Osječki matematički list 23 (2023), 1–11

Neke metode faktorizacije prirodnih brojeva

Maja Andrijević*, Ivan Soldo†

Sažetak

Faktorizacija prirodnih brojeva u praksi može biti vrlo zahtjevna. Jedna od najčešćih primjena je u dešifriranju kriptosustava s javnim ključem, kao što je primjerice RSA kriptosustav. U ovome članku prezentiramo neke od manje poznatih metoda faktorizacije kao što su Fermatova metoda i metoda verižnog razlomka za faktorizaciju velikih prirodnih brojeva.

Ključne riječi: *Fermatova metoda faktorizacije, verižni razlomci, metoda verižnog razlomka*

Some methods of factorization natural numbers

Abstract

Factoring of positive integers can be very demanding in practice. One of the most common applications is the decryption of cryptosystems with a public key, such as the RSA cryptosystem. In this paper, we present some of the less known factorization methods such as the Fermat's method and the continued fraction method for factoring large positive integers.

Keywords: *Fermat's factoring method, continued fractions, continued fraction factoring method*

*Odjel za matematiku, Sveučilište J. J. Strossmayera u Osijeku, email: mandrije@mathos.hr
†Odjel za matematiku, Sveučilište J. J. Strossmayera u Osijeku, email: isoldo@mathos.hr

1 Uvod

Ako prirodni broj n ne prođe neki od testova prostosti (mogu se pogledati primjerice u [2]), onda znamo da je n složen i možemo ga zapisati kao produkt prostih faktora. Međutim, takav način zapisivanja prirodnih brojeva nije uvijek jednostavan. Faktorizacija može biti vrlo složen problem i upravo zbog toga koristi se u različitim kriptosustavima. Primjerice, sigurnost RSA kriptosustava zasnovana je upravo na težini faktorizacije prirodnih brojeva. Više o tome također se može pogledati u [1, 2].

Matematičari su se godinama bavili proučavanjem metoda za faktorizaciju prirodnih brojeva, a neke metode se i dalje proučavaju. U ovom radu pokazat ćemo i primjerima ilustrirati neke algoritme faktorizacije prirodnih brojeva.

Kako bismo mogli lakše pratiti sadržaj rada ponovimo neke osnovne definicije i rezultate teorije brojeva, a ostale zanimljive rezultate može se pronaći u [3].

Definicija 1.1. *Prirodan broj $p > 1$ zove se prost, ako p nema niti jednog djelitelja d sa svojstvom $1 < d < p$. Ako prirodan broj nije prost, onda kažemo da je složen.*

Sljedeći rezultat poznat kao *Osnovni teorem aritmetike* govori nam kako svaki prirodni broj $n \geqslant 2$ možemo zapisati kao produkt potencija prostih brojeva te je moguć samo jedan izbor prostih faktora i pripadnih eksponenata.

Teorem 1.1 (vidjeti [3, Teorem 2.12]). *Svaki prirodni broj $n \geqslant 2$ može se na jedinstven način zapisati u obliku*

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

gdje su $1 < p_1 < p_2 < \cdots < p_k$ prosti brojevi, a $e_1, \ldots, e_k$ prirodni brojevi.

Lako se može pokazati kako svaki složeni prirodni broj n ima prosti faktor $p \leq \sqrt{n}$. Naime, ako je p najmanji djelitelj od n koji je veći od 1, jasno je kako postoji $t \in \mathbb{N}$ sa svojstvom $n = p \cdot t$. Budući je $t \geq p$, odmah slijedi $p \leq \sqrt{n}$. Ovo pravilo možemo primijeniti kod provjere je li neki prirodni broj n prost. Dakle, n pokušamo dijeliti redom s 2, 3, ..., do najviše $\sqrt{n}$. Primjerice, kako bismo zaključili da je 367 prost broj, dovoljno je uvjeriti se da nije djeljiv s prostim brojevima do najviše 19.

Prethodno pravilo možemo upotrijebiti i kod faktorizacije prirodnih brojeva koju smo koristili već u osnovnoj i srednjoj školi. Dakle, kako bismo faktorizirali prirodni broj n i dobili faktorizaciju kao u teoremu 1.1, pokušamo n dijeliti s 2 sve dok je novodobiveni kvocijent paran pa onda s 3 sve

dok je novodobiveni kvocijent djeljiv s 3. Ponavljamo dijeljenje s prostim brojevima p sve do najviše kvadratnog korijena iz zadnjeg novodobivenog kvocijenta. Tako primjerice dobivamo faktorizaciju $54000 = 2^4 \cdot 3^3 \cdot 5^3$. Ovo je najstarija metoda faktorizacije i poznata je kao naivna metoda (probno dijeljenje, eng. trial division). Vidjeli smo kako je algoritam naivne metode lagan za razumjeti i učinkovit je u slučaju da je prirodni broj koji želimo faktorizirati djeljiv s relativno malim prostim brojem. Koliko „malim", ovisi nam o sposobnosti računala. Međutim, vrlo je neučinkovit za faktorizaciju velikih n-ova jer broj operacija dijeljenja može biti vrlo velik. Stoga ćemo u nastavku promotriti i neke druge metode koje nam mogu olakšati faktorizaciju.

2 Fermatova metoda faktorizacije

Fermatova metoda faktorizacije temelji se na sljedećoj činjenici: ako je prirodni broj n produkt dva prirodna broja koji su relativno blizu jedan drugome, onda se n može zapisati kao razlika dva kvadrata od kojih je jedan mali.

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

Propozicija 2.1 (vidjeti [4, Proposition V.3.1.]). *Neka je n neparan prirodan broj takav da je $n = a \cdot b$, gdje je $a > b > 0$. Tada se n može na jedinstven način napisati u obliku $n = t^2 - s^2$, gdje su t i s prirodni brojevi takvi da je*

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

Naime, kako je $n = a \cdot b$, možemo pisati

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

pa imamo traženi prikaz broja n u obliku razlike dva kvadrata.

Obratno, ako je $n = t^2 - s^2 = (t-s)(t+s)$, onda za

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

dobivamo polaznu faktorizaciju $n = a \cdot b$.

Ako je $n = a \cdot b$ i ako su a i b jako blizu, tada je $s = \frac{a-b}{2}$ jako mali broj, a $t = \frac{a+b}{2}$ je malo veći od $\sqrt{n}$. U tom slučaju brojeve a i b možemo naći

tako da za t odabiremo $\lfloor\sqrt{n}\rfloor+1$, $\lfloor\sqrt{n}\rfloor+2$, ... sve dok ne pronađemo takav t za koji je t^2-n potpun kvadrat jednak s^2. Pritom, za realni broj x broj $\lfloor x\rfloor=\max\{m\in\mathbb{Z}: m\leqslant x\}$ zovemo najveći cijeli dio od x ili najveće cijelo od x.

Primjer 2.1. *Neka je* $n=200819$. *Imamo* $t=\lfloor\sqrt{200819}\rfloor+1=449$. *Sada pogledamo je li* $t^2-n=449^2-200819=782$, *potpun kvadrat. Kako to nije istina, pokušajmo s* $t=\lfloor\sqrt{200819}\rfloor+2=450$. *Imamo* $t^2-n=450^2-200819=1681=41^2$ *pa je* $n=200819=450^2-41^2=(450+41)(450-41)=491\cdot 409$.

Ako a i b nisu blizu jedan drugome, onda će Fermatova metoda dati faktorizaciju $n=a\cdot b$, ali nakon više pokušaja za $t=\lfloor\sqrt{n}\rfloor+1,\lfloor\sqrt{n}\rfloor+2,\ldots$.

Primjer 2.2. *Primijenimo li prethodnu metodu na* $n=540143$ *dobili bismo* $t=\lfloor\sqrt{540143}\rfloor+118=852$, *pa je* $s^2=852^2-n=185761=431^2$ *i imamo* $540142=852^2-431^2=(852-431)(852+431)=421\cdot 1283$.

Stoga je razvijena i modifikacija Fermatove metode poznata kao generalizirana Fermatova metoda. Umjesto da tražimo s i t za koje je $n=t^2-s^2$, pokušamo naći brojeve s i t ali takve da $n\mid(t^2-s^2)$ ($s\neq t$, jer je u protivnom $n=0$). Dakle, $t^2\equiv s^2\pmod n$ uz uvjet $t\not\equiv\pm s\pmod n$. Tada imamo $n\mid(t+s)(t-s)$ uz uvjet $n\nmid(t+s)$ ili $n\nmid(t-s)$. Tada su $(t+s,n)$ i $(t-s,n)$ faktori od n. (Napomenimo kako izraz $(\cdot,\cdot)$ označava najvećeg zajedničkog djelitelja dva cijela broja.)

Drugim riječima, tražimo s i t takve da je $t^2-s^2=kn$, $k\in\mathbb{N}$. Tada redom tražimo $t=\lfloor\sqrt{kn}\rfloor+1,\lfloor\sqrt{kn}\rfloor+2,\ldots$ dok ne dobijemo takav t za koji je t^2-kn potpun kvadrat jednak s^2.

U primjeru 2.2 za $k=3$ i $t=\lfloor\sqrt{3n}\rfloor+1=1273$ dobivamo $s=10$. Tada je $(t+s,n)=(1283,540143)=1283$ i faktorizacija je $n=421\cdot 1283$.

Primjer 2.3. *Primjenom prethodno opisanih metoda, faktorizirajmo prirodne brojeve* n, *ako je:*

a) $n=3827$;

b) $n=141467$;

c) $n=154275$.

Rješenje. a) Uzmemo li u modificiranoj Fermatovoj metodi $k=3$ za $t=\left\lfloor\sqrt{3\cdot 3827}\right\rfloor+2=109$ dobijemo $t^2-kn=400=20^2$ pa je $s=20$. Sada je $(t+s,n)=(129,3827)=43$ i tražena faktorizacija je $3827=43\cdot 89$.

b) Analogno, za $k = 3$ i $t = \left\lfloor \sqrt{3 \cdot 141467} \right\rfloor + 4 = 655$ slijedi nam $t^2 - kn = 4624 = 68^2$. Dakle, $s = 68$, $(t + s, n) = (723, 141467) = 241$ i $141467 = 241 \cdot 587$.

c) Primijenimo opet modificiranu Fermatovu metodu. Stavimo li $k = 4$ i $t = \left\lfloor \sqrt{4 \cdot 154275} \right\rfloor + 3 = 788$ imamo $t^2 - kn = 3844 = 62^2$. Stoga je $s = 62$, $(t + s, n) = 425$ te zaključujemo $154275 = 425 \cdot 363$. Uočavamo kako je broj 425 djeljiv s 5 i broj 363 djeljiv je s 3 pa bismo ih dalje mogli faktorizirati i srednjoškolskim metodama te dobiti potpun rastav broja 154275 na proste faktore. Međutim, pogledajmo što bismo dobili primjenom prethodno opisane metode.

Ako je $k = 3$ i $t = \left\lfloor \sqrt{3 \cdot 425} \right\rfloor + 3 = 38$ dobijemo $s = 13$, $(t + s, 425) = 17$ pa je $425 = 17 \cdot 5^2$.

S druge strane, za $k = 5$ i $t = \left\lfloor \sqrt{5 \cdot 363} \right\rfloor + 2 = 44$ slijedi $s = 11$, $(t + s, 363) = 11$ i $363 = 3 \cdot 11^2$.

Prema tome, $154275 = 3 \cdot 17 \cdot 5^2 \cdot 11^2$. ◀

3 Metoda verižnog razlomka

Ova metoda motivirana je prethodno opisanom modifikacijom Fermatove metode. Naziva se još i Brillhart-Morrisonova metoda jer su je Brillhart i Morrison iskoristili za faktorizaciju Fermatovog[1] broja $2^{2^7} + 1$ i dobili

$$2^{2^7} + 1 = 59\,649\,589\,127\,497\,217 \cdot 5\,704\,689\,200\,685\,129\,054\,721.$$

Kako bismo razumjeli samu metodu najprije ćemo se upoznati s osnovnim pojmovima i rezultatima vezanim uz verižne razlomke. Citirat ćemo najvažnije rezultate čiji se dokazi mogu pronaći u predloženoj literaturi.

3.1 Osnovni pojmovi i rezultati teorije verižnih razlomaka

Neka je α proizvoljan realni broj. Stavimo $a_0 = \lfloor \alpha \rfloor$. Ako je $a_0 \neq \alpha$ zapišemo $\alpha = a_0 + \frac{1}{\alpha_1}$, tj. $\alpha_1 = \frac{1}{\alpha - a_0} > 1$ i stavimo $a_1 = \lfloor \alpha_1 \rfloor$. Ako je sada $a_1 \neq \alpha_1$, onda pišemo $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, tj. $\alpha_2 = \frac{1}{\alpha_1 - a_1} > 1$ i analogno stavimo $a_2 = \lfloor \alpha_2 \rfloor$. Taj postupak ponavljamo i on staje ako je za neki $n \in \mathbb{N}$,

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

$a_n = \alpha_n$. Tada je α racionalan broj i pišemo ga u obliku

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

ili kraće, $\alpha = [a_0, a_1, a_2, \ldots, a_n]$, i ovaj izraz nazivamo razvojem broja α u konačni jednostavni verižni razlomak.

Ako je α iracionalan broj, onda uvodimo oznaku

$$\lim_{n\to\infty} [a_0, a_1, a_2, \ldots, a_n] =: [a_0, a_1, a_2, \ldots].$$

Tada se izraz $\alpha = [a_0, a_1, a_2, \ldots]$ zove razvoj broja α u beskonačni jednostavni verižni razlomak.

Pretpostavimo sada da je $a_n \neq \alpha_n$, za sve n. Racionalni broj

$$\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n]$$

zovemo n-ta konvergenta od α. Može se pokazati (npr. [3, Lema 8.13]) kako konvergente $\frac{p_n}{q_n}$ zadovoljavaju rekurzije

$$\begin{aligned} p_0 &= a_0, & q_0 &= 1, \\ p_1 &= a_0 a_1 + 1, & q_1 &= a_1, \\ p_k &= a_k p_{k-1} + p_{k-2}, & q_k &= a_k q_{k-1} + q_{k-2}, \quad k \geq 2. \end{aligned}$$

Definicija 3.1. *Za beskonačni verižni razlomak $[a_0, a_1, a_2, \ldots]$ kažemo da je periodičan ako postoje cijeli brojevi $k \geqslant 0$, $m \geqslant 1$ takvi da je $a_{m+n} = a_n$ za sve $n \geqslant k$. Tada taj verižni razlomak pišemo u obliku*

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

„Crta" iznad brojeva $a_k, \ldots, a_{k+m-1}$ znači da se taj blok brojeva ponavlja unedogled. Najmanji prirodni broj m s ovim svojstvom naziva se duljina perioda.

Euler, 1737. godine i Lagrange, 1770. godine pokazali su da je razvoj u jednostavni verižni razlomak realnog broja α periodičan ako i samo ako je α kvadratna iracionalnost, odnosno, korijen kvadratne jednadžbe s racionalnim koeficijentima (vidjeti [3, Teorem 8.39]). U okviru dokaza ovog rezultata pokazano je da se razvoj kvadratne iracionalnosti $\alpha = \frac{s_0 + \sqrt{n}}{t_0}$, gdje su

n, s_0, t_0 cijeli bojevi, $t_0 \neq 0$, i n nije potpun kvadrat, može dobiti primjenom sljedećeg algoritma:

$$a_i = \left\lfloor \frac{s_i + \sqrt{n}}{t_i} \right\rfloor, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{n - s_{i+1}^2}{t_i}, \quad i \in \mathbb{N}_0. \tag{1}$$

Primjer 3.1. *Odredimo razvoj od $\alpha = \frac{1+\sqrt{13}}{3}$ u jednostavni verižni razlomak.*

Ovdje imamo $s_0 = 1$ i $t_0 = 3$ pa je $a_0 = \left\lfloor \frac{1+\sqrt{13}}{3} \right\rfloor = 1$. Nadalje, primjenom navedenog algoritma dobivamo:

$$s_1 = 2,\ t_1 = 3,\ a_1 = \left\lfloor \frac{2+\sqrt{13}}{3} \right\rfloor = 1,$$
$$s_2 = 1,\ t_2 = 4,\ a_2 = \left\lfloor \frac{1+\sqrt{13}}{4} \right\rfloor = 1,$$
$$s_3 = 3,\ t_3 = 1,\ a_3 = \left\lfloor \frac{3+\sqrt{13}}{1} \right\rfloor = 6,$$
$$s_4 = 3,\ t_4 = 4,\ a_4 = \left\lfloor \frac{3+\sqrt{13}}{4} \right\rfloor = 1,$$
$$s_5 = 1,\ t_5 = 3,\ a_5 = \left\lfloor \frac{1+\sqrt{13}}{4} \right\rfloor = 1,$$
$$s_6 = 2,\ t_6 = 3.$$

Dakle, $\alpha = [1, \overline{1, 1, 6, 1, 1}]$.

Nadalje, ako je $\alpha = \sqrt{n}$, gdje je n prirodan broj koji nije potpun kvadrat, onda je poznato kako je njegov razvoj u jednostavni verižni razlomak periodičan i to oblika

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

gdje je $a_0 = \lfloor \alpha \rfloor$ i vrijedi $a_i = a_{r-i}$ za $i = 1, 2, \ldots, r-1$ (vidjeti [3, Teorem 8.41]).

Primjer 3.2. *Odredimo razvoj od $\alpha = \sqrt{14}$ u jednostavni verižni razlomak. Primjenom navedenoga algoritma dobivamo:*

$$s_0 = 0,\ t_0 = 1,\ a_0 = \left\lfloor \frac{0+\sqrt{14}}{1} \right\rfloor = 3,$$

$$
\begin{aligned}
&s_1 = 3,\ t_1 = 5,\ a_1 = \left\lfloor \frac{3+\sqrt{14}}{5} \right\rfloor = 1,\\
&s_2 = 2,\ t_2 = 2,\ a_2 = \left\lfloor \frac{2+\sqrt{14}}{2} \right\rfloor = 2,\\
&s_3 = 2,\ t_3 = 5,\ a_3 = \left\lfloor \frac{2+\sqrt{14}}{5} \right\rfloor = 1,\\
&s_4 = 3,\ t_4 = 1,\ a_4 = \left\lfloor \frac{3+\sqrt{14}}{1} \right\rfloor = 6,\\
&s_5 = 3,\ t_5 = 5.
\end{aligned}
$$

Dakle, $\alpha = [3, \overline{1,2,1,6}]$.

Primjer 3.3. *Izračunajmo prve tri konvergente u razvoju broja* $\alpha = \sqrt{7}$ *u jednostavni verižni razlomak.*

Najprije odredimo razvoj broja $\alpha = \sqrt{7}$ *u jednostavan verižni razlomak. Dobivamo* $\alpha = [2, \overline{1,1,1,4}]$*, pa su njegove prve tri konvergente:*

$$
\begin{aligned}
&\frac{p_0}{q_0} = 2,\\
&\frac{p_1}{q_1} = 2 + \frac{1}{1} = 3,\\
&\frac{p_2}{q_2} = 2 + \frac{1}{1+\frac{1}{1}} = \frac{5}{2},\\
&\frac{p_3}{q_3} = 2 + \frac{1}{1+\frac{1}{1+\frac{1}{1}}} = \frac{8}{3}.
\end{aligned}
$$

3.2 Faktorizacija prirodnog broja n pomoću metode verižnog razlomka

U prethodnoj točki opisali smo kako se mogu odrediti pripadne konvergente u razvoju realnog broja u jednostavni verižni razlomak. Može se pokazati kako vrijedi i sljedeći rezultat (vidjeti [3, Teorem 10.19]): ako je $\frac{p_i}{q_i}$, $i \geq 0$, i-ta konvergenta razvoja broja $\sqrt{n}$ u jednostavni verižni razlomak, onda vrijedi

$$
p_i^2 - nq_i^2 = (-1)^{i+1} t_{i+1}, \quad 0 < t_i < 2\sqrt{n}, \quad \text{za sve } i \geq -1, \tag{2}
$$

gdje je niz t_i definiran u (1). Ovaj rezultat može se iskoristi pri formiranju metode za faktorizaciju prirodnog broja n koji nije potpun kvadrat.

Ako uvedemo oznaku

$$v_i = (-1)^{i+1} t_{i+1},$$

primjenom (2) zaključujemo kako konvergente verižnog razlomka zadovoljavaju kongruencije

$$p_i^2 \equiv v_i \pmod{n}.$$

Pretpostavimo da smo pronašli produkt $v_{k_1} \cdot v_{k_2} \cdots v_{k_m}$ koji je potpun kvadrat, npr. jednak z^2. Tada smo primjenom (2) pronašli željenu kongruenciju

$$p_{k_1}^2 p_{k_2}^2 \cdots p_{k_m}^2 \equiv z^2 \pmod{n}.$$

Brojevi $(p_{k_1} \cdots p_{k_m} - z, n)$ i $(p_{k_1} \cdots p_{k_m} + z, n)$ su faktori od n. Ako je barem jedan od njih različit od 1 i n, naš zadatak je dovršen. Pogledajmo sada kako to izgleda na primjerima.

Primjer 3.4. *Metodom verižnog razlomka faktorizirajmo sljedeće prirodne brojeve n, ako je:*

a) $n = 55$;

b) $n = 377$;

c) $n = 1643$;

d) $n = 8051$.

Rješenje. a) Najprije odredimo razvoj od $\sqrt{55}$ u jednostavni verižni razlomak. Dobiva se

i	0	1	2	3	4	5
s_i	0	7	5	5	7	7
t_i	1	6	5	6	1	6 ,
a_i	7	2	2	2	14	
p_i	7	15	37	89	1283	

odnosno $\sqrt{55} = [7, \overline{2, 2, 2, 14}]$. Uočimo kako je $v_0 v_2 = (-1)^1 t_1 \cdot (-1)^3 t_3 = 6^2$. Stoga je

$$p_0^2 p_2^2 = (7 \cdot 37)^2 \equiv 259^2 \equiv 39^2 \equiv 6^2 \pmod{55}.$$

Sada računamo

$$(39 + 6, 55) = 5 \quad \text{i} \quad (39 - 6, 55) = 11.$$

Zaista vrijedi $55 = 5 \cdot 11$.

b) Razvijemo li broj $\sqrt{377}$ u jednostavni verižni razlomak, dobivamo:

i	0	1	2	3	4	5
s_i	0	19	13	13	19	19
t_i	1	16	13	16	1	16
a_i	19	2	2	2	38	
p_i	19	39	97	233	8951	

.

Dakle, $\sqrt{377} = [19, \overline{2, 2, 2, 38}]$. Jasno je $v_0 v_2 = (-1)^1 16 \cdot (-1)^3 16 = 16^2$. Dakle,

$$p_0^2 p_2^2 = (19 \cdot 97)^2 \equiv (335)^2 \equiv 16^2 (\text{mod } 377).$$

Sada je $(335 + 16, 377) = 13$ i slijedi $377 = 13 \cdot 29$.

c) Razvojem broja $\sqrt{1643}$ u jednostavni verižni razlomak dobivamo sljedeću tablicu:

i	0	1	2	3	4	5	6	7	8	9
s_i	0	40	3	35	31	31	35	3	40	40
t_i	1	43	38	11	62	11	38	43	1	43
a_i	40	1	1	6	1	6	1	1	80	
p_i	40	41	81	527	608	4175	4783	8958	721423	

.

Prema tome, $\sqrt{1643} = [40, \overline{1, 1, 6, 1, 6, 1, 1, 80}]$. Uočimo kako je $v_2 v_4 = (-1)^3 t_3 \cdot (-1)^5 t_5 = 11^2$, pa imamo:

$$p_2^2 p_4^2 = (81 \cdot 608)^2 \equiv (1601)^2 \equiv 11^2 (\text{mod } 1643).$$

Sada dobivamo $(1601 - 11, 1643) = 53$ i $(1601 + 11, 1643) = 31$ pa je faktorizacija jednaka $1643 = 53 \cdot 31$.

d) Odredimo li razvoj u jednostavan verižni razlomak broja $\sqrt{8051}$ dobivamo tablicu

i	0	1	2	3	4	5	6	7	8	9	10	11
s_i	0	89	41	57	41	89	89	41	57	41	89	89
t_i	1	130	49	98	65	2	65	98	49	130	1	130
a_i	89	1	2	1	2	89	2	1	2	1	178	
p_i	89	90	269	359	987	88202	177391	265593	708577	974170	18058237	

Dakle, $\sqrt{8051} = [89, \overline{1, 2, 1, 2, 89, 2, 1, 2, 1, 178}]$. Budući da je $v_0 v_2 v_3 = (-1)^1 t_1 \cdot (-1)^3 t_3 \cdot (-1)^4 t_4 = 130 \cdot 98 \cdot 65 = 828100 = 910^2$, imamo

$$p_0^2 p_2^2 p_3^2 = (89 \cdot 269 \cdot 359)^2 \equiv 4402^2 (\text{mod } 8051).$$

Prema tome, $(4402 - 910, 8051) = 97$ i $(4402 + 910, 8051) = 83$ pa je tražena faktorizacija $8051 = 97 \cdot 83$. ◀

Analogno primjeru 2.3 c, napomenimo kako se i metoda verižnog razlomka također može uzastopno primjenjivati pri faktorizaciji prirodnog broja koji ima više od dva djelitelja. To ostavljamo čitatelju za samostalnu analizu.

Literatura

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

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

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

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