ *i* 16463 *pomoću Euklidovog algoritma, čime dobivamo brojeve* 101 *i* 163. *To su upravo faktori broja kojeg želimo faktorizirati. Dakle,* $16463 = 101 \cdot 163$.

2.2 Poboljšanje korištenjem faktorske baze

U prethodnom primjeru prikazana je faktorizacija relativno malog broja te je bilo jednostavno pronaći kombinaciju brojeva $t_i = (-1)^i Q_i$ koji daju potpuni kvadrat. No ako je broj koji želimo faktorizirati puno veći, tada je teže pronaći takvu kombinaciju. Zbog toga je potrebno koristiti faktorsku bazu za faktorizaciju brojeva t_i, kako bi se olakšalo nalaženje potpunog kvadrata.

Definicija 2.2.1. *Faktorska baza je skup $\mathcal{B} = \{p_1, p_2, \ldots, p_m\}$ različitih prostih brojeva, s time da može biti $p_1 = -1$.*

Faktorsku bazu sastavljamo od prostih brojeva koji su manji od neke odabrane granice p_m te od broja -1. Ne stavljamo svaki prost broj u faktorsku bazu, već za svaki neparan prost broj manji od p_m računamo vrijednost *Legendreovog simbola* $\left(\frac{N}{p_i}\right)$.

Definicija 2.2.2. *Neka je p neparan prost broj. Legendreov simbol $\left(\frac{a}{p}\right)$ je jednak 1 ako je a kvadratni ostatak modulo p, -1 ako je a kvadratni neostatak, a 0 ako p|a.*

Propozicija 2.2.3 (Eulerov kriterij za Legendreov simbol)**.** *Ako je p neparan prost broj, a n cijeli broj, tada vrijedi*

$$n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \pmod{p}.$$

Izračunajmo sada vrijednost Legendreovog simbola $\left(\frac{N}{p_i}\right)$ za proste brojeve p_i koji su u faktorskoj bazi. Prema teoremu 2.1.2 vrijedi

$$A_{n-1}^2 - NB_{n-1}^2 = (-1)^n Q_n.$$

Ako je p_i u faktorskoj bazi tada p_i dijeli neki Q_n pa slijedi

$$A_{n-1}^2 - NB_{n-1}^2 \equiv 0 \pmod{p_i},$$

odnosno

$$N \equiv \left(\frac{A_{n-1}}{B_{n-1}}\right)^2 \pmod{p_i}.$$

To znači da je N kvadratni ostatak modulo p_i pa je zbog toga za svaki p_i iz faktorske baze, Legendreov simbol $\left(\frac{N}{p_i}\right) = 1$. Slučaj kada je $\left(\frac{N}{p_i}\right) = 0$ je slučaj kada $p_i|N$ i njega možemo odmah provjeriti i isključiti. U faktorsku bazu moramo uključiti i broj -1 zbog negativnog predznaka broja $t_i = (-1)^n Q_n$ kada je n neparan te broj 2 koji je prost, ali paran. Dakle, faktorska baza će se sastojati od brojeva -1, 2 te svih prostih brojeva manjih od p_m za koje je $\left(\frac{N}{p_i}\right) = 1$

Nakon odabira faktorske baze, brojevi t_i se pokušavaju faktorizirati koristeći proste brojeve iz te faktorske baze. Ukoliko se neki t_i ne može u potpunosti faktorizirati, on se odbacuje. No, kako se ne bi odbacili korisni brojevi t_i, zadržavaju se oni koji, osim faktora iz baze, imaju jedan veliki prosti faktor koji je veći od postavljene granice p_m, ali manji od p_m^2. Ako se nađu dva takva broja s istim velikim prostim faktorom, moguće je da će njihov produkt biti potpun kvadrat.

Ako faktorska baza ima m elemenata, nakon što je uspješno faktorizirano $m+1$ brojeva t_i, gledamo vektore parnosti eksponenata u svakoj faktorizaciji. Vektor parnosti za pojedini

t_i dobivamo tako da pogledamo s kojim eksponentom se pojavljuje pojedini broj iz faktorske baze u faktorizaciji. Za parne eksponente pišemo broj 0, a za neparne broj 1. Na taj način je odmah vidljivo postoji li neki potpuni kvadrat jer će svi eksponenti biti parni, a pripadni vektor parnosti će biti nul-vektor.

Nakon što je faktorizirano $m + 1$ brojeva t_i, imamo matricu koja nije regularna pa se Gaussovom eliminacijom modulo 2 na toj matrici može pronaći nul-redak. Kada dobijemo nul-vektor na ovakav način, kombiniramo pripadne brojeve t_i kako bismo dobili potpun kvadrat te ranije opisanim postupkom provjeravamo daje li on netrivijalnu faktorizaciju od N. Ne dobijemo li faktore od N, odbacujemo redak u kojem je potpun kvadrat jer nam on ne daje faktore te tražimo neku drugu kombinaciju. Ako su isprobane sve moguće kombinacije i faktori nisu pronađeni, vraćamo se na početak i faktoriziramo još više brojeva t_i te ponavljamo postupak.

2.3 CFRAC na primjeru

Sada ćemo prikazati CFRAC metodu faktorizacije na primjeru. Uzmimo $N = 12378523$. Odabiremo faktorsku bazu $\mathcal{B} = \{-1, 2, 3, 11, 13\}$ tako da izračunamo vrijednosti Legendreovog simbola za sve $p \leq p_m = 13$. Zapravo su u bazu uključeni svi kvadratni ostaci modulo N koji su manji ili jednaki 13, s time da za gornju granicu prostih faktora uzimamo broj 79. Računajući razvoj broja $\sqrt{12378523}$ u verižni razlomak, dobivamo brojeve Q_i koji su nam potrebni. Uzimamo samo one Q_i koji se mogu u potpunosti faktorizirati pomoću faktorske baze i svi faktori su im manji od 79. Faktorizirani brojevi Q_i s pripadnim vektorima parnosti eksponenata prikazani su u tablici:

i	$(-1)^i Q_i$	-1	2	3	11	13	79	41	59	37
3	$-3 \cdot 13$	1	0	1	0	1				
6	$3^3 \cdot 79$	0	0	1	0	0	1			
7	$-2 \cdot 3^2 \cdot 41$	1	1	0	0	0	0	1		
8	$3^2 \cdot 13^2$	0	0	0	0	0	0	0		

Tablica 2.2: Faktorizacija brojeva Q_i u faktorskoj bazi

U retku $i = 8$ u tablici imamo nul-redak što znači da je

$$(-1)^8 Q_8 = (3 \cdot 13)^2$$

potpun kvadrat. Provjeravamo daje li taj broj neki faktor od N tako da odredimo rješenje kongruencije

$$A_7^2 \equiv (-1)^8 Q_8.$$

Dobivamo $12378484^2 \equiv 39^2 \pmod{N}$. Sada računanjem najvećeg zajedničkog djelitelja brojeva 12378484 − 39 i N dobivamo broj 1 što znači da nismo uspjeli faktorizirati N. Budući da redak $i = 8$ ne pomaže u faktorizaciji broja N, odbacujemo ga te dalje računamo razvoj u verižni razlomak.

i	$(-1)^i Q_i$	-1	2	3	11	13	79	41	59	37
11	$-3^2 \cdot 59$	1	0	0	0	0	0	0	1	
13	$-2 \cdot 3^2 \cdot 11^2$	1	1	0	0	0	0	0	0	
16	$2 \cdot 3 \cdot 13 \cdot 41$	0	1	1	0	1	0	1	0	
22	$3 \cdot 13 \cdot 59$	0	0	1	0	1	0	0	1	
25	$-3 \cdot 37^2$	1	0	1	0	0	0	0	0	0
32	$11^2 \cdot 41$	0	0	0	0	0	0	1	0	0
43	$-3 \cdot 13 \cdot 41$	1	0	1	0	1	0	1	0	0

Tablica 2.3: Faktorizacija brojeva Q_i u faktorskoj bazi (nastavak)

Trenutno u tablici imamo 10 redaka, s time da ne računamo redak $i = 8$ jer smo ga odbacili, a u skupu svih faktora koji se pojavljuju u faktorizacijama ima 9 elemenata. To znači da postoji mogućnost nalaženja potpunog kvadrata. Gaussovim eliminacijama, odnosno postupnim zbrajanjem redaka modulo 2 pokušavamo naći kombinaciju koja daje potpuni kvadrat. Neke kombinacije koje daju potpuni kvadrat te odgovarajuće kongruencije su

$$\begin{aligned} Q_3 Q_7 Q_{16} &\equiv A_2^2 A_6^2 A_{15}^2 \pmod{N}, \\ Q_3 Q_{11} Q_{22} &\equiv A_2^2 A_{10}^2 A_{21}^2 \pmod{N}, \\ Q_7 Q_{13} Q_{32} &\equiv A_6^2 A_{12}^2 A_{31}^2 \pmod{N}, \\ Q_7 Q_{11} Q_{16} Q_{22} &\equiv A_6^2 A_{10}^2 A_{15}^2 A_{21}^2 \pmod{N}. \end{aligned}$$

Računanjem dolazimo do zaključka da nijedna od tih kombinacija ne daje netrivijalne faktore od N. Zbog toga nastavljamo tražiti nul-redak te dolazimo do kombinacije

$$Q_3 Q_{32} Q_{43} = (3^2 \cdot 11^2 \cdot 13^2 \cdot 41^2) = 17589^2.$$

Imamo kongruenciju

$$\begin{aligned} A_2^2 A_{31}^2 A_{42}^2 &\equiv 17589^2 \pmod{N}, \\ (56293 \cdot 1351545 \cdot 9955325)^2 &\equiv 17589^2 \pmod{N}, \\ 12342301^2 &\equiv 17589^2 \pmod{N}, \\ 12342301^2 - 17589^2 &\equiv 0 \pmod{N}. \end{aligned}$$

Računanjem najvećeg zajedničkog djelitelja brojeva 12342301 − 17589 i $N = 12378523$ dobivamo broj 1993 koji je jedan faktor od N. Drugi faktor možemo dobiti kao najveći zajednički djelitelj brojeva 12342301 + 17589 i $N = 12378523$ i on je jednak 6211. Time smo dobili faktorizaciju od N:

$$12378523 = 1993 \cdot 6211.$$

Kao što smo vidjeli, nalaženje potpunog kvadrata među brojevima Q_i ne znači uvijek da ćemo dobiti faktore od N. Moguće je da će najveći zajednički djelitelj ispasti broj 1 ili N. Tada trebamo tražiti neki drugi potpuni kvadrat ili, ako ga nema, vratiti se na početak i izračunati još više brojeva Q_i.

2.4 Još neki detalji

Često se kod CFRAC metode koristi razvoj u verižni razlomak broja $\sqrt{kN}$ umjesto $\sqrt{N}$, za neki cijeli broj k koji nije potpun kvadrat. Faktor k se koristi u slučaju da verižni razlomak za $\sqrt{N}$ nema dovoljno dugi period pa se brojevi Q_i počinju ponavljati prije nego što smo pronašli potpuni kvadrat. Pritom se u računu i dalje provode operacije modulo N, a ne modulo kN.

Još jedan razlog zbog kojeg se koristi k je taj što njegova vrijednost utječe na proste brojeve koji će biti u faktorskoj bazi. Ako razvijamo broj $\sqrt{kN}$ u verižni razlomak, tada prema teoremu 2.1.2 imamo

$$A_{n-1}^2 - kNB_{n-1}^2 = (-1)^n Q_n.$$

Ako pretpostavimo da je broj p iz faktorske baze i dijeli Q_n tada je

$$kN \equiv \left(\frac{A_{n-1}}{B_{n-1}}\right)^2 \pmod{p}.$$

To znači da je kN kvadratni ostatak modulo p pa se faktorska baza sastoji od prostih brojeva p za koje je Legendreov simbol $\left(\frac{kN}{p}\right) = 1$. Također u faktorskoj bazi su i prosti faktori od k i broj 2. Prema tome, korištenjem faktora k imamo djelomičnu kontrolu nad faktorskom bazom. Prikladnim odabirom k moguće je da će u njoj biti manji prosti brojevi nego inače.

U primjeru faktorizacije koji smo ranije prikazali, brojeve Q_i faktorizirali smo dijeljenjem prostim faktorima iz faktorske baze. To nije bio problem zbog toga što je u bazi bilo 5 brojeva. No, u situacijama kada faktoriziramo velike brojeve (od npr. 60 znamenaka) i faktorska baza je puno veća. Tada nije praktično svaki Q_i dijeliti svakim faktorom iz baze. Zbog toga postoji strategija ranog zaustavljanja koja nam govori kada trebamo odbaciti neki Q_i i prijeći na sljedeći. Ako Q_i nema malih faktora, moguće je da se uopće neće

faktorizirati unutar faktorske baze pa ga možemo odbaciti nakon što dostignemo neku postavljenu granicu na faktore u bazi. Drugi slučaj je da Q_i ima malih faktora, ali preostali dio se ne može faktorizirati pomoću baze. Strategija ranog zaustavljanja daje teoretske granice te preporuku kada odbaciti neki Q_i i prijeći na Q_{i+1}, zbog čega je korisna za ubrzavanje faktorizacije.

Brillhart i Morrison su 1970. godine pomoću CFRAC metode faktorizirali Fermatov broj

$$F_7 = 2^{2^7} + 1 = 59649589127497217 \cdot 5704689200685129054721.$$

Računali su razvoj broja $\sqrt{257F_7}$ u verižni razlomak, pri čemu su izračunali 1330000 brojeva Q_n.

Poglavlje 3

Testiranje prostosti pomoću verižnih razlomaka

Ovdje ćemo se baviti testiranjem prostosti prirodnih brojeva. Opisat ćemo test prostosti pomoću verižnog razlomka te ćemo testirati prostost Mersennovih brojeva.

3.1 O testiranju prostosti

U prethodnom poglavlju bavili smo se faktorizacijom velikih prirodnih brojeva. Broj smo rastavili na faktore koji su bili prosti brojevi. Kako bismo bili sigurni da je neki broj prost, on mora proći neki test prostosti. Jedan jednostavan test prostosti uključuje dijeljenje broja n svim prostim brojevima manjim od $\sqrt{n}$. Ako nijedan prosti broj ne dijeli n, tada je n prost. Postoje brojevi koji prolaze određene testove prostosti, a nisu prosti, već složeni. Mi ćemo se baviti testom prostosti koji uključuje verižne razlomke. Pritom će nam biti potrebne konvergente verižnog razlomka dobivenog razvojem broja $\sqrt{3}$. Da bismo opisali taj test prostosti, najprije ćemo navesti neke tvrdnje i postupke iz teorije brojeva o testiranju prostosti.

Definicija 3.1.1. *Neka je $\varphi(n)$ broj svih prirodnih brojeva koji su manji ili jednaki n te su relativno prosti s n. Funkciju φ zovemo Eulerova funkcija.*

Kada je n prost broj, tada su svi brojevi $1, 2, \ldots, n-1$ relativno prosti s n. Jasno je da je u tom slučaju $\varphi(n) = n - 1$. U sljedećem teoremu iskazano je jedno svojstvo Eulerove funkcije za prirodan broj n.

Teorem 3.1.2. *Neka je* $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$, *tada je*

$$\begin{aligned}\varphi(n) &= p_1^{a_1-1}(p_1-1)\dots p_r^{a_r-1}(p_r-1)\\ &= n\cdot(1-\frac{1}{p_1})\cdot\ldots\cdot(1-\frac{1}{p_r}).\end{aligned}$$

Za testiranje prostosti važan je sljedeći teorem.

Teorem 3.1.3 (Mali Fermatov teorem)**.** *Neka je p prost broj. Ako* $p \nmid b$, *onda je*

$$b^{p-1} \equiv 1 \pmod{p}.$$

Definicija 3.1.4. *Neka je n neparan složen broj koji je relativno prost s b. Ako je*

$$b^{n-1} \equiv 1 \pmod{n},$$

tada kažemo da je n pseudoprost u bazi b.

Pomoću Fermatovog teorema možemo testirati je li neki prirodni broj n prost tako da provjerimo zadovoljava li taj broj gornju kongruenciju za sve baze s kojima je relativno prost. Ako u nekoj bazi n nije pseudoprost, tada je složen. No, postoje složeni brojevi koji su pseudoprosti u svim bazama pa se na ovaj način ne može uvijek odrediti je li broj prost ili ne. Takvi složeni brojevi zovu se *Carmichaelovi brojevi*.

Definicija 3.1.5. *Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je* $a^d \equiv 1 \pmod{n}$ *zove se red od a modulo n.*

Teorem 3.1.6. *Neka je d red od a modulo n. Tada za prirodan broj k vrijedi* $a^k \equiv 1 \pmod{n}$ *ako i samo ako* $d|k$. *Posebno,* $d|\varphi(n)$.

Definicija 3.1.7. *Ako je red od a modulo n jednak* $\varphi(n)$, *onda se a zove primitivni korijen modulo n.*

Opišimo sada jedan test prostosti koji je sličan testu s verižnim razlomcima te će nam kasnije biti potreban za njegovo bolje razumijevanje. Neka je n broj za kojeg želimo provjeriti je li prost te neka je b prirodan broj manji od n za koji je n pseudoprost:

$$b^{n-1} \equiv 1 \pmod{n}.$$

Poznat nam je red od b modulo n te prema teoremu 3.1.6, on dijeli $\varphi(n)$. Želimo provjeriti je li taj red jednak $n-1$ jer bi to značilo da je i $\varphi(n) = n-1$ pa je tada n prost broj. Ako n nije prost, tada je red od b najviše $\varphi(n)$ što je u tom slučaju strogo manje od $n-1$.

Pretpostavimo da nam je poznata faktorizacija broja $n-1$ i brojevi $p_1, p_2, \ldots, p_r$ su različiti prosti faktori koji dijele $n-1$. Tada za svaki $p_i,\ i = 1, \ldots, r$ provjeravamo vrijedi li:

$$b^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n}.$$

Ako vrijedi, tada je red od b modulo n jednak $n-1$ što znači da je n prost broj i da je b primitivni korijen modulo n. Ako je u nekom slučaju potencija od b kongruentna 1, onda je red od b jednak $\frac{n-1}{p_i}$ i dijeli $\varphi(n)$. To znači da je n složen broj ili b nije primitivni korijen modulo n. Ako smatramo da je n ipak prost, možemo ponoviti test za druge brojeve b dok ne pogodimo neki primitivni korijen.

3.2 Test prostosti pomoću verižnog razlomka

Kod ovog testa prostosti bit će nam potreban razvoj broja $\sqrt{3}$ u verižni razlomak te njegove konvergente. U tablici je prikazano nekoliko brojnika i nazivnika konvergenti:

i	A_i	B_i
1	1	1
2	2	1
3	5	3
4	7	4
5	19	11
6	26	15
7	71	41
8	97	56
9	265	153
10	362	209
11	989	571
12	1351	780
13	3691	2131
14	5042	2911
15	13775	7953
16	18817	10864
17	51409	29681
18	70226	40545

Tablica 3.1: Konvergente $\frac{A_i}{B_i}$ verižnog razlomka broja $\sqrt{3}$

Promatrajući nazivnike konvergenti (B_i), možemo uočiti da je svaki treći, počevši od $i = 3$, djeljiv s 3 te je svaki četvrti djeljiv s 4. No, ako gledamo djeljivost s brojem 5 vidimo

da je svaki šesti B_i djeljiv s 5, a prvi koji je djeljiv s 5 je B_6. Zanimljivo nam je promatrati najmanji B_i kojeg dijeli neki prost broj pa ćemo prema tome definirati rang tog broja.

Definicija 3.2.1. *Neka je p neparan prost broj te neka su B_i nazivnici konvergenti verižnog razlomka koji je dobiven razvojem broja $\sqrt{3}$. Najmanji prirodni broj e takav da p dijeli B_e zove se rang od p.*

Primjer 3.2.2. *Promatrajući tablicu 3.1 vidimo da je rang broja 3 jednak 3 jer najmanji B_i kojeg dijeli broj 3 je B_3. Isto tako, najmanji B_i kojeg dijeli broj 5 je B_6 pa je njegov rang 6. Rang od 7 je 8, rang od 11 je 5, itd.*

Primijetimo da je definicija ranga slična definiciji reda. Sada ćemo navesti dvije leme koje će nam biti potrebne pri dokazivanju nekih teorema u ovom poglavlju.

Lema 3.2.3. *Neka su A_m i B_m brojnici i nazivnici konvergenti verižnog razlomka dobivenog razvojem broja $\sqrt{3}$. Tada vrijedi*

$$2^{\lfloor m/2 \rfloor} \cdot (A_m + B_m \cdot \sqrt{3}) = (1 + \sqrt{3})^m.$$

Lema 3.2.4. *Neka je:*

$$t_i = 2^{\lfloor i/2 \rfloor} \cdot A_i,$$
$$u_i = 2^{\lfloor i/2 \rfloor} \cdot B_i,$$

tada je

$$t_{i+j} = t_i t_j + 3u_i u_j, \tag{3.1}$$
$$u_{i+j} = u_i t_j + u_j t_i. \tag{3.2}$$

i ako je $i \geq j$, onda je

$$(-2)^j \cdot u_{i-j} = u_i t_j - u_j t_i, \tag{3.3}$$
$$(-2)^j \cdot t_{i-j} = t_i t_j - 3u_i u_j. \tag{3.4}$$

Teorem 3.2.5. *Neka su B_i nazivnici konvergenti verižnog razlomka broja $\sqrt{3}$. Neka je m prirodni broj veći od 1 i neka je e njegov rang. Tada m dijeli B_i ako i samo ako e dijeli i.*

Skica dokaza. Neka je e rang od m i neka m dijeli neki B_i. Tada trebamo pokazati da e dijeli i. Ako zapišemo i u obliku:

$$i = q \cdot e + r, \quad 0 \leq r < e,$$

trebamo pokazati da je $r = 0$. Ako je r različit od 0 tada iz izraza (3.3) slijedi da je $(-2)^r \cdot u_{i-r} = u_i t_r - u_r t_i$ te da m i t_i nisu relativno prosti. Tada za $i = j$ iz jednakosti (3.4) dobivamo da je $(-2)^i = t_i^2 - 3u_i^2$, pri čemu je m relativno prost s lijevom stranom jednakosti, a nije s desnom stranom. Zbog toga r mora biti 0. □

Ovaj teorem zapravo potvrđuje da ako m ima rang e, tada m dijeli B_e, B_{2e}, B_{3e}, B_{4e} i svaki sljedeći B_k takav da je k višekratnik od e.

Pri testiranju prostosti broja n u prethodnom odjeljku tražili smo element b koji ima red $n-1$ modulo n. Ako takav element postoji, tada je n prost. Sličnu metodu ćemo koristiti i u ovom testu, no umjesto reda koristit ćemo rang. Prisjetimo se da ako je p prost broj veći od 3, tada red od p dijeli $\varphi(p) = p-1$. No, u ovom slučaju rang od p ne dijeli uvijek $p-1$. Možemo provjeriti u tablici 3.1 da ponekad rang od p dijeli i p (za $p = 3$, $p = 4$) i $p+1$ (za $p = 5$, $p = 7$). To nam potvrđuje sljedeći teorem.

Teorem 3.2.6. *Neka je p neparan prost broj. Rang od p dijeli $p - \left(\frac{3}{p}\right)$, gdje je $\left(\frac{3}{p}\right)$ Legendreov simbol.*

Dokaz. Uz oznake iz leme 3.2.4 i prema lemi 3.2.3 imamo:

$$\begin{aligned} t_p + u_p\sqrt{3} &= (1+\sqrt{3})^p \\ &= 1 + p\sqrt{3} + \frac{p(p-1)}{1\cdot 2}\cdot 3 + \ldots + p\cdot 3^{\frac{p-1}{2}} + 3^{\frac{p}{2}} \\ &\equiv 1 + 3^{\frac{p-1}{2}}\cdot\sqrt{3} \pmod{p}. \end{aligned}$$

Izjednačavanjem koeficijenata dobivamo da je

$$\begin{aligned} t_p &\equiv 1 \pmod{p} \\ u_p &\equiv 3^{\frac{p-1}{2}} \equiv \left(\frac{3}{p}\right) \pmod{p}. \end{aligned} \tag{3.5}$$

Druga kongruencija slijedi iz Eulerovog kriterija za Legendreov simbol (2.2.3). Nadalje koristimo jednadžbe (3.2) i (3.3) te činjenicu da je $t_1 = u_1 = 1$. Dobivamo:

$$\begin{aligned} u_{p+1} = u_p t_1 + u_1 t_p &\equiv \left(\frac{3}{p}\right) + 1 \pmod{p}, \\ -2u_{p-1} = u_p t_1 - u_1 t_p &\equiv \left(\frac{3}{p}\right) - 1 \pmod{p}. \end{aligned}$$

Vidimo da ako je $\left(\frac{3}{p}\right) = 1$, onda p dijeli u_{p-1}, odnosno B_{p-1}. Ako je $\left(\frac{3}{p}\right) = -1$, onda p dijeli u_{p+1}, odnosno B_{p+1}. Ako je $p = 3$, tada p dijeli B_p. Dakle, rang od p dijeli $p-1$ ili $p+1$ ili p.

□

Sada ćemo definirati funkciju ψ koja je analogon Eulerove funkcije.

Definicija 3.2.7. *Neka je n neparni prirodni broj čija je faktorizacija*

$$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}.$$

Funkciju $\psi(n)$ definiramo kao:

$$\psi(n) = 2^{1-r} \cdot \left(p_1 - \left(\frac{3}{p_1}\right)\right) \cdot p_1^{a_1-1} \cdot \ldots \cdot \left(p_r - \left(\frac{3}{p_r}\right)\right) \cdot p_r^{a_r-1}.$$

Teorem 3.2.8. *Neka je n neparni prirodni broj koji nije djeljiv s* 3. *Tada rang od n dijeli $\psi(n)$.*

Skica dokaza. Najprije pokazujemo da ako je n potencija neparnog broja, tada rang od n dijeli $\psi(n)$. Odnosno, pokazujemo da n dijeli $B_{\psi(n)}$. Pritom koristimo lemu 3.2.3 i matematičkom indukcijom pokazujemo da ako p^i dijeli B_m, tada p^{i+1} dijeli B_{pm}. Nadalje, neka su m i n relativno prosti neparni brojevi koji nisu djeljivi s 3 te neka su $i = \psi(m)$ i $j = \psi(n)$. Pokazujemo da tada mn dijeli $B_{\frac{ij}{2}}$. Koristeći te tvrdnje, teorem slijedi iz indukcije po r, broju svih različitih prostih faktora od n. □

U sljedećem teoremu se govori o Jacobijevom simbolu zbog toga što n nije nužno prost broj. Jacobijev simbol je zapravo umnožak Legendreovih simbola kod kojih su donji brojevi prosti faktori od n.

Teorem 3.2.9. *Neka je n neparni prirodni broj koji nije djeljiv s 3 i neka je $\left(\frac{3}{n}\right)$ Jacobijev simbol. Ako je rang od n jednak $n - \left(\frac{3}{n}\right)$, tada je n prost.*

Dokaz. Pretpostavimo da je n složen broj. Najprije promatramo slučaj kada je n potencija prostog broja, neka je $n = p^i$, $i > 1$. Ako je rang od n jednak $n \pm 1$, tada je rang relativno prost s p. Prema teoremu 3.2.8, rang od n dijeli

$$\psi(n) = p - \left(\frac{3}{p}\right) \cdot p^{i-1}.$$

Kako je rang relativno prost s p, on ne dijeli p^{i-1} pa mora dijeliti $p - \left(\frac{3}{p}\right)$. No, prema pretpostavci je rang barem $n - 1$, odnosno barem $p^i - 1$, što je strogo veće od $p - \left(\frac{3}{p}\right)$ pa rang od n ne dijeli $\psi(n)$. Dakle, ako je n složen, tada njegov rang nije $n \pm 1$. Neka je sada n djeljiv sa barem dva različita prosta broja, na primjer

$$n = p_1^{a_1} \dots p_r^{a_r},$$

tada je

$$\begin{aligned}
\psi(n) &= 2^{1-r} \cdot \left(p_1 - \left(\frac{3}{p_1}\right)\right) \cdot p_1^{a_1-1} \cdot \ldots \cdot \left(p_r - \left(\frac{3}{p_r}\right)\right) \cdot p_r^{a_r-1} \\
&= 2 \cdot \frac{1}{2^r} \cdot \left(1 - \frac{\left(\frac{3}{p_1}\right)}{p_1}\right) p_1^{a_1} \cdot \ldots \cdot \left(1 - \frac{\left(\frac{3}{p_r}\right)}{p_r}\right) p_r^{a_r} \\
&= 2 \cdot n \cdot \left(\frac{1}{2} - \frac{\left(\frac{3}{p_1}\right)}{2p_1}\right) \cdot \ldots \cdot \left(\frac{1}{2} - \frac{\left(\frac{3}{p_r}\right)}{2p_r}\right) \\
&\leq 2n \left(\frac{1}{2} + \frac{1}{2p_1}\right) \cdot \ldots \cdot \left(\frac{1}{2} + \frac{1}{2p_r}\right) \\
&= 2n \left(\frac{p_1+1}{2p_1}\right) \cdot \ldots \cdot \left(\frac{p_r+1}{2p_r}\right) \\
&\leq 2n \left(\frac{5+1}{2 \cdot 5}\right) \cdot \left(\frac{7+1}{2 \cdot 7}\right) \\
&= \frac{24}{35} n \\
&< n - 1 \\
&\leq n - \left(\frac{3}{n}\right).
\end{aligned}$$

Vidimo da ako je n složen, tada je $\psi(n) < n - \left(\frac{3}{n}\right)$ pa zbog toga $n - \left(\frac{3}{n}\right)$ ne može dijeliti $\psi(n)$. Prema teoremu 3.2.8 znamo da rang od n mora dijeliti $\psi(n)$ pa zaključujemo da $n - \left(\frac{3}{n}\right)$ nije rang od n ako je on složen broj. Dakle, ako je rang od n jednak $n - \left(\frac{3}{n}\right)$ onda je n prost. □

Ovaj teorem daje nam test prostosti koji je sličan onom iz prethodnog odjeljka. Da bismo provjerili je li neki broj n prost, moramo pronaći faktorizaciju broja $n - \left(\frac{3}{n}\right)$. Tada za svaki prosti faktor p provjeravamo dijeli li n broj $B_{n-\left(\frac{3}{n}\right)}$, a ne dijeli $B_{(n-\left(\frac{3}{n}\right))/p}$. Ako je $B_{n-\left(\frac{3}{n}\right)}$ najmanji nazivnik kojeg dijeli n, onda je rang od n jednak $n - \left(\frac{3}{n}\right)$ pa je prema prethodnom teoremu 3.2.9 broj n prost. Primijetimo da ne vrijedi obrat, odnosno ako je broj n prost, to ne znači da je njegov rang jednak $n - \left(\frac{3}{n}\right)$. Jedino što znamo o njegovom rangu je da dijeli $\psi(n)$. Ukoliko izračunamo da je rang broja n različit od $\psi(n)$, ne možemo odmah zaključiti da je taj broj složen jer može biti i prost.

Primjer 3.2.10. *Gledajući tablicu 3.1, možemo vidjeti da je rang broja* 11 *jednak* 5. *Dakle,* 11 *je prost broj kojem je rang različit od* $\psi(11) = 10$.

Pomoću ovog testa ne možemo uvijek odrediti je li neki broj prost ili ne. U nastavku ćemo vidjeti da je drugačija situacija kod testiranja prostosti Mersennovih brojeva.

3.3 Mersennovi brojevi

Definicija 3.3.1. *Mersennovi brojevi su brojevi oblika* $M_p = 2^p - 1$.

Budući da se u ovom poglavlju bavimo testiranjem prostosti, nećemo promatrati sve Mersennove brojeve jer za neke odmah možemo zaključiti da nisu prosti. Sljedeći teorem govori nam kada Mersennov broj nije prost.

Teorem 3.3.2. *Ako je n složen, tada je i* M_n *složen.*

Dokaz. Neka je $n = a \cdot b, a > 1, b > 1$. Tada je

$$\begin{aligned} M_n &= 2^{a\cdot b} - 1 \\ &= (2^a)^b - 1 \\ &= (2^a - 1) \cdot (1 + 2^a + 2^{2a} + \ldots + 2^{(b-1)a}). \end{aligned}$$

Budući da je u ovom slučaju broj M_n umnožak dvaju brojeva koji su veći od 1, broj M_n je složen. □

Prvih nekoliko Mersennovih brojeva koji su prosti su: $M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127$. No, već je za prost broj $p = 11$, broj $M_{11} = 2047 = 23 \cdot 89$ složen.

Kod testa prostosti pomoću verižnih razlomaka, koji je ranije opisan, treba pronaći faktorizaciju broja $n - \left(\frac{3}{n}\right)$. O vrijednosti Jacobijevog simbola $\left(\frac{3}{n}\right)$ ovisi koji treba biti rang od n da bismo znali je li on prost. Pokazat ćemo da je kod Mersennovih brojeva taj Jacobijev simbol uvijek jednak -1, što znači da ako je rang Mersennovog broja M_n jednak $M_n + 1$, onda je on prost. Da bismo to pokazali, koristit ćemo neka pravila za računanje Jacobijevog simbola:

Propozicija 3.3.3. *Neka je m neparan pozitivan broj. Za Jacobijev simbol* $\left(\frac{n}{m}\right)$ *vrijedi:*

1. $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$,

2. $\left(\frac{-1}{m}\right) = \begin{cases} 1 & za\ m \equiv 1 \pmod 4 \\ -1 & za\ m \equiv -1 \pmod 4, \end{cases}$

3. $\left(\frac{2}{m}\right) = \begin{cases} 1 & za\ m \equiv 1\ ili\ m \equiv -1 \pmod 8 \\ -1 & za\ m \equiv 3\ i\ m \equiv -3 \pmod 8, \end{cases}$

4. $\left(\frac{n}{m}\right) = \begin{cases} \left(\frac{m}{n}\right) & za\ m \equiv 1\ ili\ n \equiv 1 \pmod 4 \\ -\left(\frac{m}{n}\right) & za\ m \equiv 3\ i\ n \equiv 3 \pmod 4. \end{cases}$

Svi Mersennovi brojevi M_p, kod kojih je p paran broj veći od 2, su složeni. Zbog toga nema smisla testirati njihovu prostost pa ćemo promatrati samo one brojeve $2^p - 1$ kod kojih je p neparan broj veći od 3. Računamo vrijednost Jacobijevog simbola $\left(\frac{3}{2^p-1}\right)$. Broj 3 je očito kongruentan 3 modulo 4. Ako je p neparan broj veći od 3, zapišimo ga u obliku $p = 2k + 1$, $k > 1$. Tada imamo

$$M_{2k+1} = 2^{2k+1} - 1 = 2^{2k} \cdot 2 - 1 = 4^k \cdot 2 - 1 \equiv -1 \equiv 3 \pmod 4.$$

Dakle, oba broja su kongruentna 3 modulo 4 pa prema pravilima iz propozicije 3.3.3 vrijedi $\left(\frac{3}{2^p-1}\right) = -\left(\frac{2^p-1}{3}\right)$. Sada reduciramo Legendreov simbol tako da izračunamo vrijednost $2^p - 1$ modulo 3. Kao i prije, stavimo da je $p = 2k + 1$ pa imamo

$$M_{2k+1} = 2^{2k+1} - 1 = 4^k \cdot 2 - 1 \equiv 1 \cdot 2 - 1 \equiv 1 \pmod 3.$$

Broj 1 je kvadratni ostatak modulo 3 pa dobivamo da je za svaki Mersenov broj $M_p = 2^p - 1$, kod kojeg je p neparan broj veći od 3, vrijednost Jacobijevog simbola:

$$\left(\frac{3}{2^p - 1}\right) = -\left(\frac{2^p - 1}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Prema teoremu 3.2.9, ako je rang Mersennovog broja jednak $M_n - \left(\frac{3}{M_n}\right) = M_n + 1$, tada je taj broj prost. Primijetimo da je u tom slučaju potrebno faktorizirati broj $M_n + 1 = 2^n$ kako bismo provjerili da je rang zaista $M_n + 1$. To je jednostavan zadatak jer su svi faktori jednaki 2. Dakle, da bismo testirali prostost Mersennovog broja M_n, trebamo provjeriti dijeli li on nazivnik B_{M_n+1} verižnog razlomka, a ne dijeli $B_{\frac{M_n+1}{2}}$.

Primjer 3.3.4. *Provjerimo je li broj $M_3 = 7$ prost. Promatrajući tablicu 3.1, vidimo da 7 dijeli $B_8 = 56$, a ne dijeli $B_4 = 4$ pa je njegov rang jednak $M_3 + 1 = 8$. Prema teoremu 3.2.9 zaključujemo da je M_3 prost.*

Za Mersennove brojeve postoji i drugačiji oblik ovog testa prostosti. U nastavku ćemo dokazati teorem pomoću kojeg je moguće brže testirati prostost Mersennovih brojeva.

Teorem 3.3.5. *Neka je $M_n = 2^n - 1$ Mersennov broj kod kojeg je n neparan broj veći ili jednak 3. M_n je prost ako i samo ako M_n dijeli $A_{\frac{M_n+1}{2}} = A_{2^{n-1}}$.*

Dokaz. Pretpostavimo najprije da M_n dijeli $A_{2^{n-1}}$. Treba pokazati da je rang od M_n jednak $M_n - \left(\frac{3}{M_n}\right) = M_n + 1$. Uvrštavanjem $i = j$ u formulu iz leme 3.2.4, imamo $u_{2i} = 2 \cdot t_i \cdot u_i$. Sada za $i = 2^{n-1}$ imamo $u_{2^n} = 2 \cdot t_{2^{n-1}} \cdot u_{2^{n-1}}$. Prema pretpostavci M_n dijeli $t_{2^{n-1}}$ pa mora

dijeliti i lijevu stranu jednakosti, odnosno u_{2^n} što znači da mora dijeliti B_{2^n}. Znamo da su brojevi $A_{2^{n-1}}$ i $B_{2^{n-1}}$ relativno prosti jer su brojnik i nazivnik konvergente verižnog razlomka pa M_n ne može dijeliti oba, što znači da ne dijeli $B_{2^{n-1}}$. Zbog toga je rang od M_n jednak $2^n = M_n + 1$ pa je prema teoremu 3.2.9 broj M_n prost. Još treba pokazati drugi smjer, pretpostavimo sada da je M_n prost. Stavljanjem $i = j$ u jednakosti iz leme 3.2.4 dobivamo:

$$t_{2i} = t_i^2 + 3u_i^2,$$
$$(-2)^i = t_i^2 - 3u_i^2.$$

Zbrajanjem ovih dviju jednakosti dobivamo:

$$t_{2i} + (-2)^i = 2t_i^2. \tag{3.6}$$

U dobivenu jednadžbu uvrstimo $i = 2^{n-1}$:

$$2t_{2^{n-1}}^2 = t_{2^n} + (-2)^{2^{n-1}}.$$

Sada opet koristimo jednakost (3.1) da bismo zapisali t_{2^n} u drugačijem obliku:

$$2t_{2^{n-1}}^2 = t_{M_n} \cdot t_1 + 3u_{M_n} \cdot u_1 - 2 \cdot (-2)^{2^{n-1}-1}.$$

Budući da je $t_1 = A_1 = 1$ i $u_1 = B_1 = 1$, slijedi:

$$2t_{2^{n-1}}^2 = t_{M_n} + 3u_{M_n} - 2 \cdot (-2)^{\frac{M_n-1}{2}}. \tag{3.7}$$

Koristeći izraze za t_{M_n} i u_{M_n} dobivene u (3.5) imamo:

$$2t_{2^{n-1}}^2 \equiv 1 + 3 \cdot 3^{\frac{M_n-1}{2}} - 2 \cdot (-2)^{\frac{M_n-1}{2}} \pmod{M_n},$$

Koristeći pravilo iz propozicije 2.2.3 znamo da je $x^{\frac{M_n-1}{2}} \equiv \left(\frac{x}{M_n}\right) \pmod{M_n}$ pa dobivamo:

$$2t_{2^{n-1}}^2 \equiv 1 + 3 \cdot \left(\frac{3}{M_n}\right) - 2 \cdot \left(\frac{-2}{M_n}\right) \pmod{M_n}.$$

Prije smo ustanovili da je vrijednost Jacobijevog simbola $\left(\frac{3}{M_n}\right)$ jednaka -1. Koristeći pravila za računanje, možemo provjeriti da je i $\left(\frac{-2}{M_n}\right) = -1$. Uvrštavanjem tih vrijednosti u prethodnu kongruenciju dobivamo da je $2t_{2^{n-1}}^2 \equiv 0 \pmod{M_n}$ što znači da M_n dijeli $2t_{2^{n-1}} = 2 \cdot 2^{\lfloor 2^{n-2} \rfloor} \cdot A_{2^{n-1}}$. Zbog toga M_n mora dijeliti $A_{2^{n-1}}$. □

Napomena 3.3.6. *Pokazali smo da ako je M_n prost, tada on dijeli $A_{2^{n-1}}$. Također smo pokazali da ako dijeli $A_{2^{n-1}}$, tada M_n dijeli i B_{2^n}, a ne dijeli $B_{2^{n-1}}$ pa je njegov rang jednak $2^n = M_n + 1$. Dakle, zapravo smo pokazali da je Mersennov broj M_n prost ako i samo ako je njegov rang jednak $M_n + 1$.*

Dokazali smo teorem koji nam govori kada je neki Mersennov broj prost. Budući da vrijede oba smjera u teoremu, test prostosti pomoću verižnih razlomaka uvijek daje rezultat u slučaju testiranja prostosti Mersennovog broja. Svaki prosti Mersennov broj ima rang $M_n + 1$, što nije bilo tako u općenitom slučaju.

Za testiranje prostosti možemo računati brojnike A_i konvergenti verižnog razlomka, ili možemo koristiti bržu varijantu testa. Prikažimo način bržeg provjeravanja prostosti. Pomoću formule (3.6) iz dokaza teorema 3.3.5 možemo lako računati brojeve $A_{2^{n-1}}$ koji su potrebni za testiranje prostosti Mersennovih brojeva. Formula je ekvivalentna:

$$2^i \cdot A_{2i} + (-2)^i = 2 \cdot 2^i \cdot A_i^2,$$

odnosno $A_{2i} = 2A_i^2 - 1$, ako je i paran broj. Ako uzmemo da je $S_t = 2A_{2^t}$, tada je $S_1 = 2A_2 = 4$ pa možemo zapisati formulu u obliku:

$$S_{t+1} = S_t^2 - 2.$$

Teorem 3.3.5 u tom slučaju govori da je M_n prost broj ako i samo ako M_n dijeli S_{n-1}. Dakle, na ovaj način možemo provesti test prostosti bez direktnog određivanja konvergenti verižnog razlomka.

3.4 Test na primjerima

Prikazat ćemo na primjeru test prostosti za Mersennove brojeve $M_7 = 127$ i $M_{11} = 2047$. Neka su A_i brojnici konvergenti verižnog razlomka $\sqrt{3}$. Testirajmo najprije broj M_7. Prema teoremu 3.3.5, da bi M_7 bio prost broj, mora dijeliti $A_{2^6} = A_{64}$. Imamo:

$$A_{64} = 1002978273411373057 = 7897466719774591 \cdot 127.$$

Vidimo da je A_{64} djeljiv brojem $M_7 = 127$ pa zaključujemo da je prost.
Testirajmo sada broj M_{11}. Računamo $A_{2^{10}}$:

$$\begin{aligned} A_{1024} = {} & 343648412033221386194187431158737654621235770543233358760963092915442437028954789823664415345512805217183898319677975860211786532974581723030372823564340391438040276015123291797195087904419554893330929378587077705422474632502375836905842529636890909498769196303047261326826374254509399406018577 \equiv 868 \pmod{2047}. \end{aligned}$$

Iz toga vidimo da A_{1024} nije djeljiv brojem $M_{11} = 2047$ pa možemo zaključiti da je M_{11} složen broj. Budući da provjeravamo djeljivost broja A_{1024} brojem M_{11}, zapravo nije nužno

računati cijeli broj. Dovoljno je u svakom koraku računanja brojeva A_i reducirati trenutni rezultat modulo 2047.

Pokažimo sada na primjeru M_7 brži način testiranja prostosti, koji smo ranije opisali. Računamo brojeve S_i prema formuli

$$S_{i+1} = S_i^2 - 1,$$

s time da je $S_1 = 4$. U tablici su prikazane vrijednosti od S_i za $i \leq n - 1 = 6$.

i	S_i	$S_i \pmod{M_7}$
1	4	4
2	14	14
3	194	67
4	37634	42
5	1416317954	111
6	2005956546822746114	0

Tablica 3.2: Vrijednost brojeva S_i

Budući da je $S_6 \equiv 0 \pmod{M_7}$, broj $M_7 = 127$ je prost. Ni ovdje nije potrebno računati sve brojeve S_i, već samo ostatke modulo M_7. Pri testiranju prostosti na ovaj način nema očite primjene verižnih razlomaka. No brojevi S_i su zapravo povezani s brojnicima konvergenti verižnog razlomka koji je u ovom slučaju dobiven razvojem broja $\sqrt{3}$. Rekurzivna formula koju smo koristili za računanje brojeva S_i je dobivena pomoću različitih svojstava koja vrijede za brojnike i nazivnike konvergenti verižnog razlomka.

Bibliografija

[1] D.M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, 1989.

[2] B. Dakić, *Riječ-dvije o verižnim razlomcima*, MiŠ **53** (2012), 131–136.

[3] A. Dujella, *Uvod u teoriju brojeva (skripta)*, https://web.math.pmf.unizg.hr/ duje/utb/utblink.pdf.

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

[5] C. Pomerance i S.S. Wagstaff, *Implementation of the continued fraction integer factoring algorithm*, Congressus Numerantium **37** (1983), 99–118.

[6] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, 1994.

[7] WolframMathWorld, *Jacobi Symbol*, http://mathworld.wolfram.com/JacobiSymbol.html, (listopad 2017.).

Sažetak

Metoda faktorizacije velikih prirodnih brojeva pomoću verižnih razlomaka (CFRAC) razvijena je 1975. godine te je u to vrijeme bila najbrža metoda faktorizacije. Osnovna ideja ove metode je traženje netrivijalnog rješenja kongruencije $x^2 \equiv y^2 \pmod{N}$. Pomoću njega može se dobiti neki faktor broja N. U ovom radu opisan je način na koji se različiti koeficijenti iz razvoja broja $\sqrt{N}$ u verižni razlomak koriste za dobivanje kongruencije navedenog oblika. Opisana je i primjena verižnih razlomaka pri testiranju prostosti. U tom slučaju bio je korišten razvoj broja $\sqrt{3}$ u verižni razlomak te konvergente tog verižnog razlomka. Proučavanjem nazivnika konvergenti uočene su neke pravilnosti pomoću kojih je dobiven test prostosti. Osim općenitog slučaja, opisan je i način testiranja prostosti Mersennovih brojeva. U radu su navedeni i različiti primjeri faktorizacije i testiranja prostosti pomoću verižnih razlomaka.

Summary

Continued fraction method for factoring large natural numbers was developed in 1975 and it was the fastest factorization method at the time. The basic idea behind this method is finding non-trivial solutions to congruence $x^2 \equiv y^2 \pmod{N}$. After they have been found, there is a chance that a factor of N will be discovered. To produce a congruence of that form, coefficients from a continued fraction expansion of $\sqrt{N}$ are used. The way of calculating them is described in this paper. Another application of continued fractions is in primality testing. In this paper, there is a description of using a continued fraction expansion of $\sqrt{3}$ and the convergents of that fraction. By observing denominators of convergents, certain regularities were found and they were used to describe a primality test. Apart from a general test, a test for Mersenne numbers was also described. In this paper there are various examples of factorization and primality testing with continued fractions.

Životopis

Rođena sam 2. studenog 1993. godine u Čakovcu. Osnovnu školu I.G. Kovačića Sv. Juraj na Bregu završila sam 2008. godine te sam upisala Gimnaziju u Čakovcu, smjer opća gimnazija. Maturirala sam 2012. godine te sam iste godine upisala studij Matematika, nastavnički smjer na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu. Nakon završenog preddiplomskog studija, 2015. godine sam upisala diplomski studij Matematika i informatika, nastavnički smjer, koji trenutno završavam.