Univerzitet u Beogradu
MATEMATIČKI FAKULTET

MASTER RAD

FAKTORIZACIJA POMOĆU VERIŽNIH RAZLOMAKA

Profesor:
Miodrag Živković

Student:
Aleksandra Hubert 1096/2009

SADRŽAJ

1. Uvod

RSA, najpoznatiji i najrasprostranjeni šifarski sistem današnjice zasnovan je na činjenici da je faktorizacija velikog složenog celog broja, vremenski složen i skup proces. S tim u vezi, jedna od prvih, modernijih metoda faktorizacije koja je prethodila metodi sita, bila je metoda faktorizacije pomoću verižnih razlomaka (eng. CFRAC, Continued FRACtion Method). Originalna ideja potiče još od M. Krajčika iz 1920. godine ili čak i ranije od A. M. Ležandra (1752 – 1883), a koju su usavršili Lemer (Lehmer) i Pauers (Powers) 30-ih godina prošlog veka. [3]. Prvu uspešnu računarsku implementaciju algoritma izveli su Brilhart (Brillhart) i Morison (Morrison) 1970. godine [2] i primenili je na faktorizaciju sedmog Fermaovog broja od 38 cifara

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

Ubrzo nakog toga, sve do 80-tih godina prošlog veka, ova metoda koristila se kao glavna metoda u faktorizaciji velikih celih složenih brojeva do 50 cifara.

2. Verižni razlomci

Svakom realnom broju mogu se pridružiti racionalni brojevi koji ga dobro aproksimiraju. Jedna od metoda koja se u tu svrhu koristi je metoda verižnih ralomaka.

Prva upotreba verižnih razlomaka u cilju aproksimacije datira još iz 17. veka kada je danski astronom i fizičar Hajgens (Huygens) pokušao da konstruiše mehanički model sunčevog sistema [4]. Naime, njegov ‘automatski planetarijum’ dizajniran je da opiše kretanja šest najpoznatih planeta oko Sunca, i posebno kretanje Meseca oko Zemlje. Služeći se 1680. godine najrelevantnijim astronomskim podacima koje je mogao dobiti. Koristeći aproksimaciju $365\frac{35}{144}$ za broj dana u jednoj godini, izračunao je odnos perioda planetarnih orbita jedne kalendarske godine, a zatim je svaki od ovih razlomaka razvio u verižni razlomak aproksimirajući dobijene rezultate kovergentom tog razvoja.

Blisko povezan problem aproksimacije prikazan na Hajgensovom modelu bio je i problem konstrukcije kalendara (nakon revolucionarnog otkrića da se Zemlja okreće oko Sunca i rotira oko svoje ose). I u tu svrhu korišćeni su verižni razlomci. Naime, u izradi Julijanskog kalendara jedna godina aproksimirana je sa $365\frac{1}{4}$ dana, odnosno kalendarska godina traje 365 dana pri čemu se svakoj 4. godini dodaje jedan dan radi korekcije, da bi nakon skoro 16 vekova od upotrebe ovog kalendara došlo do odstupanja od 10 dana. U cilju boljeg ujednačavanja, 1582. godine Papa Gregorian XIII uveo je novi kalendar uz aproksimaciju godine od $365\frac{97}{400}$ dana, pri čemu se svake 400-te godine dodaje jedan dan tekućoj godini, tj. prestupnoj godini.

2.1. Osnovna teorija verižnih razlomaka

2.1.1. Definicija. Neka su su $a_i \in \mathbb{Z}$ i $a_i > 0$ za $i > 0$. Verižni razlomak je formalno niz $a_0, a_1, \ldots$ kome odgovara izraz

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ldots}}}} \tag{1}$$

pod kojim se podrazumeva realni niz

$$a_0, a_0 + \frac{1}{a_1}, a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}}, \ldots$$

U nastavku sledi dokaz da je ovaj niz konvergentan, odnosno da svakom verižnom razlomku odgovara jedinstveni realni broj. Broj elemenata (1) može biti konačan ili beskonačan. U slučaju da je broj elemenata konačan, verižni razlomak se zapisuje kao:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \qquad (2)$$

$$+ \frac{1}{a_n}$$

i naziva *konačan* verižni razlomak *n*-tog reda (pri čemu verižni razlomak *n*-tog reda sadrži *n+1* elemenata). U suprotnom zapisuje se kao (1) i naziva *beskonačan* verižni razlomak.

Elementi gore navedenog niza (običnih) razlomaka su *konvergenti* verižnog razlomka (1). Neka je sa $[x_1, x_2, \ldots, x_n]$ označen brojilac n-tog konvergenta verižnog razlomka $x_1; x_2, x_3, \ldots$. Tada je

$$\frac{[x_1, x_2, \ldots, x_n]}{[x_2, \ldots, x_n]} = x_1 + \frac{[x_3, \ldots, x_n]}{[x_2, \ldots, x_n]}$$

tj.

$[x_1, x_2, \ldots, x_n] = x_1[x_2, \ldots, x_n] + [x_3, \ldots, x_n]$ (2)

Ako se prazan verižni razlomak definiše sa [] = 1, ova rekurentna relacija važi i za n > 1, tj.

$[\,] = 1$
$[x_1] = x_1$
$[x_1, x_2] = x_1x_2 + 1$
$[x_1, x_2, x_3] = x_1x_2x_3 + x_1 + x_3$
$[x_1, x_2, x_3, x_4] = x_1x_2x_3x_4 + x_3x_4 + x_2x_3 + x_1x_2 + 1$
$[x_1, x_2, x_3, x_4, x_5] = x_1x_2x_3x_4x_5 + x_3x_4x_5 + x_1x_4x_5 + x_1x_2x_5 + x_1x_2x_3 + x_1 + x_5$

2.2. Ojlerovo pravilo

Tvrđenje 2.2.1. (Ojlerovo pravilo). Neka je n ≥ 1. Neka je za $0 \leq 2k \leq n+1, T_k$ familija svih $(n+1-2k)$ – torki dobijenih tako što su u $n+1$ –orci $(0, 1, \dots, n)$ ispuštene neke grupe od parnog broja uzastopnih brojeva, i neka je

$$S_k = \sum_{I \in T_k} \prod_{i \in I} a_i$$

Tada je

$[a_0, a_1, a_2, \dots, a_n] = \sum_{0 \leq 2k \leq n+1} S_k$

Dokaz. Dokaz se izvodi indukcijom polazeći od izraza

$$[a_0, a_1, a_2, \dots, a_n] = a_0[a_1, a_2, \dots, a_n] + [a_2, a_3, \dots, a_n]$$

□

Posledica 2.2.2. $[a_0, a_1, \dots, a_n] = [a_n, a_{n-1}, \dots, a_0]$

Dokaz. Kako se pri invertovanja redosleda ne menjaju grupe uzastopnih članova, suma iz prethodnog tvrđenja ostaje nepromenjena. □

Preimenujući promenljive u (2) dobija se

$$[a_n, a_{n-1}, \dots, a_0] = a_n[a_{n-1}, \dots, a_0] + [a_{n-2}, \dots, a_0]$$

Primenom prethodne posledice dobija se:
$[a_0, a_1, \dots, a_n] = a_n[a_0, a_1, \dots, a_{n-1}] + [a_0, a_1, \dots, a_{n-2}]$ (3)

Ova relacija pogodnija je za razvoj jer se na desnoj strani ne vrše promene na početku neprekidnog razlomka već na njegovom kraju.

Neka su za verižni razlomak $s(a_0, a_1, \dots, a_n)$ određen nizom $a_0, a_1, \dots, a_n$ sa $s_m = [a_0, a_1, \dots, a_m]$ *i* $t_m = [a_1, a_2, \dots, a_m]$ označeni brojilac i imenilac verižnog razlomka. Rekurenta veza (3), za $m \geq 2$ dobija oblik:

$s_m = a_m s_{m-1} + s_{m-2}$ (4)
$t_m = a_m t_{m-1} + t_{m-2}$

Kako je $s(a_0) = a_0 = \frac{a_0}{1}$, to je $s_0 = a_0$ i $t_0 = 1$. Takođe iz $s(a_0, a_1) = \frac{a_0 a_1 + 1}{a_1}$, sledi $s_1 = a_0 a_1 + 1$ i $t_1 = a_1$. Ove jednakosti, zajedno sa (4) u potpunosti određuju s_k i t_k, za $k \leq n$. Kako je $s(a_0, a_1, \dots, a_n) = \frac{s_n}{t_n}$, na taj način se dobija vrednost verižnog razlomka. Zgodno je staviti da je $s_{-2} = 0$, $s_{-1} = 1$, $t_{-2} = 1$, $t_{-1} = 0$.

Primer 2.2.3. Početak razvoja verižnog razlomka broja $\sqrt{2}$ je

i	-2	-1	0	1	2	3	4	5
a_i			1	2	2	2	2	2
s_i	0	1	1	3	7	17	41	99
t_i	1	0	1	2	5	12	29	70

Primer 2.2.4. Početak razvoja verižnog razlomka broja π

i	-2	-1	0	1	2	3
a_i			3	7	15	1
s_i	0	1	3	22	333	355
t_i	1	0	1	7	106	113

Broj π se može aproksimirati poznatim odnosom $\frac{22}{7}$, a još mnogo bolje odnosom $\frac{355}{113}$, jer je $\frac{355}{113} = 3.1415929$ ..., dok je $\pi = 3.1415926535$ ...

Tvrđenje 2.2.5. Imenilac i brojilac konvergenta s_m/t_m su uzajamno prosti brojevi i važi jednakost

$$s_m t_{m+1} - s_{m+1} t_m = (-1)^{m+1}.$$

Dokaz. Sledi indukcijom po m. Za $m = 1$ imamo $s_1t_0 - s_0t_1 = (a_0a_1) \cdot 1 - a_0a_1 = 1$. Pretpostavimo da je tvrđenje tačno za $m < n$ i dokažimo da važi za $m = n$

Polazeći od $s_{n+1} = a_n s_n + s_{n-1}$ i $t_{n+1} = a_n t_n + t_{n-1}$, dobija se

$$\begin{aligned} s_n t_{n+1} - s_{n+1} t_n &= s_n(a_n t_n + t_{n-1}) - (a_n s_n + s_{n-1}) \\ &= -(s_{n-1} t_n - s_n t_{n-1}) \\ &= (-1) \cdot (-1)^{m-1} \\ &= -1^m. \quad \square \end{aligned}$$

Posledica 2.2.6.

Neka je $\frac{s}{t} = s(a_0, a_1, \dots, a_n)$. Tada se niz $\frac{s_m}{t_m}$, $0 \le m \le n$, alternativno odozdo pa odozgo približava broju $\frac{s}{t}$.

Dokaz. Iz Tvrđenja 2.2.5. dobijamo deljenjem sa $t_m t_{m-1}$,

(6) $\frac{s_m}{t_m} - \frac{s_{m-1}}{t_{m-1}} = (-1)^{m-1} \frac{1}{t_m t_{m-1}}$.

Otuda ta razlika za m neparno pozitivna, a za m parno negativna. Kako prema (4) t_m raste, ta je razlika po apsolutnoj vrednosti sve manja. Otuda je niz sa parnim indeksima rastući, a niz sa neparnim indeksima opadajući. Između njih se kao poslednji (najveći u rastućem podnizu ako je n paran i najmanji u opadajućem ako je n neparan) nalazi razlomak $\frac{s_n}{t_n} = \frac{s}{t}$. $\square$

Lema 2.2.7.

$\left|\frac{s_n}{t_n} - \frac{s_{n+1}}{t_{n+1}}\right| < \frac{1}{t_n^2}$.

Dokaz.

$$\left|\frac{s_n}{t_n} - \frac{s_{n+1}}{t_{n+1}}\right| = \left|\frac{s_n t_{n+1} - t_n s_{n+1}}{t_n t_{n+1}}\right| < \frac{1}{t_n^2}$$

sledi iz Tvrđenja 2.2.5. jer je niz t_m rastući.

2.3. Verižni razlomak realnog broja

Neka je za proizvoljni realni broj x sa $[x]$ označen najveći celi broj manji ili jednak od x. Ako je ε celi broj, tada je $\varepsilon = [\varepsilon]$; u suprotnom može se zapisati:

$\varepsilon = [\varepsilon] + \varepsilon - [\varepsilon] = [\varepsilon] + \frac{1}{\frac{1}{\varepsilon - [\varepsilon]}}$,

Neka je $\varepsilon_1 = \frac{1}{\varepsilon-[\varepsilon]}$. Ukoliko je $\varepsilon_1 = [\varepsilon_1]$, ε je racionalan broj, u suprotnom $\varepsilon_2 = \frac{1}{\varepsilon_1-[\varepsilon_1]}$, i tada je

$$\varepsilon = [\varepsilon] + \frac{1}{[\varepsilon_1]+\frac{1}{\varepsilon_2}}. \quad (7)$$

Nastavljajući na isti način dobija pochetni deo verižnog razlomak realnog broja ε:

$$\varepsilon = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots a_n + \cfrac{1}{\varepsilon_n}}}}$$

Pomoću datog algoritma moguće je odrediti niz relanih brojeva $\varepsilon_{3,}\varepsilon_{4,\dots}$, pri čemu se algoritam zaustavlja ukoliko je $\varepsilon_n = [\varepsilon_n]$ celi broj za neko n.

Algoritam (7) naziva se algoritam razvoja realnog broja u verižni razlomak. Ukoliko je ε iracionalan broj, razvoj u verižni razlomak je beskonačan.

Primer 2.3.2.

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{\varepsilon}}}}}$$

gde je ε iracionalan broj.

Može se pokazati da veirižni ralomak konvergira ka realnom broju ε slično kao u Lemi 2.2.7.

Tvrđenje 2.3.3.

$$\left|\boldsymbol{\varepsilon} - \frac{s_n}{t_n}\right| \leq \frac{\mathbf{1}}{\boldsymbol{t_n^2}}$$

Dokaz. Sledi iz činjenice da je

$$\varepsilon = \frac{\varepsilon_n s_n + s_{n-1}}{\varepsilon_n t_n + t_{n-1}}$$

gde je $\varepsilon_n > 0$. □

2.4. Verižni razlomak racionalnog broja i Euklidov algoritam

Neka je $D(a,b)$ skup zajedničkih delilaca celih brojeva a,b, i neka je (a,b) njihov najveći zajednički delilac.

Lema 2.4.1. Neka su $a,b,q,r \in \mathbb{Z}$

(i) Ako je $a = qb$, tada je $(a,b) = b$
(ii) Ako je $a = qb + r$, tada je $(a,b) = (b,r)$.

Dokaz. (i) Neka je $(a,b) = d$. Kako je $|b| \in D(a,b)$, to $|b| \leq d$. Kako $d \in D(a,b)$, to $d|b$, pa je $|d| \leq |b|$. Dakle, $d = |b|$

(ii) Dokazaćemo da je $\mathrm{D(a,b)} = \mathrm{D(b,r)}$. Neka je $t \in D(a,b)$. Tada $t|a$ i $t|b$, pa $t|a - bq = r$. Dakle $t \in D(r,b)$. Slično, ako je $t \in D(b,r)$, tada $t|b$ i $t|r$. Otuda $t|qb + r$, tj. $t|a$. Dakle $t \in D(a,b)$. Odavde je $\max D(a,b) = \max D(b,r)$, tj $\mathrm{(a,b) = (b,r)}$.

Definicija 2.4.2. Neka su $a,b \in \mathbb{Z}, b \neq 0$. Neka je $r_0 = b$. Niz jednakosti

$a = bq_1 + r_1, 0 < r_1 < |b|$
$b = r_1q_2 + r_2, 0 < r_2 < r_1$
$r_1 = r_2q_3 + r_3, 0 < r_3 < r_2$
…
$r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1}$
$r_{n-1} = r_nq_{n+1}$

naziva se Euklidovim algoritmom dužine *n* za *a* i *b*

Euklidov algoritam omogućuje da se odredi $(a,b) = r_n$.

Primer 2.4.3. Euklidov algoritam za brojeve 93 i 14.

$$93 = 6 \cdot 14 + 9$$
$$14 = 1 \cdot 9 + 5$$
$$9 = 1 \cdot 5 + 4$$
$$5 = 1 \cdot 4 + 1$$
$$4 = 1 \cdot 4$$

Dakle, $(93,14) = 1$

Euklidov algoritam je u vezi sa razvojem racionalnog broja u verižni razlomak. Ukoliko se posmatra razlomak $\frac{a}{b}$, gde je $b > 0$, tada $a = qb + r$ i $\left[\frac{a}{b}\right] = q$ i dalje sledi:

$$\left[\frac{a}{b}\right] = q + \frac{r}{b} = q + \frac{1}{\frac{b}{r}}$$

a zatim se verižni razvoj nastavlja za razlomak $\frac{b}{r}$.

Primer 2.4.4. Razvoj racionalnog broja u verižni razlomak

$$\frac{103993}{33102}$$

$$103993 = 3 \cdot 33102 + 4687$$
$$33102 = 7 \cdot 4687 + 293$$
$$4687 = 15 \cdot 293 + 292$$
$$293 = 1 \cdot 292 + 1$$

$$\frac{103993}{33102} = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292}}}}$$

2.5. Verižni razlomak iracionalnog broja

Kvadratni iracionalan broj α je neracionalni realni koren kvadratne jednačine
$Ax^2 + Bx + C = 0$, (*)
gde su $A, B, C \in \mathbb{Z}$.

Definicija 2.5.1. Ako je α kvadratni iracionalni koren jednačine (*), tada je α' drugi koren iste jednačine. Drugi koren naziva se algebarski konjugat od α.

Tvrđenje 2.5.2. Neka je α kvadratni iracionalni koren jednačine (*) i $q \in \mathbb{Z}$ tada:

i) $\frac{1}{\alpha}$ je kvadratni iracional
ii) $\alpha + q$ je kvadratni iracional
iii) $(\alpha + q)' = \alpha' + q$ i $(\frac{1}{\alpha})' = \frac{1}{\alpha'}$.

Dokaz:

Gornje tvrđenje pokazuje da ukoliko je α kvadratni iracional i ukoliko je $\alpha = q + \frac{1}{\alpha_1}$ gde je $q = [\alpha]$, tada je $\alpha_1$takođe kvadratni iracional. Drugim rečima svi koraci u razvoju verižnog razlomka proizvode kvadratne iracionalnosti polazeći od jedinice. Ukoliko je α kvadrtani iracional, tada

$$\alpha = \frac{P \pm \sqrt{D}}{Q}$$

za $P, Q, D \in \mathbb{Z}$ gde je $D \geq 0$. Polazeći od prvog koraka u algoritmu za verižni razvoj dobija se:

$$[\alpha] = \left[\frac{P + [\pm\sqrt{D}]}{Q}\right].$$

Ukoliko se analizira inverzni algoritam razvoja, tj

$$\frac{1}{\frac{P+\sqrt{D}}{Q}} = \frac{P - \sqrt{D}}{\frac{P^2 - D}{Q}}$$

Primetno je da $Q \mid P^2 - D$, pri čemu $P = -B, D = B^2 - 4AC$ *i* $Q = 2A,$ pri čemu $A\alpha^2 + B\alpha + C = 0$ i $A, B, C \in \mathbb{Z}$.

Opisani proces jasno determiniše algoritam razvoja u verižni razlomak kvadratne iracionalnosti. Sledeća teroja pruža uvid u prelep algoritam, otkriven u 19.-om veku, zahvaljujući velikom francuskom matematičaru tog vremena Galoisu (Évariste Galois, 1811.)

Definicija 2.5.3. Kvadratni iracional naziva se redukovani kvadratni iracional ukoliko:

i) $\alpha > 1$
ii) $-1 < \alpha' < 0$

Primer 2.5.4.

$\sqrt{2}$ nije redukovani broj jer $(\sqrt{2})' = -\sqrt{2} < -1$. Ali $1 + \sqrt{2}$ je redukovani broj jer $(1 + \sqrt{2})' = 1 - \sqrt{2}$. Uopšteno $q_0 + \sqrt{N}$ je redukovani broj pri čemu je $q_0 = [\sqrt{N}]$

Verižni razlomak napisan u formi $a_0, a_1, a_2, \dots, a_n, a_0, a_1, a_2, \dots, a_n$ naziva se potpuni verižni razlomak.

Primer 2.5.5. Najjednistavniji primer potpunog verižnog razlomka je verižni razlomak $1, 1, 1, 1, 1, \dots$ Ukoliko je φ realni broj

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\dots}}}}$$

tada je $\varphi = 1 + \frac{1}{\varphi}$, pa zato i $\varphi^2 - \varphi - 1 = 0$ i

$$\varphi = \frac{1 \pm \sqrt{5}}{2}$$

Ukoliko se posmatra samo zbir u brojiocu, razlomak ima formu zaltnog preseka. Zlatni presek je redukovani kvadratni iracional.

Lema 2.5.6. Ako je α redukovani kvadratni iracional, tada je

$$\alpha = q_0 + \frac{1}{\alpha_1}$$

gde je $q_0 = [\alpha]$, tada je α_1 redukovani kvadratni iracional.
Dokaz.

Teorema 2.5.7. (Galoa) $\xi \in \mathbb{R}$ ima potpuni periodični verižni razlomak ako i samo ako je ξ kvadratni iracional.

Dokaz. Pretpostavimo da ξ ima potpuni periodični razvoj u verižni razlomak, tj

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots a_n + \cfrac{1}{\xi}}}}$$

za neko n. Tada $\xi = \frac{\xi s_n + s_{n-1}}{\xi t_n + t_{n-1}}$ i ξ mora biti kvadratni iracional jer je $t_n\xi^2 + (t_{n-1} - s_n)\xi - s_{n-1} = 0$
Ukoliko je

$$\xi_1 = a_n + \cfrac{1}{a_{n-1} + \cfrac{1}{a_{n-2} + \cfrac{1}{\dots a_0 + \cfrac{1}{\xi_1}}}}$$

tada $\xi' = \frac{[a_n,\dots,a_0,\xi_1]}{[a_{n-1},\dots,a_0,\xi_1]} = \frac{[a_n,\dots,a_0]\xi_1 + [a_n,\dots,a_1]}{[a_{n-1},\dots,a_0]\xi_1 + [a_{n-1},\dots,a_1]} = \frac{s_n\xi_1 + t_n}{s_{n-1}\xi_1 + t_{n-1}}$ i

$$s_{n-1}\xi_1^2 + (t_{n-1} - s_n)\xi_1 - t_n = 0$$

Tada sledi da je $\xi' = -\frac{1}{\xi_1}$ pri čemu je $-1 < \xi' < 0$.
Dokažimo suprotno. Neka je ξ redukovani kvadratni iracional. Tada

$\xi = \frac{P + \sqrt{D}}{Q}$ i $\xi' = \frac{P - \sqrt{D}}{Q}$. Ukoliko je $Q > 0$ pri čemu $(\xi - \xi')$ tada $P > 0$ i

i) $P < \sqrt{D}$
ii) $Q < 2\sqrt{D}$

Neka je $q = [\xi]$, tada

$$\xi - q = \frac{P - qQ + \sqrt{D}}{Q}$$

Iz Leme 2.5.6. sledi

$$\xi_1 = \frac{1}{\frac{P - qQ + \sqrt{D}}{Q}} = \frac{Q}{P - qQ + \sqrt{D}} = \frac{Q(-(P - qQ) + \sqrt{D})}{D - (P - qQ)^2}$$

Ukoliko je $P_1 = qQ - P$ i $Q_1 = \frac{(D - P_1^2)}{Q}$ sledi da je

$$\xi_1 = \frac{P_1 + \sqrt{D}}{Q_1}$$

Ponavljanjem istog postupka za ξ_1 pri čemu postoji konačno mnogo P i Q koji zadovoljavaju uslov $P < \sqrt{D}$ i $Q < 2\sqrt{D}$, indukcijom dokazujemo da $\xi_m = \xi_n$ za $m < n$.

Ukoliko je $\xi_{m-1} = \xi_{n-1}$ sledi razvoj u verižni razlomak $[a_0, a_1, a_2, \dots, a_{n-m}, a_0, a_1, a_2, \dots]$ odakle seldi da je n-ti korak u razvoju

$\xi_n = [\xi_n] + \frac{1}{\xi_{n+1}}$ odakle sledi da je $[\xi_n] = [-\frac{1}{\xi'_{n+1}}]$ sobzirom da je $[\xi_n] < \frac{1}{\xi'_{n+1}} < [\xi_n] + 1$. Ukoliko je $\xi_m = \xi_n$ sledi $[\xi_{m-1}] = [\xi_{n-1}]$, odnosno $\xi_{m-1} = \xi_{n-1}$. Na kraju se pokazuje da je redukovani kvadratni iracional ima potpuni periodični verižni razvoj □

2.6. Periodičan verižni razlomak broja $\sqrt{N}$

Poznato je da ukoliko je N prirodni broj i nije potpuni kvadrat, njegov razvoj u verižni razlomak je periodičan.

Primer 2.6.1. Periodični razvoj u verižni razlomak broja $\sqrt{14} = 3, \overline{1, 2, 1, 6}, 1, 2, 1, 6, \dots$

Periodični razvoj u verižni razlomak broja $\sqrt{19} = 4, \overline{2, 1, 3, 1, 2, 8}, 2, 1, 3, 1, 2, 8, \dots$

U primerima se može uočiti periodično ponavljanje određenog niza konvergenti nakon što sledeća konvrgenta dostigne vrednost $2a_0$. Takođe se može primetiti da je niz simetričan, što nije slučajnost, tj

Teorema 2.6.2. Ako je N prirodni broj koji nije potpuni kvadrat, tada:

$$\sqrt{N} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\dots + \cfrac{1}{q_n + \cfrac{1}{2q_0 + \cfrac{1}{q_1 + \cfrac{1}{\dots}}}}}}$$

gde je $q_1 = q_n, q_2 = q_{n-1}, \dots$

Dokaz. Neka je $q_0 = [\sqrt{N}]$, tada iz Teoreme 2.5.8. sledi da $q_0 + \sqrt{N}$ ima potpuni periodični razvoj verižnog razlomka. Tako je $\sqrt{N} + q_0 = 2q_0, q_1, \dots, q_n, 2q_0, q_1, \dots$ Ovim je dokazano prvo tvrđenje. Posmatrajmo konjugat $-\sqrt{N} + q_0$, tada

$$-\frac{1}{-\sqrt{N} + q_0} = q_n, q_{n-1}, \dots, q_1, 2q_0, q_n, \dots$$

odakle sledi da je $\sqrt{N} = q_0, q_n, q_{n-1}, \dots, q_1, 2q_0, q_n, \dots$

Iz jedinstvenosti verižnog razlomka sledi da je $q_1 = q_n, q_2 = q_{n-1}, \dots$□

2.7. Pelova jednačina

Definicija 2.7.1. Pelova jednačina je diofantska jednačina oblika $x^2 - Ny^2 = 1, x, y \in \mathbb{Z}$, za zadato $N \in \mathbb{N}$ koje nije potpuni kvadrat.

Uz pomoć algoritma za razvoj broja (koji nije potpuni kvadrat) $\sqrt{N}$ u verižnih razlomaka mogu se na vrlo elegantan način izračunati rešenja ove jednačine. Na osnovu Teoreme 2.6.2. sledi da je

$$\sqrt{N} = \frac{(q_0 + \sqrt{N})s_n + s_{n-1}}{(q_0 + \sqrt{N})t_n + t_{n-1}}$$

Množenjem desne strane jednačine dobija se:

$s_{n-1} = Nt_n - q_0 s_n,$
$t_{n-1} = s_n - q_0 t_n,$

tada
$s_{n-1}t_n - s_n t_{n-1} = (Nt_n - q_0 s_n)t_n - s_n(s_n - q_0 t_n) = Nt_n^2 - s_n^2$, odakle sledi da je

$$s_n^2 - Nt_n^2 = -(s_{n-1}t_n - s_n t_{n-1}) = -(-1)^n = (-1)^{n+1}$$

Primer 2.7.2. Naći rešenja Pelove jednačine $x^2 - 19y^2 = 1$

Razvoj verižnog razlomka $\sqrt{19} = 4, \overline{2, 1, 3, 1, 2, 8}, 2, 1, 3, 1, 2, 8, \dots$. Konvergente su date u sledećoj tabeli:

i	-2	-1	0	1	2	3	4	5	6

a_i			4	2	1	3	1	2	8
s_i	0	1	4	9	13	48	61	170	1421
t_i	1	0	1	2	3	11	14	39	326

Tako je rešenje $170^2 - 19 \cdot 39^2 = 1$

3. Faktorizacija pomoću verižnih razlomaka

3.1. Metoda Ferma-Krajčik

Trenutno najefektivniji algoritmi za faktorizaciju velikih brojeva koriste osobinu da se svaki ceo broj N može zapisati kao razlika dva kvadrata $x^2 - y^2$, tj.

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

U suprotnom, ako je neparan broj N složen, tj $N = uv$, tada

$$N = \left(\frac{u+v}{2}\right)^2 - \left(\frac{u-v}{2}\right)^2$$

Preteča ove metoda je Fermaov algoritam. Pretpostavimo da želimo da faktorišemo broj N. Fermaov algoritam polazi od funkcije:

$$S(x) = x^2 - N$$

i svodi se na pronalaženje x-a tako da je $S(x) = y^2$ kvadrat. Obično se polazi od $x = \lceil\sqrt{N}\rceil$, $x = \lceil\sqrt{N}\rceil + 1$, $x = \lceil\sqrt{N}\rceil + 2$, itd…

Primer 3.1.1. Naći faktore od $N = 2491$

$S(49) = -90,\ S(50) = 9 = 3^2$, tj
$2491 = (50 + 3)(50 - 3) = 53 \cdot 47$,

Naravno da se ova metoda za faktorisanje velikih brojeva, npr 2^{1000}, izvršava veoma sporo, međutim uz pomoć osobine kongurencije koju je dao M. Krajčik (M. Kraitchik) ova metoda se može svesti na činjenicu da je dovoljan uslov za pronalaženje faktora osobina da N deli $(x^2 - y^2)$, tj.

$$N \mid x^2 - y^2 = (x - y)(x + y)$$

ukoliko N ne deli $(x - y)$ ni $(x + y)$ tada je $gcd(x + y, N) > 1$ i primenom Euklidovog algoritma za pronalaženje $gcd(x + y, N)$ izračunavaju se netrivijalni faktori od N, tako da se nalaženje faktora svodi na kongruenciju:

$$x^2 \equiv y^2 \ (mod\ N)$$
$$x^2 \not\equiv \pm y \ (mod\ N).$$

Pretpostavimo da smo pronašli $x_1, \dots, x_n$ tako da ${x_1}^2 \equiv a_1 (mod\ N), \dots, {x_n}^2 \equiv a_n (mod\ N)$ za neke cele brojeve $a_1, \dots, a_n$. Ukoliko postoji podniz $a_{i_1}, \dots, a_{i_r}$ niza $a_1, \dots, a_n$ tako da je $a_{i_1} \dots a_{i_r}$ potpuni kvadrat, tada

$\left(x_{i_1} \cdots x_{i_r}\right)^2 \equiv a_{i_1} \cdots a_{i_r} \ (mod\ N)$, tj (3.1.2.)
$x^2 \equiv y^2 \ (mod\ N)$.

Ova kongruencija može ili ne mora zadovoljiti uslov da je $x \not\equiv \pm y \ (mod\ N)$. Da bi saznali da je li je n potpuni kvadrat faktorišemo ga $n = {p_1}^{n_1} \cdots {p_r}^{n_r}$, koristeći predefinisanu bazu faktora $P = \{p_1, \dots, p_r\}$ (malih) prostih brojeva. Tada je n potpuni kvadrat akko su svi eksponenti $n_1 \dots n_r$ parni.

Primer 3.1.2. Faktorisati broj $N = 2041$

x	$x^2 - N$	$Faktorizacija$	$Označeno$
46	75	$3 \cdot 5^2$	✓
47	168	$2^3 \cdot 3 \cdot 7$	✓
48	263	263	
49	360	$2^3 \cdot 3^2 \cdot 5$	✓
50	459	$3^3 \cdot 17$	
51	560	$2^4 \cdot 5 \cdot 7$	✓

Sledi da je

$S(46)S(47)S(49)S(51) = 75 \cdot 168 \cdot 360 \cdot 560 = (2^5 \cdot 3^2 \cdot 5^2 \cdot 7)^2$ kvadrat. Za $u = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7$ sledi da je $u^2 = 50400^2 \equiv 1416^2 \ (mod\ 2041)$. Kako je $u^2 \equiv v^2 (\mathrm{mod}\ 2041)$ pri čemu je $v = 46 \cdot 47 \cdot 49 \cdot 51 = 5402838 \equiv 311 \ (mod\ 2041)$.

Faktor dobijamo izračunavanjem najvećeg zajedničkog delioca od $(u - v)$ i 2041, a to je $13 \cdot 157$. Korišćenjem Fermaove teoreme, morali bismo čekati na izvršenje algoritma do $x = 80$ da bi pronašli faktor od N.

Najteži deo algoritma je faktorisanje $S(x) = x^2 - N$. Oko 1982. godine Pomerans (Pommerance) je pronašao zanimljiv trik da bi ovo izbegao. Primetio je da p^r deli $S(x)$ akko deli $S(x + kp^r)$, gde je $k \in \mathbb{Z}$. Ukoliko pronađemo x tako da p^r deli $S(x)$, tada $p^r \mid S(x + p^r), S(x + 2p^r)$, ...Ova metoda naziva se Metoda kvadratnog sita i trenutno je najpoznatija metoda za faktorisanje velikih brojeva korišćena na RSA takmičenjima. Na RSA takmičenju 155-ocifreni broj faktorisan je korišćenjem kvadratnog sita.

U sledećem poglavlju predstavljen je najbolji metod za faktorisanje velikih brojeva korišćenjem verižnih razlomaka koji je prethodio metodi kvadratnog sita.

3.2. Primena verižnog razvoja √n

Problem sa Fermaovom metodom je vremenska složenost izračunavanja f-je $S(x) = x^2 - N$.

Umesto toga mogu se koristiti konvergente $\frac{s_n}{t_n}$ u verižnom razvoju $\sqrt{N}$ (ili $\sqrt{kN}, k \in \mathbb{N}$). Za konvergente mogu se uzeti brojevi:

$x_n = s_n$
$y_n = s_n^2 - Nt_n^2$

Tačnije
$x_n^2 \equiv y_n \ (mod\ N)$

pri čemu
$|y_n| < 2\sqrt{N}$.

Dokaz. Na osnovu Teoreme 2.5.7.

Uvedemo oznake:

$a_0 = \sqrt{N}, s_0 = 0, t_0 = 1$

$s_{i+1} = a_i t_i - s_i$

$t_{i+1} = \frac{N - s_{i+1}^2}{t_i}$

$a_i = \left[\frac{\sqrt{N} + s_i}{t_i}\right], i \geq 0$

$p_i = a_i p_{i-1} + p_{i-2},\ p_0 = a_0, p_1 = a_0 a_1 + 1$

$q_i = a_i q_{i-1} + q_{i-2}\ , q_0 = 1, q_1 = a_1$

Ukoliko pronađemo podniz $t_{r_1}, \dots, t_{r_k}$ koji je potpuni kvadrat, npr. jednak u^2 tada iz (3.1.2) sledi da je $p_{k_1}^2\, p_{k_2}^2 \dots p_{k_m}^2 \equiv u^2\ (mod\ N)$. Ukoliko je bar jedan od brojeva $(p_{k_1}\, p_{k_2}\, \dots\, p_{k_m} - u, N)$ i $(p_{k_1}\, p_{k_2}\, \dots\, p_{k_m} + u, N)$ različit od N, to su sigurno faktori od N, pri čemu važi $p_i^2 - Nq_i^2 = (-1)^{i+1} t_{i+1}$

U svakoj iteraciji računamo i kvadratne ostatke parcijalnog razlomka po modulu N i formiramo faktorsku bazu ostataka. Za bazu faktora koristimo proste brojeve manje od b, tj od izabrane granice glatkosti koju računamo po formuli $sqrt(exp(sqrt(log(n)\ log(log(n)))))$

Ako je A matrica baze kvadratnih ostataka i x nenula vektor tada $A^t x = 0$

x dobijamo tako što tražimo nula prostor matrice A^t, tj linearnu kombinaciju svih nenula vektora iz nula prostora matrice A^ti to su ostaci koje koristimo dalje u ispitivanju.

4. Programska realizacija algoritma

Zadatak: napisati program koji izračunava netrivijalne faktore proizvoljno unetog velikog složenog celog broja N korišćenjem verižnog razvoja.

4.1. Struktura programa

Koraci u izvršavanju algoritma:

1. Čita korisnički broj sa standardnog ulaza N
2. Računa glatkost unetog broja b
3. Generiše bazu faktora do granice b
4. Računa konvergente primenom sledećeg algoritma

$a_0 = \sqrt{N}, s_0 = 0, t_0 = 1$

$s_{m+1} = a_m t_m - s_m$

$t_{m+1} = \frac{N - s_{m+1}^2}{t_m}$

$a_m = \left[\frac{\sqrt{N} + s_m}{t_m}\right], m \geq 0$

$p_m = a_m p_{m-1} + p_{m-2}$

$q_m = q_m q_{m-1} + q_{m-2}$

4.1. U svakoj iteraciji generiše bazu faktora kvadratnih ostataka parcijalnih razlomaka koji se pojavljuju u verižnom razlomku i čuva u matrici A, pri čemu se kvadratni ostaci čuvaju u vrstama, dok se faktori čuvaju u kolonama.

4.2. Računa nula prostor matrice A^t i traži nenula vektor tog prostora po modulu 2, tj vektor x jednačine $A^t x = 0$

4.2.1. Ukoliko je $p_{k_1} \cdot p_{k_2} \cdot p_{k_3} \cdots p_{k_r} \equiv u^2$računa $(p_{k_1} p_{k_2} \dots p_{k_m} - u, N)$ i $(p_{k_1} p_{k_2} \dots p_{k_m} + u, N)$

4.2.1.1. Ako je bar jedan od njih različit od N, to su sigurno faktori od N, pri čemu važi $p_i^2 - Nq_i^2 = (-1)^{i+1} t_{i+1}$. Zatim računa količnik i vraća se na korak 2.

4.2.1.2. Ukoliko nije pronašao faktor vraća se na korak 4. i računa sledeću konvergentu

5. KRAJ

Koristi JAVA BigInteger biblioteku za rad sa velikim brojevima. Kreirana interna biblioteka sadrži klase prikazane na slici1.

Class Summary

Class	Description
BigMath	Pocna klasa za rad sa BigInteger brojevima.
CFRACFactorization	Klasa CFRACFactorization Rastavlja broj na proste cinioce metodom veriznih razlomaka
Dialog	Interaktivni korisnicki dijalog.
Files	Omogucava rad sa file-ovima
Log	Stampa korisnickih i programskih obavestenja
Matrix	
Test	Omogucava razna testiranja

4.2. Dobijeni rezultati

Program u veoma kratkom vremenskom intervalu i sa velikom preciznosću računa konvergente velikog složenog broja, dok je više vremena potrebno za pronalaženje faktora istog.

Algoritam zahteva $\exp(\sqrt{2 \ln n \ln \ln n})$ koraka za realizaciju [5]

Primer:

Enter number: 17873

[Thu Oct 10 05:12:13 CEST 2013]INFO: 17873

[Thu Oct 10 05:12:13 CEST 2013]INFO: Start continued fraction factorization of: 17873

[Thu Oct 10 05:12:13 CEST 2013]INFO: Number smoothness: 11

[Thu Oct 10 05:12:13 CEST 2013]INFO: Squere root: 133

Primes: [2, 3, 5, 7, 11, -1]

1. 134/1, 134^2 = 184 (mod 17873) []

2. 401/3, 401^2 = 83 (mod 17873) []

3. 1738/13, 1738^2 = 56 (mod 17873) [3, 0, 0, 1, 0, 1]

4. 3877/29, 3877^2 = 107 (mod 17873) []

5. 13369/100, 13369^2 = 64 (mod 17873) [6, 0, 0, 0, 0, 1]

NZD(17599 + 3584, 17873) = 1

NZD(17599 - 3584, 17873) = 1

6. 17246/129, 17246^2 = 161 (mod 17873) []

NZD(17599 + 3584, 17873) = 1

NZD(17599 - 3584, 17873) = 1

7. 12115/358, 12115^2 = 77 (mod 17873) [0, 0, 0, 1, 1, 1]

NZD(16668 + 4312, 17873) = 1

NZD(16668 - 4312, 17873) = 1

8. 11488/487, 11488^2 = 149 (mod 17873) []

NZD(16668 + 4312, 17873) = 1

NZD(16668 - 4312, 17873) = 1

9. 17218/1332, 17218^2 = 88 (mod 17873) [3, 0, 0, 0, 1, 1]

NZD(13327 + 4928, 17873) = 1

NZD(13327 - 4928, 17873) = 1

NZD(7272 + 4928, 17873) = 61

NZD(7272 - 4928, 17873) = 293

NZD(17716 + 6776, 17873) = 1

NZD(17716 - 6776, 17873) = 1

NZD(16668 + 4312, 17873) = 1

NZD(16668 - 4312, 17873) = 1

[Thu Oct 10 05:12:13 CEST 2013]INFO: FACTOR FOUNDED.

[Thu Oct 10 05:12:13 CEST 2013]INFO: Factors: [293]

[Thu Oct 10 05:12:13 CEST 2013]INFO: 17873 --

****

[Thu Oct 10 05:12:13 CEST 2013]INFO: Start continued fraction factorization of: 61

[Thu Oct 10 05:12:13 CEST 2013]INFO: Number smoothness: 4

[Thu Oct 10 05:12:13 CEST 2013]INFO: Squere root: 7

Primes: [2, 3, -1]

1. 8/1, 8^2 = 12 (mod 61) [2, 1, 0]

2. 39/5, 39^2 = 3 (mod 61) [0, 1, 0]

NZD(56 + 6, 61) = 1

NZD(56 - 6, 61) = 1

3. 3/16, 3^2 = 4 (mod 61) [2, 0, 1]

4. 42/21, 42^2 = 9 (mod 61) [0, 2, 0]

5. 26/58, 26^2 = 5 (mod 61) []

6. 33/15, 33^2 = 5 (mod 61) []

7. 59/12, 59^2 = 9 (mod 61) [0, 2, 1]

NZD(6 + 6, 61) = 1

NZD(6 - 6, 61) = 61

NZD(31 + 36, 61) = 1

NZD(31 - 36, 61) = 1

NZD(6 + 6, 61) = 1

NZD(6 - 6, 61) = 61

8. 27/51, 27^2 = 4 (mod 61) [2, 0, 0]

NZD(6 + 6, 61) = 1

NZD(6 - 6, 61) = 61

NZD(31 + 36, 61) = 1

NZD(31 - 36, 61) = 1

NZD(6 + 6, 61) = 1

NZD(6 - 6, 61) = 61

9. 45/33, 45^2 = 3 (mod 61) [0, 1, 1]

NZD(31 + 36, 61) = 1

NZD(31 - 36, 61) = 1

10. 11/23, 11^2 = 12 (mod 61) [2, 1, 0]

NZD(53 + 15552, 61) = 1

NZD(53 - 15552, 61) = 1

11. 16/50, 16^2 = 1 (mod 61) [0, 0, 1]

NZD(13 + 108, 61) = 1

NZD(13 - 108, 61) = 1

NZD(13 + 108, 61) = 1

NZD(13 - 108, 61) = 1

****

[Thu Oct 10 05:12:13 CEST 2013]INFO: === Factors: [293, 61] ====

Enter 'q' for exit.

Enter number:

5. Zaključak

Primena verižnih razlomaka u faktorizaciji velikog prirodnog složenog celog broja predstavlja veoma dobar primer kako se različiti matematički modeli i njihove osobine mogu iskoristiti kao adekvatan alat u rešavanju raznih praktičnih problema. U slučaju faktorizacije, metoda verižnih razlomaka, jedna je od prvih modernijih metoda koja je u ovu svrhu uspešno upotrebljena.

U radu je prikazan metod razvoja broja u verižni razlomak, pri čemu se određuju konvergente tog razvoja koje se dalje koriste u izračunavanju faktora. I ako vreme izvršavanja algoritma eksponencijalno raste sa porastom broja konvergenti, ipak je moguće u realnom vremenu faktorisati brojeve i do 50 cifara na personalnom računaru sa ograničenim resursima. Algoritam se može dalje optimizovati paralelizacijom, što bi u mnogome smanjilo vreme izvršavanja kao i ostale resurse.

6. Literatura

[1] **Niels Lauritzen**, CONTINUED FRACTIONS AND FACTORING, DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF AARHUS, DENMARK

[2] **J. Brillhart, M. A. Morrison**, A method of factoring and the factorization of F7, Math. Comp. 29, 183-205 (1975).

[3] **D. H. Lehmer, R. E. Powers**, On factoring large numbers, Bull. Amer. Math. Soc. 37, 770-776 (1931).

[4] **A. M. Rockett, Peter Szüs**, Continued Fractions, World Scientific, 59 – 64 (1992)

[5] **Weisstein, Eric W.** Continued Fraction Factorization Algorithm. http://mathworld.wolfram.com/ContinuedFractionFactorizationAlgorithm.html

[6] **Alan Baker,** (dobitnik Filcove medalje), A concise introduction to the theory of numbers