Природно-математички факултет, Универзитет у Нишу, Србија
http://www.pmf.ni.ac.rs/mii
Математика и информатика 6(1) (2025), 1-38

Верижни разломци у криптографији

Наталија Ранђеловић
Природно-математички факултет, Универзитет у Нишу
natalija.randjelovic1@pmf.edu.rs

Милица З. Колунџија
Природно-математички факултет, Универзитет у Нишу
milica.kolundzija@gmail.com, milica.kolundzija@pmf.edu.rs

Сажетак

Верижне разломке уводимо преко Еуклидовог алгоритма. Користимо их за апроксимацију реалних бројева, за израчунавање децимала броја π и других ирационалних бројева, као и код решавања Диофантових једначина. Идеја која представља основу RSA и Рабин криптосистема је факторизација великих природних бројева на просте чиниоце. Управо због тога посматрамо методу факторизације помоћу верижих разломака. За факторизацију броја n користиће се развој броја $\sqrt{n}$ у верижни разломак. Када желимо да разбијемо неки код, потребно је да то урадимо за неко коначно време, као и да можемо да разбијемо систем произвољне дужине. Да бисмо то урадили потребно је да нађемо оптимално решење, а то ће за RSA и Рабин криптосистеме бити оно решење које убрзава факторизацију бројева. Један од начина оптимализације факторизације су свакако, већ поменути, верижни разломци.

1 Увод

Зачетком верижних разломака сматра се време старогрчког математичара Еуклида и везује се за настанак Еуклидовог алгоритма.

Прве примене верижних разломака у математици уочавамо у решавању линеарних Диофантових једначина у раду индијског математичара *Aryabhata*. Његов рад садржао је примену верижних разломака, али не кроз опште алгоритме, већ само у конкретним примерима.

Модерна теорија верижних разломака почиње у 16. и 17. веку у доба италијанских математичара *R. Bombellia* и *P.Cataldia*. Златно доба за истраживање верижних разломака било је у 19. веку, али још у 18. веку је Ојлер уочио како Еуклидов алгоритам помаже при развоју рационалног броја у верижни разломак. Метода факторизације бројева помоћу верижних разломака нашла је примену у криптосистемима који садрже податке од неколико стотина битова.

Криптосистемима бави се криптографија - наука која проучава методе очувања тајности информација. Проблем прислушкивања се може избећи криптовањем (шифровањем) информација. Постоје симетричан и антисиметричан криптосистем и они користе јавни и/или приватни кључ за шифровање и дешифровање информација. Најпознатији криптосистем са јавним кључем је RSA криптосистем чија сигурност се огледа у немогућности факторизације великих природних бројева.

Прости бројеви који се користе у овом алгоритму углавном садрже неколико стотина цифара. Да бисмо помножили такве бројеве морамо користити посебне алгоритме за множење. За такве операција потребно је више времена, па ови алгоритми могу бити спори. Ипак, уколико користимо неку од напреднијих метода факторизације броја, можемо убрзати алгоритам, смањити његову сложеност и на тај начин пренети жељену информацију. Зато ћемо се у раду фокусирати на криптосистеме конструисане над проблемима факторизације, као и на методу убрзавање исте помоћу верижних разломака. Најпре ћемо се осврнути на теоријску основу верижних разломака и криптосистема конструисаним над проблемима факторизације, а затим на саме методе факторизације.

2 Верижни разломци

У овом одељку дефинисаћемо појам верижног разломка, као и приказати доказе неких особина верижних разломака. Велики део ових резултата може се наћи у раду Д. Ђукића [2], као и у књизи [3].

2.1 Дефиниција и особине

Нека је α реалан број и q_1 највећи цео број који није већи од α. Ако $\alpha \notin \mathbb{Z}$, онда је

$$\alpha = q_1 + \frac{1}{\alpha_1},\ \alpha_1 > 1.$$

Настављајући поступак, у случају да $\alpha_1, \alpha_2, ..., \alpha_k$ нису цели бројеви, добијамо

$$\alpha_1 = q_2 + \frac{1}{\alpha_2},\ \alpha_2 > 1,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots,$$
$$\alpha_{k-1} = q_k + \frac{1}{\alpha_k},\ \alpha_k > 1$$

па је

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{k-1} + \cfrac{1}{\alpha_k}}}}} \quad . \tag{1}$$

Дефиниција 2.1. Кажемо да је реалан број α *разложив у верижни разломак* ако и само ако постоје $q_1, q_2, ..., q_{k-1} \in \mathbb{Z}$, $\alpha_k \in \mathbb{R}$ такви да важи (1).

Постоји и општи верижни разломак који је израз облика $a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cdots}}}$, али, уколико другачије не нагласимо, под појмом верижног разломка подразумеваћемо разломке као у (1).

Ако је α ирационалан број, онда су и $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{R}$ ирационални бројеви па се процес може неограничено настављати.

Ако је α рационалан број представљен у облику нескративог разломка $\frac{a}{b}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, процес је коначан и може бити реализован помоћу Еуклидовог алгоритма. Заиста, из

$$\begin{array}{ll}
a = q_1 b + r_1, & \dfrac{a}{b} = q_1 + \dfrac{1}{\frac{b}{r_1}} \\
b = q_2 r_1 + r_2, & \dfrac{b}{r_1} = q_2 + \dfrac{1}{\frac{r_1}{r_2}} \\
r_1 = q_3 r_2 + r_3, & \dfrac{r_1}{r_2} = q_3 + \dfrac{1}{\frac{r_2}{r_3}} \\
\cdots\cdots\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\cdots\cdots \\
r_{n-2} = q_n r_{n-1} + r_n, & \dfrac{r_{n-2}}{r_{n-1}} = q_n + \dfrac{1}{\frac{r_{n-1}}{r_n}} \\
r_{n-1} = q_{n+1} r_n, & \dfrac{r_{n-1}}{r_n} = q_{n+1}
\end{array}$$

па је

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_n + \cfrac{1}{q_{n+1}}}}}} .$$

Верижни разломак, којим је представљен број $\frac{a}{b}$, означавамо са $[q_1; q_2, ..., q_{n+1}]$. Приметимо, q_1 је цео број, док су бројеви $q_2, ..., q_{n+1}$ природни бројеви.

Дефиниција 2.2. Нека је $[q_1; q_2, ..., q_n]$ верижни разломак за рационалан број $\frac{a}{b}$ и нека $k \in \{1, \dots, n\}$. Тада број q_k називамо *k-ти парцијални количник (k-ти парцијални коефицијент)*, а број $\delta_k = q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}} = [q_1; q_2, \dots, q_k]$, *$k$-тим парцијалним разломком (k-том конвергентом)* полазног верижног разломка. Израз $q'_k = [q_k, q_{k+1}, \dots, q_n]$ називамо *k-тим комплетним количником.*

Пример 2.1. $\frac{45}{16} = [2; 1, 4, 3]$.

Решење. Заиста, из Еуклидовог алгоритма је

$$\begin{aligned} 45 &= 2 \cdot 16 + 13, \\ 16 &= 1 \cdot 13 + 3, \\ 13 &= 4 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 \end{aligned}$$

па је

$$\frac{45}{16} = 2 + \frac{13}{16} = 2 + \frac{1}{\frac{16}{13}} = 2 + \frac{1}{1 + \frac{3}{13}} = 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{3}}}.$$

Одговарајући реципрочан број, $\dfrac{16}{45}$, се може представити у облику верижног разломка $[0; 2, 1, 4, 3]$. $\square$

Важи и обратно, сваки коначан верижни разломак се може приказати у облику разломка па је очигледно следеће тврђење.

Теорема 2.1. *Постоји бијекција између скупа рационалних бројева и коначних верижних разломака.*

Приметимо да се k-ти парцијални разломак δ_k, $k > 1$ верижног разломка $[q_1; q_2, ..., q_n]$ добија из претходног δ_{k-1} заменом количника q_{k-1} са $q_{k-1} + \frac{1}{q_k}$.

Сада можемо доказати следећу теорему која нам даје рекурентну везу за бројиоце и имениоце парцијалних разломака.

Теорема 2.2. *Нека је P_k бројилац и Q_k именилац k-тог парцијалног разломка, тј. $\delta_k = \frac{P_k}{Q_k}$. Тада за низове $\{P_k\}_{k\in\mathbb{N}}$ и $\{Q_k\}_{k\in\mathbb{N}}$, за $k \geq 2$, важи следеће:*

$$\begin{array}{lll} P_0 = 1, & P_1 = q_1 & P_k = q_k P_{k-1} + P_{k-2} \\ Q_0 = 0, & Q_1 = 1 & Q_k = q_k Q_{k-1} + Q_{k-2} \end{array} \tag{2}$$

Доказ. Доказ изводимо индукцијом по $k \geq 2$.

За $k = 2$, важи

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_2 q_1 + 1}{q_2 1 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2}.$$

Нека је тврђење испуњено за k. Докажимо да важи и за $k+1$.
Како δ_{k+1} добијамо када у δ_k заменимо број q_k изразом $q_k+\frac{1}{q_{k+1}}$, то ћемо δ_{k+1} добити када и у формули $\delta_k = \frac{P_k}{Q_k} = \frac{q_kP_{k-1}+P_{k-2}}{q_kQ_{k-1}+Q_{k-2}}$ уместо q_k ставимо $q_k + \frac{1}{q_{k+1}}$. Тада важи

$$\begin{aligned}\frac{P_{k+1}}{Q_{k+1}} &= \delta_{k+1} = \frac{(q_k+\frac{1}{q_{k+1}})P_{k-1}+P_{k-2}}{(q_k+\frac{1}{q_{k+1}})Q_{k-1}+Q_{k-2}} = \frac{(q_kq_{k+1}+1)P_{k-1}+q_{k+1}P_{k-2}}{(q_kq_{k+1}+1)Q_{k-1}+q_{k+1}Q_{k-2}} \\ &= \frac{(q_kq_{k+1}+1)P_{k-1}+q_{k+1}(P_k-q_kP_{k-1})}{(q_kq_{k+1}+1)Q_{k-1}+q_{k+1}(Q_k-q_kQ_{k-1})} = \frac{q_{k+1}P_k+P_{k-1}}{q_{k+1}Q_k+Q_{k-1}},\end{aligned}$$

чиме је доказано да тврђење важи и за $k+1$, па важи и за свако $k \geq 2$. □

Вредност верижног разломка дефинише се као

$$\delta = \lim_{k\to\infty} \delta_k$$

уколико одговарајући лимес постоји. Тада се коначни верижни разломак δ_k назива *к-том апроксимацијом* верижног разломка.

Последица 2.1. *Важи* $[q_1; q_2, \ldots, q_{k-1}, q_k'] = \frac{q_k'P_{k-1}+P_{k-2}}{q_k'Q_{k-1}+Q_{k-2}}$ *за* $k \geq 2$.

Теорема 2.3. *Нека је* $n \in \mathbb{N}$ *и нека је* $[q_1; q_2, \ldots, q_n] = \frac{P_n}{Q_n}$. *Тада је* $[q_n; q_{n-1}, \ldots, q_1] = \frac{P_n}{P_{n-1}}$.

Доказ. Доказ изводимо индукцијом по $n \geq 1$. За $n = 1$ тврђење тривијално важи, тј. $[q_1] = \frac{q_1}{1} = \frac{P_1}{Q_1} = \frac{P_1}{P_0}$. Претпоставимо да тврђење важи за $n-1$, тј. $[q_{n-1}; q_{n-2} \ldots, q_1] = \frac{P_{n-1}}{P_{n-2}}$. Тада, користећи Теорему 2.2, добијамо

$$\begin{aligned}[q_n; q_{n-1}, \ldots, q_1] &= q_n + \frac{1}{[q_{n-1}; q_{n-2}, \ldots, q_1]} = q_n + \frac{P_{n-2}}{P_{n-1}} \\ &= \frac{q_nP_{n-1}+P_{n-2}}{P_{n-1}} = \frac{P_n}{P_{n-1}},\end{aligned}$$

чиме је доказано тврђење за свако $n \geq 1$. □

Посматрајмо, сада, разлику $\delta_k - \delta_{k-1}$, $k > 1$, суседних парцијалних разломака:

$$\delta_k - \delta_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_k Q_{k-1} - Q_k P_{k-1}}{Q_k Q_{k-1}}.$$

Означимо са $h_k = P_k Q_{k-1} - Q_k P_{k-1}$. Заменом P_k и Q_k, као у формулама (2), добијамо

$$\begin{aligned} h_k &= P_k Q_{k-1} - Q_k P_{k-1} \\ &= (q_k P_{k-1} + P_{k-2}) Q_{k-1} - (q_k Q_{k-1} + Q_{k-2}) P_{k-1} \\ &= P_{k-2} Q_{k-1} - Q_{k-2} P_{k-1} = -h_{k-1}. \end{aligned} \tag{3}$$

Одавде, непосредно, следи следеће тврђење.

Теорема 2.4. *Важи*

$$P_k Q_{k-1} - Q_k P_{k-1} = (-1)^k, \quad k \geq 1. \tag{4}$$

Доказ. Доказ индукцијом по k. Нека је $h_k = P_k Q_{k-1} - Q_k P_{k-1}$. За $k = 1$ је

$$h_1 = P_1 Q_0 - Q_1 P_0 = q_1 0 - 1 \cdot 1 = -1 = (-1)^1.$$

Нека је $k > 1$ и тврђење тачно за $k - 1$. Тада, из (3) и индуктивне претпоставке, следи

$$h_k = -h_{k-1} = -(-1)^{k-1} = (-1)^k.$$

□

Теорема 2.5. *Парцијални разломци* $\delta_k = \dfrac{P_k}{Q_k}$, $k \in \mathbb{N}$, *су нескративи.*

Доказ. Из Теореме 2.4 следи да НЗД(P_k, Q_k) дели $(-1)^k$ па је зато НЗД$(P_k, Q_k) = 1$. Дакле, како су конвергенти верижног разломка узајамно прости, то су парцијални разломци $\delta_k = \dfrac{P_k}{Q_k}$, $k \in \mathbb{N}$, нескративи. □

Теорема 2.6. *Важи*

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^k}{Q_k Q_{k-1}}, \qquad k \geq 2.$$

Доказ. Користећи Теорему 2.4 добијамо да важи

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_k Q_{k-1} - Q_k P_{k-1}}{Q_k Q_{k-1}} = \frac{(-1)^k}{Q_k Q_{k-1}}, k \geq 2.$$

□

Приметимо, за парно k разлика $\delta_k - \delta_{k-1}$ је позитивна, а за непарно k негативна. Према (2), Q_k расте па је апсолутна вредност посматране разлике све мања. Отуда је низ $\delta_k = \dfrac{P_k}{Q_k}$, са парним индексима опадајући, а низ са непарним индексима растући. Између њих се као последњи (највећи у растућем поднизу ако је k непаран број и најмањи у опадајућем низу ако је k паран број) налази разломак $\dfrac{a}{b}$.

Пример 2.2. $\frac{79}{38} = [2; 12, 1, 2]$.

Решење. Према (2), $P_1 = 2$, $P_2 = 25$, $P_3 = 27$, $P_4 = 79$, $Q_1 = 1$, $Q_2 = 12$, $Q_3 = 13$, $Q_4 = 38$ па је

$$\frac{2}{1} < \frac{27}{13} < \frac{79}{38} < \frac{25}{12}. \qquad \square$$

Теорема 2.7. *Важи*

$$P_k Q_{k-2} - Q_k P_{k-2} = q_k (-1)^{k-1}, \quad k \geq 2.$$

Такође,

$$\frac{P_k}{Q_k} - \frac{P_{k-2}}{Q_{k-2}} = \frac{(-1)^{k-1} q_k}{Q_k Q_{k-2}}, \quad k \geq 2.$$

Доказ. Користећи Теорему 2 и Теорему 4, добијамо да важи

$$\begin{aligned} P_k Q_{k-2} - Q_k P_{k-2} &= (q_k P_{k-1} - P_{k-2}) Q_{k-2} - (q_k Q_{k-1} - Q_{k-2}) P_{k-2} \\ &= q_k (P_{k-1} Q_{k-2} - Q_{k-1} P_{k-2}) = q_k (-1)^{k-1} \end{aligned}$$

и

$$\frac{P_k}{Q_k} - \frac{P_{k-2}}{Q_{k-2}} = \frac{P_kQ_{k-2} - Q_kP_{k-2}}{Q_kQ_{k-2}} = \frac{q_k(-1)^{k-1}}{Q_kQ_{k-2}}.$$

□

Шта је са ирационалним бројевима? Верижни разломак којим се представља ирационалан број је бесконачан. Ирационални бројеви се, са великом прецизношћу, могу апроксимирати верижним разломцима. На пример, број $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 1, 4, 2, 1, 1, 2, 2, 2, 2, ...]$.

Заокруживањем броја π на четири децимале, 3,1416, правимо сто пута већу грешку него када апроксимирамо број π разломком $[3; 7, 15, 1]$.

Дефиниција 2.3. Бесконачан верижни разломак $[q_1; q_2, q_3, \dots]$ називамо *периодичан верижни разломак* уколико постоји део разломка који се бесконачно пута понавља. Записујемо $[q_1; q_2, \dots, q_k, \overline{q_{k+1}, \dots, q_n}]$ уколико се део $q_{k+1}, \dots, q_n$ понавља бесконачно много пута.

Пример 2.3. Представити $\sqrt{2}$ у облику верижног разломка.

Решење. Из $\sqrt{2} = 1 + a$ следи $2 = (1 + a)^2$ па је $2 = 1 + 2a + a^2$, односно $a(2 + a) = 1$. Тада је

$$a = \frac{1}{2 + a} = \frac{1}{2 + \frac{1}{2+a}} = \frac{1}{2 + \frac{1}{2+\frac{1}{2+\dots}}}$$

па је

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2+\frac{1}{2+\dots}}}.$$

Дакле, $\sqrt{2} = [1; 2, 2, 2, 2, ...] = [1; \overline{2}]$. □

Пример 2.4. Представити $\sqrt{5}$ у облику верижног разломка.

Решење. Нека је $\lfloor\sqrt{5}\rfloor$ највећи цео број који није већи од броја $\sqrt{5}$. Из $\sqrt{5} = \lfloor\sqrt{5}\rfloor + (\sqrt{5} - \lfloor\sqrt{5}\rfloor)$ следи

$$\sqrt{5} = \lfloor\sqrt{5}\rfloor + \frac{1}{\frac{1}{\sqrt{5}-\lfloor\sqrt{5}\rfloor}} = 2 + \frac{1}{\frac{1}{\sqrt{5}-2}} = 2 + \frac{1}{\sqrt{5}+2}$$

па је први парцијални количник $q_1 = \lfloor\sqrt{5}\rfloor = 2$. Затим,

$$q_2 = \lfloor\sqrt{5}+2\rfloor = 4,$$

$$\sqrt{5} = 2 + \frac{1}{4 + \frac{1}{\frac{1}{\sqrt{5}+2-4}}} = 2 + \frac{1}{4 + \frac{1}{\frac{1}{\sqrt{5}-2}}} = 2 + \frac{1}{4 + \frac{1}{2+\sqrt{5}}}.$$

Поступак се наставља на исти начин. Сви наредни парцијални количници су једнаки количнику q_2 па је $\sqrt{5} = [2; 4, 4, 4, ...] = [2; \overline{4}]$. □

2.2 Представљање бројева преко верижних разломака

Рационални бројеви

Представљање рационалног броја верижним разломком је јединствено ако захтевамо да се развој не завршава јединицом.

Уколико допустимо да се развој завршава јединицом, тада постоји још један начин за представљање рационалног броја, као у следећој теореми.

Теорема 2.8. *Сваки рационалан број се може на тачно један начин развити у коначан верижни разломак $[q_1; q_2, \ldots, q_n]$ у коме је $q_n \neq 1$.*

Уколико је дозвољено да последњи члан буде 1, тада постоји још тачно један начин, и то је $[q_1; q_2, \ldots, q_{n-1}, q_n - 1, 1]$.

Доказ. Нека је дат рационалан број $\frac{a}{b}$, $a \in \mathbb{Z}$, $b \in \mathbb{Q}$. Фиксирајмо број a и изведимо доказ трансфинитном индукцијом по b.

За $b = 1$ тврђење је јасно, јер је $\frac{a}{1} = [a]$. Претпоставимо да је $b > 1$ и да је тврђење тачно за све рационалне бројеве са имениоцима мањим од b.

Тада важи $q_1 = \left\lfloor \frac{a}{b} \right\rfloor$, па је

$$\frac{a}{b} = q_1 + \cfrac{1}{\cfrac{b}{a - q_1 b}}.$$

Из Теореме о дељењу са остатком имамо да је $a = q_1 b + r_1$, где је $0 \leq r_1 < b$. Зато следи да је $a - q_1 b < b$, па можемо применити индукцијску претпоставку на разломак $\frac{b}{a-q_1 b}$. Дакле, разломак $\frac{b}{a-q_1 b}$ се може развити у верижни разломак на тачно један, односно два начина, па се и почетни број $\frac{a}{b}$ може развити у верижни разломак на тачно један, односно два начина, чиме је доказано тврђење. □

Теорема 2.9. *Број је рационалан ако и само ако се може представити као коначан верижни разломак.*

Доказ. ($\Leftarrow$:) Докажимо да се сваки коначан верижни разломак може представити као рационалан број. Овај смер доказујемо математичком индукцијом по дужини верижног разломка. Нека је дат коначан верижни разломак $[q_1; q_2, \ldots, q_n]$.

Уочимо да важи $[q_1] = q_1$. Докажимо, сада, базу индукције за $n = 2$:

$$[q_1; q_2] = q_1 + \frac{1}{q_2} = \frac{q_1 q_2 + 1}{q_2}$$

Како је q_1 цео, а q_2 природан број, тврђење важи, односно $\frac{q_1 q_2 + 1}{q_2}$ је рационалан број.

Нека је сада $n > 1$. Претпоставимо да тврђење важи за све верижне разломке дужине $n - 1$. Даље, важи

$$[q_1; q_2, \ldots, q_n] = q_1 + \frac{1}{[q_2; q_3, \ldots, q_n]}.$$

Из индукцијске претпоставке имамо да је $[q_2; q_3, \ldots, q_n]$ рационалан број и нека је $[q_2; q_3, \ldots, q_n] = \frac{a}{b}$. Тада је

$$[q_1; q_2, \ldots, q_n] = q_1 + \frac{1}{\frac{a}{b}} = q_1 + \frac{b}{a} = \frac{q_1 a + b}{a}$$

чиме смо доказали да је и верижни разломак $[q_1; q_2, \ldots, q_n]$ рационалан број. Тиме је доказан индукцијски корак, па је и тврђење доказано.

($\Rightarrow$:) Докажимо, сада, да се сваки рационалан број може представити као коначан верижни разломак. Претпоставимо да је $\frac{a}{b}$ рационалан број, где је $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Математичком индукцијом по b доказаћемо да се $\frac{a}{b}$ може записати као коначан верижни разломак. Најпре, покажимо базу индукције. За $b = 1$ важи

$$\frac{a}{b} = \frac{a}{1} = a = [a]$$

Претпоставимо да се сваки рационалан број чији је именилац мањи од b може приказати као коначан верижни разломак. Из Теореме о дељењу са остатком можемо закључити да постоје цели бројеви q_1 и r, $0 \leq r < b$, за које важи

$$a = bq_1 + r.$$

Када једнакост $a = bq_1 + r$ поделимо са b, добићемо

$$\frac{a}{b} = q_1 + \frac{r}{b}.$$

Ако је $r = 0$, тада је $\frac{a}{b} = q_1 = [q_1]$ и тврђење важи. Ако је $r \neq 0$, онда је

$$\frac{a}{b} = q_1 + \frac{1}{\frac{b}{r}}.$$

Како је $r < b$, можемо искористити индукцијску претпоставку за $\frac{b}{r}$, тј. за неке природне бројеве $q_2, q_3, \ldots, q_n$ важи

$$\frac{b}{r} = [q_2; q_3, \ldots, q_n].$$

Тада је

$$\frac{a}{b} = q_1 + \frac{1}{[q_2; q_3, \ldots, q_n]} = [q_1; q_2, q_3, \ldots, q_n]$$

што је и требало доказати. □

Користећи везу међу бројиоцима и имениоцима узастопних парцијалних разломака доказану у Теореми 4, као и чињеницу доказану у Теореми 2.8 да постоје тачно два представљања рационалног броја у верижни разломак, при чему се њихове дужине разликују за 1, може се доказати следећа теорема.

Теорема 2.10. *Нека су a, b, c и d природни бројеви такви да је $|ad - bc| = 1$ и $b > d$, и ако је*

$$\frac{a}{b} = [q_1; q_2, \ldots, q_n] = [q_1; q_2, \ldots, q_n - 1, 1], \quad (q_n > 1)$$

онда је

$$\frac{c}{d} = [q_1; q_2, \ldots, q_{n-1}] \qquad и \qquad ad - bc = (-1)^n,$$

или

$$\frac{c}{d} = [q_1; q_2, \ldots, q_{n-1}, q_n - 1] \qquad и \qquad ad - bc = (-1)^{n+1}.$$

Ирационални бројеви

Теорема 2.11. *Ирационалан број је решење квадратне једначине са целобројним коефицијентима ако и само ако се може представити као периодаичан верижни разломак.*

Доказ. ($\Leftarrow$:) Докажимо да ако ирационалан број можемо представити као периодичан верижни разломак, тада је он решење квадратне једначине.

Претпоставимо да је $x = [q_1; q_2, \ldots, q_m, \overline{q_{m+1}, \ldots, q_n}]$, са периодом $q_{m+1}, \ldots, q_n$. Тада је $q'_{m+1} = q'_{n+1}$, па на основу Последице 2.1 имамо да важи

$$\begin{aligned} x &= \left[q_1, \ldots, q_m, q'_{m+1}\right] = \frac{q'_{m+1}P_m + P_{m-1}}{q'_{m+1}Q_m + Q_{m-1}} \\ &= \left[q_1, \ldots, q_m, \ldots, q_n, q'_{m+1}\right] = \frac{q'_{m+1}P_n + P_{n-1}}{q'_{m+1}Q_n + Q_{n-1}}. \end{aligned}$$

Одавде је $-q'_{m+1} = \frac{P_{m-1} - Q_{m-1}x}{P_m - Q_m x} = \frac{P_{n-1} - Q_{n-1}x}{P_n - Q_n x}$, и множењем последње једнакости добијамо квадратну једначину са целобројним коефицијентима по x:

$$\begin{aligned} &(Q_{m-1}Q_n - Q_{n-1}Q_m)\, x^2 - (P_{m-1}Q_n + P_m Q_{n-1} - P_n Q_{m-1} - P_{n-1}Q_m)\, x \\ &\quad + (P_{m-1}P_n - P_{n-1}P_m) = 0. \end{aligned}$$

($\Rightarrow$:) Докажимо сада други смер, односно да је ирационалан број решење квадратне једначине са целобројним коефицијентима ако се може приказати као периодичан верижни разломак.

Нека је $x = [q_1; q_2, \ldots]$ решење квадратне једначине $P(x) = ax^2 + bx + c = 0$ са целобројним коефицијентима a, b, c. За свако $n \in \mathbb{N}$ важи

$$x = \left[q_1; q_2, \ldots, q_n, q'_{n+1}\right] = \frac{q'_{n+1}P_n + P_{n-1}}{q'_{n+1}Q_n + Q_{n-1}},$$

одакле добијамо да q'_{n+1} задовољава квадратну једначину

$$f_n\left(q'_{n+1}\right) = A_n q'^2_{n+1} + B_n q'_{n+1} + C_n = 0,$$

где је

$$\begin{aligned} A_n &= aP_n^2 + bP_nQ_n + cQ_n^2, \\ B_n &= 2aP_nP_{n-1} + b\left(P_nQ_{n-1} + P_{n-1}Q_n\right) + 2cQ_nQ_{n-1}, \\ C_n &= aP_{n-1}^2 + bP_{n-1}Q_{n-1} + cQ_{n-1}^2. \end{aligned}$$

Проценимо сада коефицијенте A_n, B_n, C_n. Ако ставимо $P(t) = a(t - x)(t - y)$ (где је $y = -\frac{b}{a} - x$ такође ирационалан број), тада важи

$$A_n = Q_n^2 P\left(\frac{P_n}{Q_n}\right) = aQ_n^2\left(\frac{P_n}{Q_n} - x\right)\left(\frac{P_n}{Q_n} + \frac{b}{a} + x\right),$$

па је

$$|A_n| < |a|Q_n^2\frac{1}{Q_n^2}\left(2|x| + \left|\frac{b}{a}\right| + 1\right) = 2|x||a| + |b| + |a|.$$

Аналогно је $|C_n| < 2|x||a| + |b| + |a|$. Даље, директним множењем и коришћењем Теореме 4, лако се проверава да је $B_n^2 - 4A_nC_n = (b^2 - 4ac)\left(P_nQ_{n-1} - Q_nP_{n-1}\right)^2 = b^2 - 4ac$, одакле је $|B_n|^2 \leq 4|A_n||C_n| + |b^2 - 4ac|$, па је $|B_n| \leq \sqrt{4|A_n||C_n| + |b^2 - 4ac|}$.

Према томе, за сваки од коефицијената A_n, B_n, C_n, па тако и за полином f_n, има само коначно много могућности, па за неке различите k, m, n важи $f_k = f_m = f_n$. То значи да су q'_{k+1}, q'_{m+1} и q'_{n+1} нуле истог квадратног полинома, па су неке две исте. Нека је без губљења општости $q'_{m+1} = q'_{n+1}$, развој броја x у верижни разломак је исти после m-тог и после n-тог места, тј. периодичан је. □

Последица 2.2. $[\overline{q_1; q_2, \ldots, q_n}] = \frac{P_n - Q_{n-1} \pm \sqrt{(P_n + Q_{n-1})^2 + 4(-1)^n}}{2Q_n}$.

Доказ. Нека је $x = [\overline{q_1; q_2, \ldots, q_n}]$, тада је $x = q_1' = q_{n+1}'$, па је

$$x = [q_1; q_2, \ldots, q_n, q_{n+1}'] = \frac{xP_n + P_{n-1}}{xQ_n + Q_{n-1}},$$

чиме смо добили квадратну једначину по x: $Q_n x^2 - (P_n - Q_{n-1})x - P_{n-1} = 0$. Решавањем добијене квадратне једначине, уз коришћење Теореме 4, налазимо да су решења једнака $\frac{P_n - Q_{n-1} \pm \sqrt{(P_n + Q_{n-1})^2 + 4(-1)^n}}{2Q_n}$, што је и требало доказати. □

Теорема 2.12. *Нека за природне бројеве a, b, c, d и реалан број $t > 1$ важи $b > d$, $|ad - bc| = 1$ и нека је $x = \dfrac{ta + c}{tb + d}$. Тада су $\dfrac{a}{b}$ и $\dfrac{c}{d}$ узастопни парцијални разломци броја x.*

Доказ. Нека је $\dfrac{a}{b} = [q_1; q_2, \ldots, q_n]$. Из Теореме 2.10 закључујемо да постоји n такво да је $(-1)^n = ad - bc$ и $\dfrac{c}{d} = [q_1; q_2, \ldots, q_{n-1}]$.

Знамо да се x може представити као $x = \dfrac{ta + c}{tb + d} = [q_1; q_2, \ldots, q_n, t]$. Како је $t > 1$, можемо га развити у верижни разломак, и то нека је $t = [q_{n+1}; q_{n+2}, \ldots]$ ($q_{n+1} \geq 1$). Тада имамо развој $x = [q_1; q_2, \ldots, q_n, q_{n+1}, \ldots]$ и у њему су узастопни парцијални разломци $\dfrac{P_n}{Q_n}$ и $\dfrac{P_{n-1}}{Q_{n-1}}$ управо једнаки $\dfrac{a}{b}$ и $\dfrac{c}{d}$. □

Теорема 2.13. *Нека је $x \in \mathbb{R}$ и нека разломак $\dfrac{a}{b}$ такав да је $\left|\dfrac{a}{b} - x\right| < \dfrac{1}{2b^2}$. Тада је $\dfrac{a}{b}$ парцијални разломак за x.*

Доказ. Развијмо $\dfrac{a}{b}$ у верижни разломак $[q_1; q_2, \ldots, q_n]$. Из Теореме 2.10 закључујемо да можемо подесити парност броја n тако да $(-1)^n \left(\dfrac{a}{b} - x\right)$ буде позитивно.

Означимо са $\dfrac{P_n}{Q_n} = \dfrac{a}{b}$ и $\dfrac{P_{n-1}}{Q_{n-1}}$ парцијалне разломке за $\dfrac{a}{b}$. Нека је x облика $x = \dfrac{tP_n + P_{n-1}}{tQ_n + Q_{n-1}}$.

Ако је $t > 1$, из Теореме 2.12 следи да су $\dfrac{P_n}{Q_n}$ и $\dfrac{P_{n-1}}{Q_{n-1}}$ парцијални разломци за x.

Заиста,

$$\begin{aligned}\frac{1}{2Q_n^2} &> (-1)^n\left(\frac{a}{b}-x\right) = (-1)^n\frac{P_nQ_{n-1}-P_{n-1}Q_n}{Q_n\left(tQ_n+Q_{n-1}\right)} = \frac{1}{Q_n\left(tQ_n+Q_{n-1}\right)}\\ &> \frac{1}{(t+1)Q_n^2},\end{aligned}$$

па је $t+1>2$, тј. $t>1$. □

Теорема 2.14. *За сваки природан број d који није квадрат, развој $\sqrt{d}$ у верижни разломак је облика $\left[q_1;\overline{q_2,q_3,q_4,\ldots,q_4,q_3,q_2,2q_1}\right]$. За свако n важи $q_n \le 2q_1 = 2\lfloor\sqrt{d}\rfloor$, при чему је $q_n = 2\lfloor\sqrt{d}\rfloor$ ако и само ако је $\left|P_{n-1}^2 - dQ_{n-1}^2\right| = 1$.*

Доказ. Нека је $\sqrt{d} = [q_1; q_2, q_3, \ldots]$. Ако је $[q_1; q_2, \ldots, q_k] = \frac{P_k}{Q_k}$, важи

$$\begin{aligned}q_{n+1} &< q'_{n+1} = \frac{q'_{n+1}Q_n + Q_{n-1} - Q_{n-1}}{Q_n} < \frac{q'_{n+1}Q_n + Q_{n-1}}{Q_n}\\ &= \frac{1}{Q_n\left(P_n - Q_n\sqrt{d}\right)} = \frac{1}{P_n^2 - dQ_n^2}\left(\frac{P_n}{Q_n} + \sqrt{d}\right)\\ &< \frac{1}{P_n^2 - dQ_n^2}(2\lfloor\sqrt{d}\rfloor + 2).\end{aligned}$$

Специјално, ако је $|P_n^2 - dQ_n^2| > 1$, важи $q_{n+1} < 2\lfloor\sqrt{d}\rfloor$.

Како Пелова једначина $x^2 - dy^2 = 1$ има бесконачно много решења (x, y) у скупу природних бројева, таква је и једначина $|x^2 - dy^2| = 1$. Свако решење (x, y) задовољава

$$\left|\frac{x}{y} - \sqrt{d}\right| = \frac{1}{y}|x - y\sqrt{d}| = \frac{1}{y(x + y\sqrt{d})} < \frac{1}{2y^2},$$

па је, према Теореми 2.13, $\frac{x}{y}$ конвергент за $\sqrt{d}$, тј. $\frac{x}{y} = [q_1; q_2, \ldots, q_n] = \frac{P_n}{Q_n}$ за неко n. Осим тога, тада је $P_n^2 - dQ_n^2 = \pm 1$ истог знака као $\frac{P_n}{Q_n} - \sqrt{d}$, па из Теореме 2.6 имамо $P_n^2 - dQ_n^2 = (-1)^n$.

Како бисмо доказали да верижни разломак за развој броја $\sqrt{d}$ има периоду $q_2, q_3, \ldots, q_3, q_2, 2q_1$, тј. да елементи периоде без последњег чине палиндром а да је последњи једнак $2q_1$, потребно је доказати $[q_1; \ldots, q_n] = [q_n; \ldots, q_1]$ и $q_{n+1} = 2q_1$.

Имамо да је $[q_2, \ldots, q_n] = \frac{Q_n}{P_n - q_1 Q_n}$ и $[q_2, \ldots, q_{n-1}] = \frac{Q_{n-1}}{P_{n-1} - q_1 Q_{n-1}}$. Из Теореме 2.3 закључујемо да важи $[q_n, \ldots, q_2] = \frac{Q_n}{Q_{n-1}}$. Дакле, довољно је доказати да је $Q_{n-1} = P_n - q_1 Q_n$.

Најпре, уочимо да важи $Q_n > P_n - q_1 Q_n$ јер је $\frac{Q_n}{P_n - q_1 Q_n} > 1$ и важи $|P_n (P_n - q_1 Q_n) - Q_n (dQ_n - q_1 P_n)| = |P_n^2 - dQ_n^2| = 1$.

Одредимо број t за који је $\frac{tP_n + (dQ_n - q_1 P_n)}{tQ_n + (P_n - q_1 Q_n)} = \sqrt{d}$. Како је ова једнакост еквивалентна са

$$\begin{aligned} t\left(P_n - Q_n\sqrt{d}\right) &= \left(q_1 + \sqrt{d}\right) P_n - \left(q_1\sqrt{d} + d\right) Q_n \\ &= \left(q_1 + \sqrt{d}\right)\left(P_n - Q_n\sqrt{d}\right), \end{aligned}$$

добијамо $t = q_1 + \sqrt{d} > 1$. Како су испуњене све претпоставке из Теореме 2.12, следи да су $\frac{dQ_n - q_1 P_n}{P_n - q_1 Q_n}$ и $\frac{P_n}{Q_n}$ узастопни парцијални разломци за $\sqrt{d}$. Одатле, даље, имамо да је $\frac{dQ_n - q_1 P_n}{P_n - q_1 Q_n} = \frac{P_{n-1}}{Q_{n-1}}$, а како су парцијални разломци нескративи, следи да је $Q_{n-1} = P_n - q_1 Q_n$. Дакле, $[q_1; \ldots, q_n] = [q_n; \ldots, q_1]$.

Сада је из Последице 2.2

$$\left[\overline{2q_1, q_2, \ldots, q_2}\right] = \frac{P_n + q_1 Q_n - Q_{n-1} - \sqrt{\left(P_n + q_1 Q_n + Q_{n-1}\right)^2 + 4(-1)^n}}{2Q_n}.$$

Како је $Q_{n-1} = P_n - q_1 Q_n$ и $P_n^2 + (-1)^n = dQ_n^2$, тада је $\left[\overline{2q_1, q_2, \ldots, q_2}\right] = \frac{q_1 Q_n + \sqrt{P_n^2 + (-1)^n}}{Q_n} = q_1 + \sqrt{d}$.

Дакле, следи да је $\left[q_1; \overline{q_2, q_3, \ldots, q_2, 2q_1}\right] = \sqrt{d}$ и $q_{n+1} = 2q_1$. □

Пример 2.5. Упоредити верижне разломке квадратних корена бројева 1234 и 2024.

Решење. Бројеви 1234 и 2024 нису квадратни корени ни једног броја. Ипак, њих можемо представити на суштински другачији начин, па ће и њихови развоји у верижне разломке бити другачијег типа - број $\sqrt{1234}$ има развој у бесконачан верижни разломак, док број $\sqrt{2024}$ има бесконачан, али периодичан развој у верижни разломак. За број $\sqrt{2024}$ можемо применити и Теорему 2.14.

Како је $\lfloor\sqrt{1234}\rfloor = 35$, то је $q_1 = 35$, односно како је $\lfloor\sqrt{2024}\rfloor = 44$, то је у том случају $q_1 = 44$. Након рачунања свих конвергената добијамо следеће развоје:

$\sqrt{1234}$ =[35; 7, 1, 3, 1, 4, 4, 2, 9, 1, 1, 2, 3, 1, 1, 34, 1, 1, 3, 2, 1, 1, 9, 2, 4, 4, 1, ...]

$\sqrt{2024} = [44; \overline{1, 88}]$

Разлог зашто се број $\sqrt{2024}$ могао представити преко периодичног верижног разломка, а број $\sqrt{1234}$ не, је зато што се број 2024 може представити као $2024 = 45 \cdot 45 - 1 = 4 \cdot 506$, тј. имамо Пелову једначину $45^2 - 506 \cdot 2^2 = 1$, а број 1234 не можемо представити на тај начин. □

Последица 2.3. *Уређени пар природних бројева (x, y) је решење једначине $|x^2 - dy^2| = 1$ ако и само ако је, за неко $n \in \mathbb{N}$, разломак $\frac{x}{y}$ n-ти парцијални разломак за $\sqrt{d} = [q_1; q_2, \ldots]$ и $q_{n+1} = 2\lfloor\sqrt{d}\rfloor$. При томе је $x^2 - dy^2 = (-1)^{n-1}$.*

Последица 2.4. *Једначина $x^2 - dy^2 = -1$ има целобројна решења ако и само ако верижни разломак за $\sqrt{d}$ има период непарне дужине.*

2.3 Алгоритам за рачунање верижних разломака

Вредност верижних разломака није практично израчунавати применом дефиниције, јер би се такво рачунање обављало са десне на леву страну. То би значило да се дубина израчунавања мора одредити унапред.

Ојлеров алгоритам представља бољи начин за рачунање вредности верижних разломака $\delta_k = \dfrac{P_k}{Q_k}$. То је алгоритам где се те вредности рачунају применом рекурентних израза из Теореме 2.2. За овај приступ није потребно познавање дубине израчунавања унапред, али директна примена израза из Теореме 2.2 доводи до тога да вредности P_k и Q_k буду или веома мале или веома велике. То може довести до поткорачења или прекорачења у аритметици покретног зареза.

Ове проблеме решава *модификовани Ленцов алгоритам за верижне разломке*.

Algorithm 1: Модификовани Ленцов алгоритам

Input: Вредности a_k, b_k тачност израчунавања ε, као и вредност $\delta > 0$

$R_0 := a_0$
if $a_0 = 0$ **then**
  $R_0 := \delta$
else
  if $|a_0| < \delta$ **then**
    $R_0 := \delta \cdot \operatorname{sign} a_0$
  end
end
$C_0 := R_0, D_0 := 0, \Delta_0 := +\infty, k := 0$
while $|\Delta_k - 1| \geq \varepsilon$ **do**
  $k := k + 1$
  $C_k := a_k + b_k / C_{k-1}$
  if $C_k = 0$ **then**
    $C_k := \delta$
  else
    if $|C_k| < \delta$ **then**
      $C_k := \delta \cdot \operatorname{sign} C_k$
    end
  end
  $D_k := a_k + b_k D_{k-1}$
  if $D_k = 0$ **then**
    $D_k := \delta$
  else
    if $|D_k| < \delta$ **then**
      $D_k := \delta \cdot \operatorname{sign} D_k$
    end
  end
  $D_k := 1/D_k, \Delta_k := C_k D_k, R_k := R_{k-1} \Delta_k$
end
return R_k

Пример 2.6. Рачунање вредности броја e.

Решење. Овом проблему приступићемо на два начина - преко Тејлоровог реда и преко верижних разломака.

Број e можемо представити преко верижног разломка као

$$e = \left[2; \frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{4}{3}, \dots\right]$$

где је $a_0 = 2$, $a_k = k (k \in \mathbb{N})$, $b_1 = 1$, $b_k = k - 1 (k \geq 2)$.

k	e_k^s	e_k^{cj}	Δ_k^s	Δ_k^{cf}
1	2.0000000000	3.0000000000	7.18e − 001	2.81e − 001
2	2.5000000000	2.6666666667	2.18e − 001	5.16e − 002
3	2.6666666667	2.7272727273	5.16e − 002	8.99e − 003
4	2.7083333333	2.7169811321	9.94e − 003	1.30e − 003
5	2.7166666667	2.7184466019	1.61e − 003	1.64e − 004
6	2.7180555556	2.7182633318	2.26e − 004	1.84e − 005
7	2.7182539683	2.7182836939	2.78e − 005	1.86e − 006
8	2.7182787698	2.7182816577	3.05e − 006	1.70e − 007
9	2.7182815256	2.7182818428	3.02e − 007	1.43e − 008
10	2.7182818011	2.7182818274	2.73e − 008	1.10e − 009
11	2.7182818262	2.7182818285	2.26e − 009	7.94e − 011
12	2.7182818283	2.7182818285	1.72e − 010	5.31e − 012
13	2.7182818284	2.7182818285	1.22e − 011	3.34e − 013
14	2.7182818285	2.7182818285	8.14e − 013	1.90e − 014
15	2.7182818285	2.7182818285	5.01e − 014	2.22e − 015

Табела 1: Вредности броја e добијене помоћу Тејлоровог реда и верижног разломка, као и одговарајуће апсолутне грешке.

У Табели 1 су дате вредности e_k^s и e_k^{cf}, као и грешке $\Delta_k^s = |e_k^s - e|$ и $\Delta_k^{cf} = \left|e_k^{cf} - e\right|$ израчунавања броја e помоћу Тејлоровог развоја броја e^x за $x = 1$ и одговарајућег облика верижног разломка.

Можемо приметити да применом верижног разломка добијамо готово за цео ред величине већу тачност него сумирањем реда. За $k = 30$

ова разлика је 3 реда величине. Тејлоров развој функције e^x за $x = 1$ веома брзо конвергира, па би у случају примене неког споријег реда, резултати били још погоднији за верижне разломке. □

Пример 2.7. Број π.

Решење. Број π можемо представити преко верижног разломка као

$$\pi = \left[\frac{4}{1}, \frac{1^2}{2}, \frac{3^2}{2}, \frac{5^2}{2}, \ldots\right] = \left[3; \frac{1^2}{6}, \frac{3^2}{6}, \frac{5^2}{6}, \frac{7^2}{6}, \ldots\right] = \left[\frac{4}{1}, \frac{1^2}{3}, \frac{2^2}{5}, \frac{3^2}{7}, \ldots\right]$$

3 Диофантове једначине

Диофантова једначина је једначина облика

$$f(x_1, \ldots, x_k) = 0$$

где је f полином (од k променљивих $x_1, \ldots, x_k$) са целим коефицијентима, чија решења тражимо искључиво у скупу целих бројева. Не постоји алгоритам који би за сваку Диофантову једначину одлучивао да ли она има решења. Диофантове једначине могу бити линеарне и нелинеарне.

Дефиниција 3.1. Једначину $ax + bz = c$, где су a, b и c цели бројеви и $a \neq 0$, $b \neq 0$, називамо *линеарна Диофанова једначина*. Бројеви x и y који задовољавају једначину називају се решења једначине.

Пример нелинеарних диофантских једначина који користи методу верижног разломка су Пелове једначине.

Дефиниција 3.2. Нека је m позитиван цео број који није потпун квадрат. Тада је Пелова једначина једначина облика

$$x^2 - my^2 = 1.$$

Тривијална решења сваке Пелове једначине су $x = \pm 1$, $y = 0$, док су сва друга решења нетривијална.

Код решавања неких Диофантових једначина јављају се парцијални разломци, док њихова важност долази до изражаја при решавању Пелових једначина. То су једначине облика $x^2 - dy^2 = 1$, где је d природан број који није потпун квадрат.

Уз ову једначину анализира се и једначина $x^2 - dy^2 = -1$. Означимо конвергенте у развоју верижног разломка броја $\sqrt{d}$ са $\frac{P_k}{Q_k}$. Тада важи

$$P_k^2 - dQ_k^2 = (-1)^{k+1} t_{k+1},$$

где је низ $\{t_k\}_{k \in \mathbb{N}}$ дефинисан у алгоритму за развој броја $\sqrt{d}$ у верижни разломак.

Одавде можемо закључити да једначина $x^2 - dy^2 = 1$ увек има (бесконачно) решења у скупу природних бројева, док једначина $x^2 - dy^2 = -1$ има решења ако и само ако је дужина периода r у развоју од $\sqrt{d}$ непарна. Ако је (X, Y) најмање решење у скупу природних бројева једначине $x^2 - dy^2 = 1$, онда је $(X, Y) = (P_{r-1}, Q_{r-1})$ или (P_{2r-1}, Q_{2r-1}) у зависности од тога да ли је дужина периода r парна или непарна.

4 Криптографија јавног кључа

4.1 Увод у криптографију

Криптографија проучава методе за успешан пренос информација преко несигурног комуникацијског канала.

Поруку коју пошиљалац жели послати примаоцу зовемо отворени текст. Пошиљалац отворени текст, најпре, промени користећи договорени кључ. Тај поступак зове се шифровање, а добијени резултат шифрат. Након тога пошиљалац пошаље шифрат преко неког комуникацијског канала. Противник прислушкујући може сазнати садржај шифрата, али како не зна кључ, не може одредити отворени текст. За разлику од њега, прималац зна кључ којим је шифрирана порука, па може дешифровати шифрат и одредити отворени текст.

Шифровање се може извршити помоћу јавног и приватног кључа у зависности од тога на који начин желимо пренети информацију и омогућити њено дешифровање.

Дефиниција 4.1. Криптосистем је уређена петорка $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, где је $\mathcal{P}$ коначан скуп свих отворених текстова, $\mathcal{C}$ коначан скуп свих шифрата, $\mathcal{K}$ коначан скуп свих могућих кључева, $\mathcal{E}$ скуп свих функција шифровања и $\mathcal{D}$ скуп свих функција дешифровања. За сваки $K \in \mathcal{K}$ постоји $e_K \in \mathcal{E}$ и одговарајући $d_K \in \mathcal{D}$. Притом су $e_K : \mathcal{P} \to \mathcal{C}$ и $d_K : \mathcal{C} \to \mathcal{P}$ функције са својством да је $d_K(e_K(x)) = x$ за сваки $x \in \mathcal{P}$.

Функције које се користе за шифровање e_K и дешифровање d_K зависе од кључа K који се мора разменити пре комуникације. Тада се уочава нови проблем: Како разменити кључ, уколико не постоји безбедан комуникацијски канал?

Идеја јавног кључа се састоји у томе да се конструишу криптосистеми код којих би из познавања функције шифровања e_K било немогуће у реалном времену израчунати функцију дешифровања d_K. Дакле, у криптосистему са јавним кључем сваки корисник K има два кључа: јавни e_K и тајни d_K. Пошиљалац шифрује отворени текст помоћу јавног кључа примаоца e_B, тј. примаоцу шаље шифрат $y = e_B(x)$. Прималац тада дешифрује шифрат користећи свој тајни кључ d_B, $d_B(y) = d_B(e_B(x)) = x$. Такође, прималац мора имати неку додатну информацију, односно скривени улаз (trapdoor), о функцији e_B, да би само он могао израчунати њен инверз d_B, док је свима другима то немогуће. Такве функције чији је инверз тешко израчунати без познавања неког додатног податка зову се хеш функције.

Криптосистеми са јавним кључем су спорији од модерних симетричних криптосистема (DES, IDEA, AES), па се у пракси не користе за шифровање порука, већ за шифровање кључева, који се потом користе у комуникацији помоћу неког симетричног криптосистема.

Криптосистеме са јавним кључем, такође, користимо када желимо да "дигитално потпишемо" поруку. Односно, ако пошиљалац пошаље

шифрат $z = d_A(e_B(x))$, онда прималац може бити сигуран да је поруку послала права особа (јер само она зна функцију d_A), а такође то показује и једнакост $e_A(z) = e_B(x)$.

4.2 Криптосистеми засновани на проблему факторизације

Криптосистеми са јавним кључем и хеш функцијама обично су конструисани над математичким проблемима велике сложености, а један од познатих и често примењиваних проблема је проблем факторизације великих природних бројева.

Најпознатији криптосистем са јавним кључем је RSA криптосистем. Он је настао у 1977. години, а име је добио по почетним словима својих проналазача: Rivest, Shamir и Adleman. Његова сигурност је заснована управо на тешкоћи факторизације великих природних бројева.

Након RSA криптосистема, налази се Рабинов криптосистем. Настао је у 1979. години, а заснован је на проблему рачунања квадратног корена сложеног броја. Његово разбијање еквивалентно је решавању проблема квадратног корена, па је, еквивалентно и проблему факторизације.

1) RSA криптосистем

Нека је n сложен број облика $n = pq$, где су p и q различити прости бројеви и $\varphi(n)$ Ојлерова функција.

Нека је $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$. Тада је

$$\mathcal{K} = \{(n, p, q, d, e) : n = pq, de \equiv_{\varphi(n)} 1\}.$$

За $K \in \mathcal{K}$ можемо дефинисати

$$e_K(x) = x^e \bmod n, \quad d_K(y) = y^d \bmod n, \quad x, y \in \mathbb{Z}_n.$$

Вредности n и e су јавне вредности, док су вредности p, q и d тајне вредности, па је (n, e) јавни, док је (p, q, d) тајни кључ.

Како је $n = pq$, то је

$$\varphi(n) = \varphi(pq) = (p-1)(q-1) = n - p - q + 1.$$

Требало би доказати да су функције e_K и d_K једна другој инверзне.

За доказ су нам потребне Ојлерова и Мала Фермаова теорема. Ојлерова теорема каже да за $x \in \mathbb{Z}, n \in \mathbb{N}$ код којих је НЗД$(x, n) = 1$ важи $x^{\varphi(n)} \equiv_n 1$. Док је Мала Фермаова теорема последица Ојлерове теореме, и каже да за прост број p који не дели x, важи $x^{p-1} \equiv_p 1$.

Закључујемо да важи $d_K\left(e_K(x)\right) \equiv_n x^{de}$. Како је $de \equiv_{\varphi(n)} 1$, следи да постоји природан број k такав да је $de = k\varphi(n) + 1$.

Дискутујемо случајеве по могућим вредностима за НЗД(n, x).

1° НЗД$(n, x) = 1$: Користећи Ојлерову теорему, имамо да важи

$$x^{de} = x^{k\varphi(n)+1} = \left(x^{\varphi(n)}\right)^k \cdot x \equiv_n x.$$

2° НЗД$(n, x) = n$: Тада је $x^{de} \equiv_n 0 \equiv_n x$.

3° НЗД$(n, x) = p$: Тада је $x^{de} \equiv_p 0 \equiv_p x$, тј. $p \mid x^{de} - x$. Из Мале Фермаове теореме следи $x^{de} = \left(x^{q-1}\right)^{(p-1)k} \cdot x \equiv_q x$, па $q \mid x^{de} - x$. Како су p и q различити прости бројеви, они су узајамно прости, па следи $pq \mid x^{de} - x$. Дакле, важи $x^{de} \equiv_n x$.

4° НЗД$(n, x) = q$: Аналогном дискусијом као у случају 3° добијамо да важи $x^{de} \equiv_n x$.

Како смо у сваком случају добили да је $x^{de} \equiv_n x$, то значи да је $d_K\left(e_K(x)\right) = x$.

Сигурност RSA криптосистема представља претпоставка да је функција $e_K(x) = x^e \bmod n$ хеш функција, тј. функција чији инверз није лако одредити без додатних података. Додатни податак који омогућава дешифровање је познавање факторизације $n = pq$. Уколико се број n факторише, може се израчунати $\varphi(n) = (p-1)(q-1)$. Тако уствари добијамо експонент d уколико преко Еуклидовог алгортима решимо линеарну конгруенцију

$$de \equiv_{\varphi(n)} 1.$$

Пример 4.1. Генерисање RSA тајног кључа.

Решење. Изаберимо велике просте бројеве p и q. Нека су то $p = 11$ и $q = 3$. Тада је $n = pq = 11 \cdot 3 = 33$ и $\varphi(n) = (p-1)(q-1) = 10 \cdot 2 = 20$.

Сада треба одабрати број e који је узајамно прост са $\varphi(n) = 20$. Нека је то број $e = 3$.

Треба пронаћи број d такав да је задовољено $de \equiv_{\varphi(n)} 1$. То радимо на следећи начин:

$$de \equiv_{\varphi(n)} 1 \quad \Leftrightarrow \quad 3d \equiv_{20} 1 \quad \overset{\text{НЗД}(7,20)=1}{\Longleftrightarrow} \quad 21d \equiv_{20} 7 \quad \Leftrightarrow \quad d \equiv_{20} 7.$$

Јавни кључ је $(n, e) = (33, 3)$, а приватни је $d = 7$.

Након израчунатог кључа d, параметре p и q потребно је уништити на сигуран начин, јер управо од њих и зависи сигурност. □

Пример 4.2. Шифрирање и дешифровање RSA криптосистема

Решење. Нека је, као у претходном примеру, јавни кључ $(n, e) = (33, 3)$, а приватни $d = 7$ и нека је изабрана порука $m = 8$.

Шифровање, односно генерисање шифрата c, представљено је на следећи начин:

$$c \equiv_n m^e, \quad c \equiv_{33} 8^3 \equiv_{33} 17.$$

Дешифровање шифрата c представљено је као:

$$m \equiv_n c^d, \quad m \equiv_{33} 17^7 \equiv_{33} 8. \qquad \square$$

2) Рабинов криптосистем

Нека је број n сложен број облика $n = pq$, где су p и q прости бројеви такви да је $p \equiv_4 q \equiv_4 3$. Нека је $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$. Тада је

$$\mathcal{K} = \{(n, p, q) : n = pq\}.$$

За $K \in \mathcal{K}$ можемо дефинисати

$$e_K(x) = x^2 \bmod n, \quad d_K(y) = \sqrt{y} \bmod n.$$

Вредност n је јавна, а вредности p и q су тајне.

Конкретно, за поруку $m < n$ рачунамо шифрат c тако да је $m^2 \equiv_n c$.

Како бисмо из шифрата c добили поруку m потребно је пронаћи решења конгруенцијске једначине $x^2 \equiv_n c$. Означимо са m_p остатак при дељењу $c^{\frac{p+1}{4}}$ са p, а са m_q остатак при дељењу броја $c^{\frac{q+1}{4}}$ са q. Овако одабрани m_p и m_q су, заправо, такви да важи $m_p^2 \equiv_p c$ и $m_q^2 \equiv_q c$. Заиста, $m_p^2 \equiv_p c^{\frac{p+1}{2}} \equiv_p c \cdot c^{\frac{p-1}{2}}$. Како је $m^2 \equiv_{pq} c$, то важи и $m^2 \equiv_p c$, па је c квадратни остатак по модулу p, тј. Лежандров симбол[1] $\left(\frac{c}{p}\right) = 1$. (Уколико $p \mid c$, доказ је тривијалан, па претпостављамо да су p и c узајамно прости.) Из Ојлеровог критеријума за квадратне остатке имамо да је $c^{\frac{p-1}{2}} \equiv_p \left(\frac{c}{p}\right) = 1$, па је $m_p^2 \equiv_p c$. Аналогно се доказује и за m_q.

Како су p и q узајамно прости бројеви, из Безуове теореме следи да постоје $a, b \in \mathbb{Z}$ тако да је $ap + bq = 1$. Користећи Кинеску теорему о остацима, добијамо четири решења полазне конгруенцијске једначине, и то:

$$\begin{aligned} r_1 &= (apm_q + bqm_p) \mod n, \\ r_2 &= n - r_1, \\ r_3 &= (apm_q - bqm_p) \mod n, \\ r_4 &= n - r_3. \end{aligned}$$

Једно од ова четири решења је почетна порука m. Које тачно решење је тражена порука не можемо тачно знати без додатних информација.

Пример 4.3. Шифрирање и дешифровање Рабин криптосистема.

Решење. Нека је $p = 7$ и $q = 19$. Тада је $n = 133$. Нека је порука $m = 25$. Шифрат c тада рачунамо из $m^2 \equiv_n 625 \equiv_{133} 93$, па је $c = 93$.

Даље, рачунамо m_7 користећи $c^{\frac{p+1}{4}} \equiv_p 93^2 \equiv_7 4$, па је $m_7 = 4$. Такође, из $c^{\frac{q+1}{4}} \equiv_{19} 93^5 \equiv_{19} 6$, следи $m_{19} = 6$. Користећи Еуклидов алгоритам, налазимо a и b тако да је $7a + 19b = 1$, и добијамо $a = -8$ и $b = 3$.

[1] Нека је a цео број и p прост број, већи од 2, такав да је $(a, p) = 1$. *Лежандров симбол* $(\frac{a}{p})$ дефинише се као: $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ако је } a \text{ квадратни остатак по модулу } p \\ -1, & \text{ако је } a \text{ квадратни неостатак по модулу } p \end{cases}$

Израчунајмо сада потенцијалне кандидате за тражену поруку:

$$\begin{aligned} r_1 &= (apm_q + bqm_p) \mod n = ((-8)\cdot 7\cdot 6 + 3\cdot 19\cdot 4) \mod 133 = \mathbf{25}, \\ r_2 &= n - r_1 = 133 - 25 = 108, \\ r_3 &= (apm_q - bqm_p) \mod n = ((-8)\cdot 7\cdot 6 - 3\cdot 19\cdot 4) \mod 133 = 32, \\ r_4 &= n - r_3 = 133 - 32 = 101. \end{aligned}$$

Тражена порука је r_1. Приметимо да за сва 4 кандидата, r_i, $i \in \{1,2,3,4\}$ важи да је $r_i^2 \equiv_{133} 93$, $i \in \{1,2,3,4\}$. □

Недостатак Рабиновог криптосистема јесте тај што функција e_K није инјективно пресликавање.

Постоје четири решења по модулу n чији квадрати дају шифрат c, па дешифровање није могуће спровести на једнозначан начин (осим ако је отворени текст неки смислени текст, а то није случај код размене кључева, за шта се криптосистеми са јавним кључем првенствено и користе). Један начин за решавање овог проблема је да се у отворени текст на одређени начин убаци извесна правилност. То се може урадити тако да се последња 64 бита понове и тада можемо очекивати да ће само једно од 4 решења дати резултат који има задату правилност.

5 Факторизација

Да бисмо разбили отворени текст RSA или Рабин криптосистема, потребно је за одређено коначно време извршити факторизацију. (То су криптосистеми са јавним кључем и они су конструисани над проблемом факторизације. Самим тим, њихово разбијање, односно дешифровање, биће решавање тог проблема факторизације).

Уколико желимо да дешифрујемо поруку која носи више информација, пожељно је, а некада и потребно, да решење проблема буде брже у односу на решење које је дешифровало поруку са мање информација. То значи да би наш унапређени алгоритам, требало за исто време да обради више информација у односу на почетни алгоритам, тј. унапређени алгоритам би требало да буде ефикаснији. Односно, сложеност алгоритма би требала бити мања.

5.1 Сложеност алгоритма

Алгоритам је метода (процедура) за решавање неке класе проблема, која за улазне податке одређеног типа даје одговор (излазне податке) у коначном времену.

Упоређујемо их у односу на број елементарних корака потребних за њихово извршавање, као и на потребан простор (меморију). Под елементарним кораком подразумевамо логичку операцију дисјункције, конјукције или негације на битовима - нулама и јединицама. Величину улазних података ћемо мерити бројем битова потребних за њихов приказ.

Да бисмо проценили сложеност неког алгоритма, потребно је да проучимо асимптотско понашање броја операција кад величина улазних података неограничено расте. Због тога нам није потребно, а често и није могуће, извести тачну формулу за број операција неког алгоритма.

Дефиниција 5.1. Нека су $f, g : \mathbb{R} \to \mathbb{R}$ две функције. Тада пишемо:

(1) $f(x) = O(g(x))$ ако постоје $x_0, M > 0$ тако да је $|f(x)| \leq M|g(x)|$ за свако $x > x_0$;

(2) $f(x) \sim g(x)$ ако је $\lim\limits_{x\to\infty} \frac{f(x)}{g(x)} = 1$;

(3) $f(x) = o(g(x))$ ако је $\lim\limits_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

Сложеност алгоритма представља број операција за „најспорији" случај при уносу произвољних података.

Просечна сложеност алгоритма представља просечан број операција.

Дефиниција 5.2. Полиномијалан алгоритам је алгоритам чији је број операција у најспоријем случају функција облика $O\left(n^k\right)$, где је n дужина улазног податка (у битовима), а k је константа. Алгоритме који нису полиномијални, зовемо експоненцијални.

Како тежимо ка најбржем алгоритму (да бисмо брже дешифровали податке) и што тежем проблему (да би се теже разбио кључ) и то у просечном случају, тада уз сложеност алгоритма посматрамо и остале елементе који могу утицати на брзину и применљивост алгоритма. То су просечан број операција, као и степен полинома сложености алгоритма. Зато, може се десити да је проблем над којим смо конструисали кључ „тежак" у изолованом, али не и у просечном случају, као и то да асимптотски спорији алгоритам, може бити брже извршен.

Дефиниција 5.3. Субекспоненцијални алгоритам је алгоритам чија је сложеност функција облика $O\left(e^{o(n)}\right)$, где је n дужина улазног податка.

Најбољи познати алгоритми за факторизацију природног броја N су субекспоненцијални и њихова сложеност је функција облика

$$L_N(v,c) = O\left(e^{c(\ln N)^v(\ln\ln N)^{1-v}}\right)$$

за $v = \frac{1}{2}$ или $v = \frac{1}{3}$. Уочимо да за $v = 0$ имамо $L_N(0,c) = O\left((\ln N)^c\right)$, док за $v = 1$ имамо $L_N(1,c) = O\left(N^c\right)$. Дакле, субекспоненцијални алгоритми који одговарају вредностима $v, 0 < v < 1$, су асимптотски спорији од полиномијалних, али су бржи од тотално експоненцијалних, тј. оних чија је сложеност функција облика $O\left(e^{n^k}\right)$. Полиномијални алгоритми спадају у ефикасне, док експоненцијални спадају у неефикасне алгоритме.

5.2 Метода верижног разломка

Општа метода факторизације мотивисана је *Фермаовом факторизацијом* примењеном на број n који је производ два „блиска" броја. Такав број n је разлика квадрата два природна броја од којих је један јако мали, а други је близу броја $\sqrt{n}$.

Односно, ако је $n = ab$, где је $|a-b|$ број близу нуле, тада је $n = t^2 - s^2$ и $t = \frac{a+b}{2}$, а $s = \frac{a-b}{2}$. Заиста, када је задовољено да је $|a-b|$ близу нуле, број s је јако мали, а број t је мало већи од $\sqrt{n}$.

Једноставним испробавањем могућности за t међу бројевима $\lfloor\sqrt{n}\rfloor + 1$, $\lfloor\sqrt{n}\rfloor + 2$, $\cdots$, налазимо t, а самим тим и одређујемо факторизацију броја n.

Касније методе, мотивисане Фермаовом факторизацијом, модификоване су тако да уместо тражења бројева s и t који задовољавају $n = t^2 - s^2$, тражимо бројеве s и t такве да задовољавају $n \mid t^2 - s^2$, тј. $t^2 \equiv_n s^2$.

Уколико $t^2 \not\equiv_n s^2$, тада кажемо да су НЗД$(t+s, n)$ и НЗД$(t-s, n)$ нетривијални фактори броја n.

Најстарија метода која се ослања на такав алгоритам је управо *метода верижног разломка.* [2]

Нека је n сложен број чију факторизацију желимо да пронађемо. Уколико n није потпун квадрат, тада је развој броја $\sqrt{n}$ у верижни разломак периодичан. Тачније биће:

$$x = [a_0; \overline{a_1, a_2, \cdots, a_{r-1}, 2a_0}]$$

Верижни разломак тада рачунамо преко алгоритма:

$$\begin{array}{lll} a_0 = \lfloor \sqrt{n} \rfloor, & s_0 = 0, & t_0 = 1 \\ a_i = \lfloor \dfrac{a_0 + s_i}{t_i} \rfloor, & s_{i+1} = a_i t_i - s_i, & t_{i+1} = \dfrac{n - s_{i+1}^2}{t_i}, \text{ за } i \geq 0 \end{array}$$

Нека је $\frac{P_i}{Q_i} = [a_0; a_i, a_i, \cdots, a_i]$. Тада важи следеће:

$$P_i^2 - nQ_i^2 = (-1)^{i+1} \cdot t_{i+1} \qquad \text{и} \qquad 0 < t_i < 2\sqrt{n}.$$

Одавде закључујемо да парцијални разломци верижног разломка задовољавају конгруенције облика

$$P_i^2 \equiv_n w_i,$$

где је w_i релативно мали број. Ако пронађемо w_i-ове такве да им је производ потпун квадрат (нека су то $w_{k_1}, \cdots, w_{k_m}$, такви да важи $w_{k_1} \cdots w_{k_m} = w^2$), тада смо пронашли конгруенцију $P_{k_1} \cdots P_{k_m} \equiv_n w^2$, па су НЗД$(P_{k_1} \cdots P_{k_m} + w, n)$ и НЗД$(P_{k_1} \cdots P_{k_m} - w, n)$ кандидати за нетривијалан фактор броја n. Уколико нисмо пронашли ни један фактор

[2] Метода верижног разломка другачије се назива *Brillhart-Morrisonova метода* будући да су је они 1970. године искористили за факторизацију Фермаовог броја $2^{2^7}+1$. Ипак, основна идеја се може наћи већ у радовима Kraitchika, Lehmera и Powersa 20-тих и 30-тих година 20. века

траженог броја n, треба потражити другу комбинацију бројева w_i и понављамо поступак. Због периодичности развоја броја $\sqrt{n}$ у верижни разломак бројеви t_i, односно w_i, почеће да се понављају.

Илуструјмо ову методу наредним примером.

Пример 5.1. Факторисати број 16463 помоћу верижних разломака.

Решење. Развој броја $\sqrt{16463}$ у верижни разломак је

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

Коефицијенти из развоја броја $\sqrt{16463}$ у верижни разломак дати су следећом табелом:

i	s_i	t_i	a_i	$P_i (\mathrm{mod} N)$
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

Из табеле видимо да је

$$(-1)^8 \cdot t_8 \cdot (-1)^{12} \cdot t_{12} = 97 \cdot 97 = 97^2$$

Можемо приметити и да је

$$P_7^2 \cdot P_{11}^2 = 8565^2 \cdot 15574^2 = (8565 \cdot 15574)^2 = 133391310^2 \equiv_{16463} 8084^2 \equiv_{16463} 97^2$$

Важи и $P_i^2 \equiv_n w_i$, па је $P_7^2 \cdot P_{11}^2 \equiv_{16463} w_7 \cdot w_{11}$, тј. одатле је

$$w_7 \cdot w_{11} \equiv_{16463} 97^2$$

Кандидати за нетривијалан фактор броја 16463 су НЗД$(8084 + 97, 16463)$ и НЗД$(8084 - 97, 16463)$. Највећи заједнички делилац тих бројева добијамо употребом Еуклидовог алгоритма, а то су бројеви 101 и 163.

Управо то су и фактори броја 16463 који је требало да факторишемо, тј. важи $16463 = 101 \cdot 163$. $\square$

5.3 Уопштена метода верижног разломка

Уколико уопштимо овај метод, метода верижног разломка постаје ефикаснија метода. Да бисмо то постигли, користимо базу фактора за налажење релација облика $w_{k_1} \cdots w_{k_m} = w^2$ на следећи начин.

Формирамо базу фактора $\mathcal{B}$ која се састоји од броја -1, као и простих бројева мањих или једнаких одабраној граници M. Неће се сваки прост број налазити у факторској бази, већ ће се за непаран прост број p_i мањи или једнак одабраној граници рачунати вредност Лежандровог симбола n по p_i. Сада треба сваки w_i приказати као линеарну комбинацију елемената базе фактора $\mathcal{B}$.

Нека база фактора има m елемената.
Након факторизације бар $m + 1$ бројева w_i, посматрамо одговарајуће векторе парности експонената. Уколико је експонент паран, пише се 0, уколико је непаран пише се 1. То су вектори у $\mathbb{Z}_2^m$, где је $\mathbb{Z}_2 = \{0, 1\}$. Како таквих вектора има више од димензије припадног векторског простора, они су линеарно зависни. Гаусовом методом елиминације можемо пронаћи њихову нетривијалну линеарну комбинацију која даје нула вектор. То значи да можемо пронаћи подскуп w_i-ова такав да је сума припадних вектора парности парна, а одатле закључујемо да је производ тих w_i-ова потпун квадрат.

Код методе верижног разломка, отприлике пола простих бројева се може изоставити из базе фактора $\mathcal{B}$. Ако $p \mid w_i$, онда $p \mid P_i^2 - nQ_i^2$, тј. $P_i^2 \equiv_p nQ_i{}^2$, па је n квадратни остатак по модулу p. Зато се из базе фактора могу избацити сви они фактори p такви да n није квадратни остатак по модулу p.

Што се тиче сложености методе верижног разломка, може се показати да је оптималан избор границе такав да је $M \approx e^{\sqrt{\ln n \ln\ln n}}$, па је очекивани број операција

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

Оваква процена није формално доказана, већ се заснива на недоказаним *хеуристичким* претпоставкама.

Пример 5.2. Факторисати број 12378523 помоћу верижних разломака.

Решење. Нека је база фактора $\mathcal{B} = \{-1, 2, 3, 11, 13\}$ таква да се састоји од броја -1 и свих простих бројева мањих или једнаких од 13. За горњу границу простих фактора узимамо број 79.

Када израчунамо развој броја $\sqrt{12378523}$ у верижни разломак, добијамо бројеве t_i. Посматрајмо само оне бројеве t_i које у потпуности можемо факторисати помоћу факторске базе. Факторисани бројеви t_i са припадним векторима парности експонената приказани су у наредној табели:

i	$(-1)^i t_i$	-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		

Како за $i = 8$ имамо нула-врсту, то је $(-1)^8 t_i = (3 \cdot 13)^2$. Сада треба испитати да ли је тај број фактор броја n и одређујемо решење $P_7^2 \equiv_n (-1)^8 t_i$. Добијамо $12378484^2 \equiv_n 39^2$. Како је највећи заједнички делилац бројева $12378484 - 39$ и n једнак 1, то је на овај начин немогуће факторисати број n. Због тога одбацујемо врсту $i = 8$ и настављамо са рачунањем развоја верижног разломка.

i	$(-1)^i t_i$	-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

Тренутно у таблици имамо 10 врста, јер не рачунамо врсту $i = 8$ (одбацили смо је, јер је нула-врста, а нисмо добили факторизацију броја n преко ње). У скупу свих фактора који се појављују у факторизацијама има 9 елемената, па одатле закључујемо да постоји могућност налажења потпуног квадрата. Гаусовим елиминацијама тражимо комбинацију која даје потпуни квадрат. Неке комбинације које дају потпуни квадрат те одговарајуће конгруенције су:

$$\begin{aligned} t_3 t_7 t_{16} &\equiv_n P_2^2 P_6^2 P_{15}^2, \\ t_3 t_{11} t_{22} &\equiv_n P_2^2 P_{10}^2 P_{21}^2, \\ t_7 t_{13} t_{32} &\equiv_n P_6^2 P_{12}^2 P_{31}^2, \\ t_7 t_{11} t_{16} t_{22} &\equiv_n P_6^2 P_{10}^2 P_{15}^2 P_{21}^2. \end{aligned}$$

Рачунањем долазимо до закључка да ни једна од тих комбинација не даје нетривијалне факторе броја n, па настављамо тражити нула-врсту.

Тако долазимо до комбинације:

$$t_3 t_{32} t_{43} = \left(3^2 \cdot 11^2 \cdot 13^2 \cdot 41^2\right) = 17589^2.$$

Имамо конгруенцију:

$$\begin{aligned} P_2^2 P_{31}^2 P_{42}^2 &\equiv_n 17589^2, \\ (56293 \cdot 1351545 \cdot 9955325)^2 &\equiv_n 17589^2, \\ 12342301^2 &\equiv_n 17589^2, \\ 12342301^2 - 17589^2 &\equiv_n 0. \end{aligned}$$

Највећи заједнички делилац бројева $12342301 - 17589$ и $n = 12378523$ је број 1993, па је он један фактор броја n. Највећи заједнички делилац

бројева $12342301 + 17589$ и $n = 12378523$ је број 6211, па је то други фактор, тј. чинилац, броја n.
На тај начин добили смо факторизацију броја $n = 1993 \cdot 6211 = 12378523$.
□

Коментар: Налажење потпуног квадрата међу бројевима t_i не значи и добијање фактора броја n. Може се десити да као НЗД добијемо број 1 или сам број n, па тада треба тражити неки други потпуни квадрат, а ако га не успемо пронаћи, тада треба да се вратимо на почетак и израчунамо још више бројева t_i.

6 Уместо закључка

У самом почетку рада прошли смо кроз теоријске основе верижних разломака, као и криптосистема.

Приказали смо то да се сваки рационалан број може приказати у облику коначног, док се сваки ирационалан број може приказати у облику бесконачног верижног разломка.

Истакли смо криптосистеме конструисане над проблемима факторизације, а затим и описали методу њиховог дешифровања помоћу верижних разломака. Такође, дат је приказ и општијег метода преко базе фактора.

Код методе верижног разломка често се уместо развоја броја $\sqrt{n}$, посматра развој броја $\sqrt{kn}$ у верижни разломак, за неки цео број k који није потпун квадрат. То радимо онда кад број $\sqrt{n}$ нема довољно дуг период. Невезано за то да ли посматрамо развој броја $\sqrt{n}$ или броја $\sqrt{kn}$, $k \in \mathbb{Z}$, операције које извршавамо су операције по модулу n.

Такође, број k утиче на просте бројеве у бази фактора, па ће добрим одабиром броја k и број простих бројева у бази фактора бити мањи.

Важно је напоменути и то да ће онај који задаје шифру имати експоненцијално лакши посао од оног који ту шифру жели да дешифрује. До тога долази зато што је испитивање простости великог броја алгоритам полиномске сложености, а самим тим је лакши проблем него факторизација.

Уз то, за исти ниво безбедности, дужина хеш вредности мора бити бар два пута већа од дужине тајног кључа код симетричног шифарског система.

Литература

[1] А. Дујела, *Теорија бројева у криптографији*, Свеучилиште у Загребу, Природно-математички факултет, Загреб, 2004.

[2] Д. Ђукић, *Верижни разломци*, `https://imomath.com/srb/dodatne/veriznirazlomci_ddj.pdf`

[3] Снежана М. Илић, Милица З. Колунџија, *Основи теорије бројева и полинома*, Универзитет у Нишу, Природно-математички факултет, Ниш, 2019.

[4] И. Тржић, *Верижни разломци*, Дипломски рад, Свеучилиште J. J. Strossamayera у Осијеку, Осијек, 2011.

[5] К. Краљ, *Примјена верижних разломака у факторизацији и тестирању простости*, Дипломски рад, Свеучилиште у Загребу, Природно-математички факултет, Загреб, 2017.

[6] Л. Сабадош, *Верижни разлоомци квадратичних бројева*, Мастер рад, Универзитет у Београду, Математички факултет, Београд, 2021.

[7] М. Веиновић, С. Адамовић, *Основе за анализу и синтезу шифарских система*, Универзитет Сингидунум, Факултет за информатику у рачунарство, Београд, 2023

[8] Марко Д. Петковић, *Алгоритми нумеричке анализе*, Универзитет у Нишу, Природно-математички факултет, Ниш 2013.

[9] `https://people.dmi.uns.ac.rs/~bojan.basic/tb/predavanja/tb12.pdf`