Opće metode faktorizacije

Aladin Crnkić[1], *Bernadin Ibrahimpašić,*[2]

Uvod

Faktorizacija velikih prirodnih brojeva jedan je od problema iz područja teorije brojeva za koji još uvijek ne postoji učinkovit algoritam koji bi se mogao izvršavati na klasičnom računalu. Cilj faktorizacije prirodnih brojeva je zapisati ga u obliku produkta $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, gdje su p_i različiti prosti i α_i prirodni brojevi. Osim u teoriji brojeva, problem faktorizacije velikih brojeva od iznimne je važnosti u području informacijske sigurnosti jer se sigurnost nekih kriptografskih algoritama, od kojih je najpoznatiji RSA, temelji upravo na nemogućnosti napadača da faktorizira velike brojeve.

Problem pronalaženja prostog faktora za složeni broj n je mnogo teži od samog problema utvrđivanja da li je n prost ili složen. Osnovna metoda faktorizacije je dijeljenje s prostim brojevima manjim ili jednakim $\sqrt{n}$, ali kako prostih brojeva manjih od $\sqrt{n}$ ima približno $2\sqrt{n}/\ln n$ to je ova metoda spora za veliki n. Međutim, ta metoda je vrlo korisna za brojeve $n < 10^{12}$.

Metode faktorizacije, zavisno od toga da li očekivani broj operacija zavisi samo o veličini broja n ili i o svojstvima prostih faktora od n, dijelimo na opće i specijalne. U [2] su detaljno opisane Pollardova ρ-metoda, Pollardova $p-1$ metoda i Fermatova metoda, koje spadaju u grupu specijalnih metoda, i faktorske baze koje pripadaju općim metodama. U sklopu ovog rada, koji predstavlja nastavak na [2], bit će opisane dvije opće metode koje koriste faktorske baze, a to su *metoda verižnih razlomaka* i *metoda kvadratnog sita*.

Metoda verižnih razlomaka

Osnovna ideja ove metode potječe još od M. Kraitchika iz 1920. godine, pa čak i ranije od Legendrea. Koristili su je D. H. Lehmer i R. E. Powers 1930. godine, ali zbog tehnološke nerazvijenosti nije bila u čestoj upotrebi, niti je bila primjenjiva. Prvu njenu primjenu na računalima, izvršili su M. A. Morison i J. Brillhart, koji su 13. rujna 1970. godine faktorizirali sedmi Fermatov broj

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

Ova metoda koristi verižne razlomke, pa ćemo početi s definicijom i osnovnim svojstvima razvoja realnog broja α u verižni razlomak.

[1] Profesor je matematike u Gimnaziji u Bihaću, e-pošta: crnkic_al@bih.net.ba

[2] Profesor je na Pedagoškom fakultetu Univerziteta u Bihaću, e-pošta: bernadin@bih.net.ba

Definicija 1. *Verižni razlomak* je izraz oblika

$$\alpha = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \ddots}}},$$

gdje je $a_0 \in \mathbf{Z}$, te $a_i, b_i \in \mathbf{N}$ $(i = 1, 2, 3, ...)$. *Jednostavan verižni razlomak* je onaj u kojem su svi b_i jednaki 1.

U ovom radu ćemo se baviti isključivo s jednostavnim verižnim razlomcima, pa ćemo riječ "jednostavan" ubuduće izostavljati.

Verižni razlomak kraće zapisujemo kao $[a_0; a_1, a_2, ...]$. Brojevi a_i se zovu *parcijalni kvocijenti*, a $\alpha_i = [a_i; a_{i+1}, a_{i+2}, ...]$ *potpuni kvocijenti*.

Racionalne brojeve

$$\frac{p_i}{q_i} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_i}}} = [a_0; a_1, a_2, ...a_i]$$

nazivamo *konvergente verižnog razlomka*. Brojnici i nazivnici konvergenti, za $i \geqslant 2$, zadovoljavaju sljedeće rekurzije:

$$p_i = a_i p_{i-1} + p_{i-2}, \qquad q_i = a_i q_{i-1} + q_{i-2},$$

uz

$$p_0 = a_0, \quad p_1 = a_0 a_1 + 1, \quad q_0 = 1, \quad q_1 = a_1.$$

Uz dogovor

$$p_{-2} = 0, \quad p_{-1} = 1, \quad q_{-2} = 1, \quad q_{-1} = 0,$$

dane rekurzivne relacije vrijede za $i \geqslant 0$.

Primjer 1. Izračunajmo $[3; 2, 1, 4, 5, 6]$.

Rješenje.

i	-2	-1	0	1	2	3	4	5
p_i	0	1	3	7	10	47	245	1517
q_i	1	0	1	2	3	14	73	452

Dakle, $[3; 2, 1, 4, 5, 6] = \dfrac{1517}{452}$. $\square$

Teorem 1. *Verižni razlomak koji predstavlja broj α je konačan ako i samo ako je α racionalan.*

Dokaz.

$(\Rightarrow)$ Neka je $\alpha = [a_0; a_1, ..., a_n]$ konačan verižni razlomak. Pokažimo indukcijom da je tada α racionalan.

Za $n = 1$ je $\alpha = [a_0; a_1] = a_0 + \dfrac{1}{a_1} = \dfrac{a_0 a_1 + 1}{a_1}$ racionalan. Pretpostavimo da je $\alpha = [a_0; a_1, ..., a_k]$ racionalan. Pokažimo da to vrijedi i za $n = k + 1$. Kako je prema

pretpostavci i $[a_1; a_2, ..., a_{k+1}]$ racionalan, postoje cijeli r i prirodan s, takvi da je $[a_1; a_2, ..., a_{k+1}] = \frac{r}{s}$, pa je

$$\alpha = [a_1; a_2, ..., a_{k+1}] = a_0 + \frac{1}{\frac{r}{s}} = \frac{a_0 r + s}{r}$$

racionalan.

($\Leftarrow$) Neka je $\alpha = \frac{a}{b}, a \in \mathbf{Z}, b \in \mathbf{N}$ i $\operatorname{nzd}(a,b) = 1$. Koristeći Euklidov algoritam imamo

$$\begin{aligned}
a &= ba_0 + r_1, & 0 < r_1 < b,\\
b &= r_1 a_1 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 a_2 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1} a_{n-1} + r_n, & 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n a_n,
\end{aligned}$$

gdje su $a_1, a_2, ..., a_n$ prirodni brojevi. Zapišimo ovo na drugi način.

$$\begin{aligned}
\frac{a}{b} &= a_0 + \frac{r_1}{b}\\
\frac{b}{r_1} &= a_1 + \frac{r_2}{r_1}\\
\frac{r_1}{r_2} &= a_2 + \frac{r_3}{r_2}\\
&\vdots\\
\frac{r_{n-1}}{r_n} &= a_n
\end{aligned}$$

Sada imamo

$$\frac{a}{b} = a_0 + \frac{1}{\frac{b}{r_1}} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}}$$

$$= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_3}{r_2}}} = \cdots = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ddots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}.$$

□

Iz dokaza vidimo da se parcijalni kvocijenti mogu dobiti kao količnici u Euklidovom algoritmu, ali se konačan verižni razlomak može dobiti i sljedećim postupkom.

Neka je α proizvoljan racionalan broj. S $\lfloor \alpha \rfloor$ ćemo označavati najveći cijeli broj koji nije veći od α, a s $\{\alpha\}$ realan broj $\alpha - \lfloor \alpha \rfloor$. Stavimo $\alpha_0 = \alpha$, $a_i = \lfloor \alpha_i \rfloor$, $\alpha_{i+1} = \frac{1}{\alpha_i - a_i}$, $i = 0, 1, 2, \ldots$. Postupak završava kada dobijemo $a_n = \alpha_n$. Tako ćemo imati $a_0 \in \mathbf{Z}$ i $a_i \in \mathbf{N}$, $i = 1, 2, \ldots$.

Primjer 2. Razvijmo broj $\dfrac{179}{52}$ u verižni razlomak.

Rješenje.

razvoj u konačan verižni razlomak od $\frac{179}{52}$		Euklidov algoritam za nzd $(179, 52)$
$\alpha_0 = \dfrac{179}{52},$	$a_0 = \lfloor \alpha_0 \rfloor = 3$	$179 = 52 \cdot 3 + 23$
$\alpha_1 = \dfrac{1}{\alpha_0 - a_0} = \dfrac{52}{23},$	$a_1 = \lfloor \alpha_1 \rfloor = 2$	$52 = 23 \cdot 2 + 6$
$\alpha_2 = \dfrac{1}{\alpha_1 - a_1} = \dfrac{23}{6},$	$a_2 = \lfloor \alpha_2 \rfloor = 3$	$23 = 6 \cdot 3 + 5$
$\alpha_3 = \dfrac{1}{\alpha_2 - a_2} = \dfrac{6}{5},$	$a_3 = \lfloor \alpha_3 \rfloor = 1$	$6 = 5 \cdot 1 + 1$
$\alpha_4 = \dfrac{1}{\alpha_3 - a_3} = \dfrac{5}{1},$	$a_4 = \lfloor \alpha_4 \rfloor = 5$	$5 = 1 \cdot 5$

Dobivamo $\dfrac{179}{52} = [3; 2, 3, 1, 5]$. $\square$

Vidjeli smo da je razvoj u jednostavni verižni razlomak realnog broja α konačan ako i samo ako je $\alpha \in \mathbf{Q}$. Dakle, za beskonačni verižni razlomak znamo da je razvoj iracionalnog broja. U tom slučaju je α jednak limesu konvergenti.

Definicija 2. Za beskonačni verižni razlomak kažemo da je *periodičan* ako postoje cijeli k i m, takvi da je $a_{i+m} = a_i$, za sve $i \geqslant k$. To zapisujemo

$$[a_0; a_1, ..., a_k, \overline{a_{k+1}, a_{k+2}, ..., a_{k+m}}].$$

Najmanji takav m se zove *period*.

Verižni razlomak koji predstavlja $\sqrt{n}$, za prirodan broj n, je periodičan ako i samo ako n nije potpun kvadrat. Čak štoviše, tada je

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

i vrijedi $a_i = a_{r-1}$, za $i = 1, 2, ..., r-1$.

U ovom slučaju, razvoj u verižni razlomak se može dobiti primjenom sljedećeg algoritma

$$a_0 = \left\lfloor \sqrt{n} \right\rfloor, \qquad s_0 = 0, \qquad s_1 = a_0, \qquad t_1 = n - a_0^2,$$

$$a_i = \left\lfloor \frac{a_0 + s_i}{t_i} \right\rfloor, \qquad s_{i+1} = a_i t_i - s_i, \qquad t_{i+1} = \frac{n - s_{i+1}^2}{t_i}, \qquad i \geqslant 1. \tag{1}$$

Proces se zaustavlja ako je $(s_k, t_k) = (s_l, t_l)$ za $k \neq l$.

Primjer 3. Zapisati broj $\sqrt{23}$ u obliku verižnog razlomka.

Rješenje.

$$a_0 = \left\lfloor \sqrt{23} \right\rfloor = \lfloor 4.796 \rfloor = 4, \quad s_0 = 0, \quad s_1 = 4, \quad t_1 = 23 - 4^2 = 7,$$

$$a_1 = \left\lfloor \frac{a_0 + s_1}{t_1} \right\rfloor = \left\lfloor \frac{4+4}{7} \right\rfloor = 1, \quad s_2 = a_1 t_1 - s_1 = 1 \cdot 7 - 4 = 3,$$

$$t_2 = \frac{n - s_2^2}{t_1} = \frac{23 - 3^2}{7} = 2,$$

$$a_2 = \left\lfloor \frac{a_0 + s_2}{t_2} \right\rfloor = \left\lfloor \frac{4+3}{2} \right\rfloor = 3, \quad s_3 = a_2 t_2 - s_2 = 3 \cdot 2 - 3 = 3,$$
$$t_3 = \frac{n - s_3^2}{t_2} = \frac{23 - 3^2}{2} = 7.$$

Nastavljajući isti postupak dobivamo

i	0	1	2	3	4	5
s_i	0	4	3	3	4	4
t_i	1	7	2	7	1	7
a_i	4	1	3	1	8	1

Kako je $(s_5, t_5) = (s_1, t_1)$, to je zapis broja $\sqrt{23}$ u verižni razlomak

$$\sqrt{23} = [4, \overline{1, 3, 1, 8}].$$

□

Vratimo se postupku faktorizacije. Neka je $\frac{p_i}{q_i} = [a_o : a_1, ..., a_i]$. Uz oznake iz (1) vrijedi

$$p_i^2 - n \cdot q_i^2 = (-1)^{i+1} t_{i+1}, \qquad i \geqslant 0,$$

te $s_i < \sqrt{n}$ i $t_i < 2\sqrt{n}$. Uvedimo oznaku $t_i^* = (-1)^i t_i$ i pretpostavimo da smo pronašli produkt

$$t_{k_1+1}^* \cdot t_{k_2+1}^* \cdot ... \cdot t_{k_l+1}^* = z^2, \tag{2}$$

koji je potpun kvadrat. Tada iz (2) slijedi

$$t_{k_1+1}^* \cdot t_{k_2+1}^* \cdot ... \cdot t_{k_l+1}^* \equiv p_{k_1}^2 \cdot p_{k_2}^2 \cdot ... \cdot p_{k_l}^2 \pmod{n}. \tag{3}$$

U relaciji (3), možemo svaki p_{k_i} zamijeniti s $p_{k_i} \bmod n$ ili s njegovim apsolutno najmanjim ostatkom modulo n. Ukoliko je

$$p_{k_1} \cdot p_{k_2} \cdot ... \cdot p_{k_l} \not\equiv \pm z \pmod{n},$$

tada su brojevi $\operatorname{nzd}(p_{k_1} \cdot p_{k_2} \cdot ... \cdot p_{k_l} + z, n)$ i $\operatorname{nzd}(p_{k_1} \cdot p_{k_2} \cdot ... \cdot p_{k_l} - z, n)$ faktori od n. Ako je bar jedan od njih različit od n, tada smo broj n uspjeli faktorizirati.

Primjer 4. Faktorizirajmo broj $n = 17\,873$ metodom verižnog razlomka.

Rješenje. Koristeći dane relacije za a_i, s_i, t_i^* i p_i dobivamo

i	0	1	2	3	4	5	6
s_i	0	133	51	115	109	105	87
t_i^*	1	−184	83	−56	107	−64	161
a_i	133	1	2	4	2	3	1
p_i	133	134	401	1738	3877	13 369	17 246

Vidimo da je $t_1^* \cdot t_3^* \cdot t_6^* = (-184) \cdot (-56) \cdot 161 = 1288^2$. Sada imamo $p_0^* \cdot p_2^* \cdot p_5^* = (133 \cdot 401 \cdot 13369)^2 \equiv 1288^2 \pmod{17\,873}$, pa je $z = 1288$. Međutim, imamo i $p_0^* \cdot p_2^* \cdot p_5^* = 133 \cdot 401 \cdot 13369 \equiv 1288 \pmod{17\,873}$, pa ne možemo faktorizirati n. Zato nastavljamo dalje i dobivamo

i	7	8	9	10	11
s_i	74	80	69	107	112
t_i^*	-77	149	-88	73	73
a_i	2	1	2	3	3
p_i	47 861	65 107	178 075	599 332	1 976 071

Opet smo dobili puni kvadrat, tj. $t_5^* \cdot t_{10}^* \cdot t_{11}^* = (-64) \cdot 73 \cdot (-73) = 584^2$. Sada je $p_4^* \cdot p_9^* \cdot p_{10}^* = (3877 \cdot 178075 \cdot 599332)^2 \equiv 5272^2 \pmod{17\,873}$, pa kako je $5272 \not\equiv 584 \pmod{17\,873}$ imamo netrivijalne faktore od n

$$\operatorname{nzd}(5272 + 584, 17\,873) = \operatorname{nzd}(5856, 17\,873) = 61,$$
$$\operatorname{nzd}(5272 - 584, 17\,873) = \operatorname{nzd}(4688, 17\,873) = 293,$$

tj. $n = 61 \cdot 293$. $\square$

Da bi metoda verižnog razlomka postala subeksponencijalna metoda, gore opisanu ideju treba kombinirati s korištenjem faktorske baze.

Definicija 3. Skup $\mathcal{B} = \{d_1, d_2, ..., d_k\}$, različitih prostih brojeva, s tim da može biti $d_1 = -1$, se zove *faktorska baza*.

Definicija 4. Kvadrat cijelog broja b je $\mathcal{B}$*-broj* (za dani n), ako se apsolutno najmanji ostatak $b^2 \bmod n$ može zapisati kao produkt brojeva iz $\mathcal{B}$.

U sljedećem primjeru ćemo koristiti algoritam metode faktorske baze, koja je detaljno opisana u [2]. Za faktorsku bazu $\mathcal{B}$ uzimamo -1 i sve proste brojeve koji se nalaze u više od jednog rastava brojeva t_i na proste faktore, i oni koji se nalaze u samo jednom rastavu, ali s parnom potencijom. Tada je

$$b_i = p_{i-1}, \quad y_i = b_i^2 \bmod n = p_{i-1}^2 \bmod n = t_i^*, \quad i \geqslant 1.$$

Primjer 5. Broj $n = 17\,873$ možemo faktorizirati metodom verižnog razlomka kao specijalnog slučaja metode faktorske baze.

Rješenje. Koristeći primjer 4, upravo opisani način formiranja faktorske baze i metodu faktorske baze opisane u [2], imamo

$$\begin{aligned}
b_1 &= 133, & y_1 &= -184 = -1 \cdot 2^3 \cdot 23,\\
b_2 &= 134, & y_2 &= 83,\\
b_3 &= 401, & y_3 &= -56 = -1 \cdot 2^3 \cdot 7,\\
b_4 &= 1738, & y_4 &= 107,\\
b_5 &= 3877, & y_5 &= -64 = -1 \cdot 2^6,\\
b_6 &= 13\,369, & y_6 &= 161 = 23 \cdot 7.
\end{aligned}$$

Vidimo da je $\mathcal{B} = \{-1, 2, 7, 23\}$, pa formirajmo tablicu čiji su elementi potencije elemenata faktorske baze za odabrane b_i-ove.

b_i	-1	2	7	23
133	1	3	–	1
401	1	3	1	–
3877	1	6	–	–
13 369	–	–	1	1

Također ne možemo dobiti nul-vektor u $\mathbf{Z}_2^4$ kao sumu nekih redaka ove matrice. To znači da ne možemo još faktorizirati broj n, pa idemo dalje

$$\begin{aligned} b_7 &= 17\,246, & y_7 &= -77 = -1 \cdot 7 \cdot 11, \\ b_8 &= 47\,861, & y_8 &= 149, \\ b_9 &= 65\,107, & y_9 &= -88 = -1 \cdot 2^3 \cdot 11, \\ b_{10} &= 178\,075, & y_{10} &= 73, \\ b_{11} &= 599\,332, & y_{11} &= -73 = -1 \cdot 73. \end{aligned}$$

Zbog novih faktora 11 i 73, faktorsku bazu proširujemo, i dobivamo $\mathcal{B} = \{-1, 2, 7, 11, 23, 73\}$, pa proširujemo tablicu.

b_i	-1	2	7	11	23	73
133	1	3	–	–	1	–
401	1	3	1	–	–	–
3877	1	6	–	–	–	–
13 369	–	–	1	–	1	–
17 246	1	–	1	1	–	–
65 107	1	3	–	1	–	–
178 075	–	–	–	–	–	1
599 332	1	–	–	–	–	1

Suma prva četiri i zadnja dva retka jednaka je nul-vektoru u $\mathbf{Z}_2^6$, pa je

$$x = 133 \cdot 401 \cdot 3877 \cdot 13\,369 \cdot 178\,075 \cdot 599\,332 \bmod 17\,873 = 16\,469,$$

$$y = (-1)^{\frac{1+1+1+1}{2}} \cdot 2^{\frac{3+3+6}{2}} \cdot 7^{\frac{1+1}{2}} \cdot 23^{\frac{1+1}{2}} \cdot 73^{\frac{1+1}{2}} \bmod 17\,873 = 1526.$$

Sada računamo

$$\operatorname{nzd}(x+y, n) = \operatorname{nzd}(16\,469 + 1526, 17\,873) = \operatorname{nzd}(17\,995, 17\,873) = 61,$$

$$\operatorname{nzd}(x-y, n) = \operatorname{nzd}(16\,469 - 1526, 17\,873) = \operatorname{nzd}(14\,943, 17\,873) = 293,$$

pa je $n = 61 \cdot 293$, i uspjeli smo faktorizirati broj n. □

Brillhart i Morrison su koristili jednu modifikaciju gore opisane metode. Naime, umjesto razvoja $\sqrt{n}$ koristili su razvoj broja $\sqrt{kn}$ za prirodan k. Oni su koristeći $k = 257$ faktorizirali sedmi Fermatov broj.

Broj operacija za faktorizaciju metodom verižnog razlomka je

$$\mathcal{O}\left(e^{(\sqrt{2}+\varepsilon)\sqrt{ln\,n \cdot ln(ln\,n)}}\right),$$

gdje je ε proizvoljno malen.

Metoda kvadratnog sita

Iako je metodu kvadratnog sita prvi uveo Pomerance 1982. godine, takvom otkriću mnogo se duguje prijašnjim metodama faktorizacije zasnovanim na idejama Kraitchika i Dixona. Dugo je bila najuspješnija metoda sve dok nije otkrivena metoda sita polja brojeva 1993. godine. Njen algoritam je još uvijek brži od te metode, ali samo za brojeve s najviše 110 znamenki.

Kvadratno sito je jedna od varijanti metode faktorske baze, gdje se za nju uzima skup

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

gdje je P odabrani broj i $\left(\frac{n}{p}\right)$ Jacobijev simbol. Skup S u kojem tražimo $\mathcal{B}$-brojeve je

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

za neki odabrani A. Brojeve P i A biramo tako da budu reda veličine $L(n) = e^{\sqrt{\ln n \cdot \ln(\ln n)}}$ i da zadovoljavaju nejednakost $P < A < P^2$.

Glavna ideja ove metode je da za svaki $s \in S$, dijeleći ga s prostim brojevima $p \in \mathcal{B}$ provjerimo je li $\mathcal{B}$-broj. Uzimamo jedan po jedan p i ispitujemo djeljivost za sve s. One s-ove koji nisu $\mathcal{B}$-brojevi izbacujemo iz skupa S. Odavde dolazi i naziv "sito", po analogiji s Eratostenovim sitom za generiranje tablice prostih brojeva. Algoritam kvadratnog sita za faktorizaciju neparnog složenog broja n je sljedeći:

1. Odaberimo optimalne P i A.

2. Za $t = \lfloor \sqrt{n} \rfloor + 1, \lfloor \sqrt{n} \rfloor + 2, \lfloor \sqrt{n} \rfloor + 3, ..., \lfloor \sqrt{n} \rfloor + A$ formirajmo stupac brojeva oblika $t^2 - n$.

3. Za svako $p \leqslant P$ provjeravamo da li vrijedi uvjet $\left(\frac{n}{p}\right) = 1$. Ako ne vrijedi, izbacujemo p iz faktorske baze $\mathcal{B}$.

4. Za neparan prost broj p iz $\mathcal{B}$ ($p = 2$ se radi posebno) rješavamo kongruenciju $t^2 \equiv n \pmod{p^\alpha}$, $(\alpha = 1, 2, 3, ...)$. Neka je β najveći α za koji postoji t, $\lfloor \sqrt{n} \rfloor + 1 \leqslant t \leqslant \lfloor \sqrt{n} \rfloor + A$, takav da je $t^2 \equiv n \pmod{p^\beta}$. Neka su t_1 i t_2 dva rješenja od $t^2 \equiv n \pmod{p^\beta}$, takva da je $t_2 \equiv -t_1 \pmod{p^\beta}$. Tako dobiveni t_1 i t_2 nisu nužno iz segmenta $\left[\lfloor \sqrt{n} \rfloor + 1, \lfloor \sqrt{n} \rfloor + A\right]$.

5. Zadržavajući isti p provjeravamo listu brojeva $t^2 - n$ iz 2. koraka. U stupcu ispod p stavimo 1 kod svih vrijednosti $t^2 - n$ kod kojih $p | t - t_1$, promijenimo 1 u 2 ako $p^2 | t - t_1$, promijenimo 2 u 3 ako $p^3 | t - t_1$ i tako sve do p^β, a zatim to isto radimo s $t - t_2$. Najveći broj koji se pojavi u stupcu je β.

6. Svaki put kad u prethodnom koraku stavimo 1 ili izvršimo bilo kakvu promjenu, podijelimo odgovarajući $t^2 - n$ s p i zabilježimo rezultat.

7. U stupcu $p = 2$, ako je $n \not\equiv 1 \pmod 8$, stavimo 1 kod svih $t^2 - n$ u kojima je t neparan, te podijelimo $t^2 - n$ s 2. Ako je $n \equiv 1 \pmod 8$, onda rješavamo kongruenciju $t^2 \equiv n \pmod{2^\beta}$ i radimo sve isto kao za neparne p, osim što će za $\beta \geqslant 3$ biti 4 različita rješenja t_1, t_2, t_3, t_4 modulo 2^β.

8. Kada završimo sa svim prostim brojevima p iz $\mathcal{B}$, odbacimo sve $t^2 - n$, osim onih koji su postali jednaki 1 nakon dijeljenja s potencijama prostih brojeva u prethodna dva koraka. Nakon toga dobit ćemo tablicu u kojoj će jedan stupac sadržavati vrijednosti elemenata $t^2 - n$ koji su $\mathcal{B}$-brojevi, a ostali stupci će sadržavati potencije od $p \in \mathcal{B}$ u rastavu brojeva $t^2 - n$ na proste faktore.

9. Na kraju tražimo relaciju modulo 2 između redaka u dobivenoj matrici p_i-ova, tj. retke čija je suma jednaka nul-vektoru. Množenjem odabranih b_i-ova modulo n dobivamo x, a y dobivamo poloveći potencije p_i-ova u produktu odgovarajućih p-ova modulo n. Tako dobiveni x i y zadovoljavaju kongruenciju $x^2 \equiv y^2 \pmod{n}$. Ako je $x \not\equiv \pm y \pmod{n}$, onda računajući $\operatorname{nzd}(x+y,n)$ dobijemo jedan netrivijalni faktor od n, a drugi računajući $\operatorname{nzd}(x-y,n)$.

Primjer 6. Faktorizirajmo broj $n = 1\,046\,603$ metodom kvadratnog sita.

Rješenje. Kako je $L(n) \approx 418$, uzmimo $P = 80$ i $A = 500$. Pošto je $\lfloor \sqrt{n} \rfloor = 1023$, imamo $1024 \leqslant t \leqslant 1524$. U prvi stupac tablice zapišemo t-ove, a u drugi elemente skupa S, kojeg smo formirali s elementima $t^2 - n$ za svaki t.

Kako je $P = 80$, kandidati za skup $\mathcal{B}$ su sljedeći prosti brojevi

$$\{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79\}.$$

Za $n = 1\,046\,603$ vrijedi

$$\begin{aligned}\left(\frac{n}{3}\right) = \left(\frac{n}{5}\right) = \left(\frac{n}{7}\right) = \left(\frac{n}{11}\right) = \left(\frac{n}{23}\right)\\ = \left(\frac{n}{31}\right) = \left(\frac{n}{43}\right) = \left(\frac{n}{53}\right) = \left(\frac{n}{59}\right)\\ = \left(\frac{n}{61}\right) = \left(\frac{n}{67}\right) = \left(\frac{n}{71}\right) = -1,\\ \left(\frac{n}{13}\right) = \left(\frac{n}{17}\right) = \left(\frac{n}{19}\right) = \left(\frac{n}{29}\right) = \left(\frac{n}{37}\right)\\ = \left(\frac{n}{41}\right) = \left(\frac{n}{47}\right) = \left(\frac{n}{73}\right) = \left(\frac{n}{79}\right) = 1,\end{aligned}$$

pa faktorsku bazu čine sljedeći elementi

$$\mathcal{B} = \{13, 17, 19, 29, 37, 41, 47, 73, 79\} \cup \{2\} = \{2, 13, 17, 19, 29, 37, 41, 47, 73, 79\}.$$

Sada provjeravamo stupac po stupac, za svaki p iz $\mathcal{B}$. Za $p = 2$ stavljamo 1 kod svih neparnih brojeva između 1024 i 1524, jer vrijedi $n \not\equiv 1 \pmod{8}$. Za $p = 13$ opisat ćemo detaljno formiranje stupca. Želimo naći rješenje

$$t_1 = t_{1,0} + t_{1,1} \cdot 13 + t_{1,2} \cdot 13^2 + t_{1,3} \cdot 13^3 + \ldots + t_{1,\beta-1} \cdot 13^{\beta-1}$$

kongruencije $t_1^2 \equiv 1\,046\,603 \pmod{13^\beta}$, gdje je $t_{i,j} \in \{0, 1, 2, \ldots, 12\}$.

Imamo:

$$\begin{aligned}&1\,046\,603 \equiv 12 \pmod{13} \implies t_{1,0}^2 \equiv 12 \pmod{13} \implies t_{1,0} = 5\\ &\qquad \implies t_1 = 5 < 1024, \quad 13^2 - 5 = 164 < 1524,\\ &1\,046\,603 \equiv 155 \pmod{13^2} \implies (5 + 13 \cdot t_{1,1})^2 \equiv 155 \pmod{13^2} \implies t_{1,1} = 1\\ &\qquad \implies t_1 = 5 + 13 = 18 < 1024, \quad 13^3 - 18 = 2179 > 1524,\\ &\implies \beta = 2, \quad t_1 = 18 \equiv 1032 \pmod{13^2}, \quad t_2 = 13^2 - 18 = 151 \equiv 1035 \pmod{13}.\end{aligned}$$

Sada za $p = 13$ konstruiramo sito. Krenuvši od 1032, skačemo za po 13 na dolje do 1024 i na gore do 1524, te svaki put stavimo 1 u stupac i podijelimo odgovarajući $t^2 - n$ s 13. Kad prođemo cijeli stupac ispod $p = 13$, ponavljamo postupak skačući po 13^2, mijenjajući vrijednosti na koje nailazimo (1 u 2, 2 u 3, itd.). Nakon toga ponovimo sve krenuvši u skokove od 1035 umjesto 1032.

Nakon što ovaj postupak primijenimo na preostalih osam brojeva u faktorskoj bazi, dobit ćemo tablicu 501×10 u kojoj redci odgovaraju t-ovima između 1024 i 1524.

Izbacimo li sve one retke gdje je u stupcu $t^2 - n$ ostalo nakon dijeljenja s potencijama od svih p-ova nešto različito od 1, dobivamo sljedeću tablicu u kojoj su svi $t^2 - n$ $\mathcal{B}$-brojevi.

$b_i = t$	$t^2 - n$	2	13	17	19	29	37	41	47	73	79
1030	14 297	–	–	1	–	2	–	–	–	–	–
1282	596 921	–	1	1	–	–	1	–	–	1	–
1319	693 158	1	–	1	1	1	1	–	–	–	–
1370	830 297	–	2	3	–	–	–	–	–	–	–
1435	1 012 622	1	1	1	–	1	–	–	–	–	1
1493	1 182 446	1	–	–	1	2	1	–	–	–	–

U tablici uočavamo da je suma prvog i četvrtog retka jednaka nul-vektoru u $\mathbf{Z}_2^{10}$, pa je

$$x = b_1 \cdot b_4 \bmod 1\,046\,603 = 1030 \cdot 1370 \bmod 1\,046\,603 = 364\,497,$$

$$y = 13^{\frac{2+2}{2}} \cdot 17^{\frac{1+3}{2}} \cdot 29^{\frac{2+0}{2}} \bmod 1\,046\,603 = 13 \cdot 17^2 \cdot 29 \bmod 1\,046\,603 = 108\,953.$$

Kako je $x^2 \equiv y^2 \pmod{n}$ i $x \not\equiv \pm y \pmod{n}$, imamo

$$\text{nzd}\,(x+y, n) = \text{nzd}\,(364\,497 + 108\,953, 1\,046\,603) = \text{nzd}\,(473\,450, 1\,046\,603) = 557,$$

$$\text{nzd}\,(x-y, n) = \text{nzd}\,(364\,497 - 108\,953, 1\,046\,603) = \text{nzd}\,(255\,544, 1\,046\,603) = 1879.$$

Sada je $n = 1\,046\,603 = 557 \cdot 1879$. □

Očekivani broj operacija kod ove metode je $\mathcal{O}\left(e^{(c\sqrt{\ln n \cdot \ln(\ln n)}}\right)$, gdje je konstanta c jednaka $3\sqrt{2}/4$.

Metodom kvadratnog sita je 1994. godine faktoriziran tzv. $RSA - 129$. To je broj od 129 znamenki koji je produkt dva prosta broja od 64 i 65 znamenki.

Trenutno najbolja metoda faktorizacije je *metoda sita polja brojeva*, koja kombinira ideje iz metode kvadratnog sita i algebarsku teoriju brojeva.

Literatura

[1] A. DUJELLA, M. MARETIĆ, *Kriptografija*, Element, Zagreb, 2007.

[2] B. IBRAHIMPAŠIĆ, *Metode faktorizacije*, MFL 4/ 224 (2006), 233–239.

[3] B. IBRAHIMPAŠIĆ, *Matematičke osnove kriptografije javnog ključa*, Magistarski rad, PMF, Sarajevo, 2008.

[4] N. KOBLITZ, *A Course in Number Theory and Cryptography*, Springer – Verlag, New York, 1994.

[5] S. Y. YAN, *Number Theory for Computing*, Springer – Verlag, Berlin, 2002.

[6] V. PETRIČEVIĆ, *Periodski verižni razlomci*, Magistarski rad, PMF, Zagreb, 2009.