Др Бернадин Ибрахимпашић, др Ариф Золић

ЕУКЛИДОВ АЛГОРИТАМ И ЊЕГОВА ПРИМЈЕНА

Еуклидов алгоритам је ефикасан начин за одређивање највећег заједничког дјелиоца два природна броја, који не захтијева њихову претходну факторизацију. То је најстарији нетривијални алгоритам који је преживио до данас. Први пут се у писаном облику појављује у Еуклидовим „Елементима“ (300. г.пр.н.е.), и то у VII књизи гдје је исказан за природне бројеве и у X књизи гдје је дата његова примјена на дужи. Иако се налази у Еуклидовим „Елементима“, вјерује се да алгоритам није његово дјело, већ да је био познат више од 200 година раније. Алгоритам је заснован на чињеници да се највећи заједнички дјелилац два природна броја неће промијенити ако се од већег броја одузме мањи па се затим посматра највећи заједнички дјелилац новодобијеног броја и мањег од два претходно посматрана. Понављајући тај поступак, а како скуп природних бројева има најмањи елемент, то се алгоритам завршава у коначно много корака. У XIX вијеку долази до уопштавања алгоритма на полиноме с једном промјењивом и на Гауссове цијеле бројеве, а након тога и на полиноме с више промјењивих. Алгоритам има велику и теоријску и практичну примјену. Ми ћемо овдје приказати неке од практичних примјена као што су рјешавање линеарних диофантских једначина, рјешавање линеарних конгруенција, одређивање мултипликативног инверза у коначном пољу и за развој рационалног броја у верижни разломак.

1. Највећи заједнички дјелилац

Теорија бројева је грана математике која се бави својствима бројева, а посебно цијелих и природних. Један од најједноставнијих, али уједно и најважнијих, појмова у теорији бројева је појам дјељивости.

Дефиниција 1. Нека су $b \neq 0$ и a цијели бројеви. Кажемо да је *a дјељив* с b, односно да b *дијели* a, ако постоји цијели број q такав да је $a = bq$. То записујемо с $b \mid a$. Ако b не дијели a, онда пишемо $b \nmid a$. Ако $b \mid a$, онда још кажемо да је b *дјелилац* од a, а да је a *садржалац* од b.

Теорема 1. [Теорема о дијељењу с остатком] *За произвољан природан број b и цијели број a постоје јединствени цијели бројеви q и r такви да је $a = qb + r$, $0 \leq r < b$.*

Број q се зове количник а r се зове остатак при дијељењу a са b.

Дефиниција 2. Нека су a и b цијели бројеви. Цијели број d зовемо *заједнички дјелилац* бројева a и b ако $d \mid a$ и $d \mid b$. Ако је барем један од бројева a и b различит од нуле, онда постоји само коначно много заједничких дјелилаца бројева a и b. Највећи међу њима зове се *највећи заједнички дјелилац* бројева a и b и означава се с НЗД(a, b) или $\gcd(a, b)$ ("greatest common divisor").

Слично се дефинише највећи заједнички дјелилац бројева $a_1, a_2, \ldots, a_n$ који нису сви једнаки нули, а означава се с НЗД$(a_1, a_2, \ldots, a_n)$.

Као што смо већ рекли, Еуклидов алгоритам за налажење највећег заједничког дјелиоца два природна (а самим тим и цијела) броја је најстарији нетривијални алгоритам који је и данас у употреби. Он је заснован на теореми о дијељењу с остатком и на чињеници исказаној у сљедећој теореми.

Теорема 2. *Нека су a, b, q и r цијели бројеви такви да је $b > 0$, $0 \leq r < b$ и $a = bq + r$. Тада је* НЗД$(a, b) =$ НЗД(b, r).

Теорема 3. [Еуклидов алгоритам] *Нека су a и $b > 0$ цијели бројеви. Претпоставимо да је узастопном примјеном теореме о дијељењу с остатком добијен низ једнакости*

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b,\\
b &= r_1 q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{j-2} &= r_{j-1} q_j + r_j, & 0 < r_j < r_{j-1},\\
r_{j-1} &= r_j q_{j+1}.
\end{aligned}$$

Тада је НЗД(a, b) *једнак r_j, тј. посљедњем остатку различитом од нуле. Вриједности од x_0 и y_0 у изразу* НЗД$(a, b) = ax_0 + by_0$ *могу се добити изражавањем сваког остатка r_i као линеарне комбинације од a и b.*

Примјер 1. Одредити $d =$ НЗД$(196, 154)$.

Рјешење. Примијенимо Еуклидов алгоритам.

$$\begin{aligned}
196 &= 154 \cdot 1 + 42\\
154 &= 42 \cdot 3 + 28\\
42 &= 28 \cdot 1 + 14\\
28 &= 14 \cdot 2
\end{aligned}$$

Добили смо да је $d =$ НЗД$\,(196, 154) = 14$.

Како сваки остатак у алгоритму можемо приказати као линеарну комбинацију претходна два, то га можемо приказати и као линеарну комбинацију бројева a и b. Из тога специјално слиједи да и посљедњи ненулти остатак, који представља

највећи заједнички дјелилац бројева a и b, можемо приказати као линеарну комбинацију бројева a и b.

$$\begin{aligned} 14 &= 42 - 28 \cdot 1 = 42 - (154 - 42 \cdot 3) \cdot 1 = 4 \cdot 42 - 1 \cdot 154 \\ &= 4 \cdot (196 - 154 \cdot 1) - 1 \cdot 154 = 4 \cdot 196 - 5 \cdot 154 \\ &= 196 \cdot 4 + 154 \cdot (-5) \end{aligned}$$

2. Линеарне диофантске једначине

Видјели смо како се НЗД(a, b) може приказати као линеарна комбинација бројева a и b. То можемо урадити и једноставније искористимо ли сљедеће рекурзивне релације. Нека је

$$\begin{aligned} x_{-1} = 1, \quad x_0 = 0, \quad x_i = x_{i-2} - q_i x_{i-1}, \\ y_{-1} = 0, \quad y_0 = 1, \quad y_i = y_{i-2} - q_i y_{i-1}; \end{aligned}$$

тада је

$$ax_i + by_i = r_i, \quad \text{за } i = -1, 0, 1, \ldots, j, j+1.$$

Важи

$$ax_j + by_j = \text{ НЗД}\,(a, b)\,.$$

Ово нам омогућује да наведене рекурзивне релације искористимо за рјешавање једначине $ax + by = \text{ НЗД}\,(a, b)$.

Примјер 2. Одредимо $d = \text{ НЗД}(222, 102)$ и нађимо цијеле бројеве x и y такве да је $222x + 102y = d$.

Рјешење.

$$\begin{aligned} 222 &= 102 \cdot 2 + 18 \\ 102 &= 18 \cdot 5 + 12 \\ 18 &= 12 \cdot 1 + 6 \\ 12 &= 6 \cdot 2 \end{aligned}$$

i	-1	0	1	2	3	4
q_i			2	5	1	2
x_i	1	0	1	-5	6	
y_i	0	1	-2	11	-13	

Добили смо да је $d = \text{ НЗД}\,(222, 102) = 6$, те да је $222 \cdot 6 + 102 \cdot (-13) = 6$.

Теорема 4. *Нека су a, b, c цијели бројеви и $d = \text{ НЗД}(a, b)$. Ако $d \nmid c$, онда једначина $ax + by = c$ нема цјелобројних рјешења. Ако $d \mid c$, онда дата једначина има бесконачно много цјелобројних рјешења. Ако је (x_0, y_0) једно њено рјешење, онда су јој сва рјешења дата с*

$$x = x_0 + \frac{b}{d} \cdot t, \qquad y = y_0 - \frac{a}{d} \cdot t, \quad t \in \mathbf{Z}.$$

Примјер 3. Ријешити једначину $77x + 98y = 7$.

Рјешење.

$$77 = 98 \cdot 0 + 77$$
$$98 = 77 \cdot 1 + 21$$
$$77 = 21 \cdot 3 + 14$$
$$21 = 14 \cdot 1 + 7$$
$$14 = 7 \cdot 2$$

Добили смо да је $d = \text{НЗД}(77, 98) = 7$, а како је у нашој једначини $c = 7$ то имамо да $d = \text{НЗД}(a, b) \mid c$ па наша једначина има рјешење.

i	-1	0	1	2	3	4
q_i			0	1	3	1
x_i	1	0	1	-1	4	-5
y_i	0	1	0	1	-3	4

Добили смо да је $77 \cdot (-5) + 98 \cdot 4 = 7$ па имамо да је $(-5, 4)$ једно рјешење полазне једначине. Закључујемо да су сва њена рјешења

$$x = -5 + \frac{77}{7} \cdot t, \qquad y = 4 - \frac{98}{7} \cdot t,$$

тј.

$$x = -5 + 11t, \qquad y = 4 - 14t, \quad t \in \mathbf{Z}.$$

Видјели смо начин рјешавања диофантске једначине облика $ax + by = \text{НЗД}(a, b)$. Погледајмо сада како рјешавамо диофантску једначину облика $ax + by = k \cdot \text{НЗД}(a, b)$, гдје је k цијели број.

Примјер 4. Ријешити једначину $96x + 68y = 48$.

Рјешење.

$$96 = 68 \cdot 1 + 28$$
$$68 = 28 \cdot 2 + 12$$
$$28 = 12 \cdot 2 + 4$$
$$12 = 4 \cdot 3$$

Добили смо да је $d = \text{НЗД}(68, 96) = 4$, а како је у нашој једначини $c = 48$ то имамо да $d = \text{НЗД}(a, b) \mid c$, па наша једначина има рјешење. Поступком као у претходним примјерима добијамо да је

$$96 \cdot 5 + 68 \cdot (-7) = 4,$$

а како је $48 : 4 = 12$, помножимо посљедњу релацију с 12. Добијамо да је

$$96 \cdot 60 + 68 \cdot (-84) = 48,$$

па закључујемо да је $(60, -84)$ једно рјешење полазне једначине. Сада су сва рјешења полазне једначине дата с

$$x = 60 + \frac{68}{4} \cdot t, \qquad y = -84 - \frac{96}{4} \cdot t,$$

тј.

$$x = 60 + 17t, \qquad y = -84 - 24t, \quad t \in \mathbf{Z}.$$

Примјер 5. У једној просторији се налазе столице с 3 и с 4 ноге. Када на све столице сједне по једна особа, у соби има укупно 69 ногу. Колико у просторији има столица с 3 а колико с 4 ноге?

Рјешење. Када на столицу с 3 ноге сједне једна особа, онда је ту укупно 5 ногу, а када на столицу с 4 ноге сједне једна особа, онда је ту укупно 6 ногу. Означимо ли с x број столица с 3 ноге, а с y број столица с 4 ноге, добијамо једначину

$$5x + 6y = 69,$$

гдје је

$$0 \le x \le \frac{69}{5}, \quad 0 \le y \le \frac{69}{6}, \quad x, y \in \mathbf{Z}.$$

Примијенимо ли до сада показано, добијамо да је НЗД$(5, 6) = 1$ и да је $(-1, 1)$ једно рјешење једначине $5x + 6y = 1$. Из тога слиједи да је $(-1, 1)$ једно рјешење једначине $5x + 6y = 69$, па су сва њена рјешења

$$x = -69 + \frac{6}{1} \cdot t = -69 + 6t, \qquad y = 69 - \frac{5}{1} \cdot t = 69 - 5t, \quad t \in \mathbf{Z}.$$

Како мора вриједити

$$0 \le -69 + 6t \le \frac{69}{5}, \quad 0 \le 69 - 5t \le \frac{69}{6}, \quad t \in \mathbf{Z},$$

добијамо да је

$$\frac{69}{6} \le t \le \frac{69}{5},$$

тј.

$$11.5 \le t \le 13.8 \qquad \Rightarrow t \in \{12, 13\}.$$

Уврстимо ли те вриједности за t у формуле за рјешење једначине, добијамо

$$\begin{aligned} t = 12: &\quad x = -69 + 6 \cdot 12 = 3, \quad y = 69 - 5 \cdot 12 = 9, \\ t = 13: &\quad x = -69 + 6 \cdot 13 = 9, \quad y = 69 - 5 \cdot 13 = 4. \end{aligned}$$

Видимо да задатак има два рјешења. Једно рјешење је да су у соби 3 столице с 3 ноге и 9 столица с 4 ноге, а друго рјешење је да је у соби 9 столица с 3 ноге и 4 столице с 4 ноге.

3. Линеарне конгруенције

Ознаку за конгруенције, која се и данас користи, увео је Гаус 1801. године у свом дјелу "Disquisitiones Arithmeticae". Сама идеја конгруенција се појављивала још код старих Грка и Кинеза.

Дефиниција 3. Ако цијели број $m \neq 0$ дијели разлику $a - b$, онда кажемо да је *a конгруентан b* модуло m и пишемо $a \equiv b \pmod{m}$. У противном кажемо да *a није конгруентан b* модуло m и пишемо $a \not\equiv b \pmod{m}$.

Овдје је потребно напоменути да је $a - b$ дјељиво с m ако и само ако је $a - b$ дјељиво с $-m$. Из тог разлога се у теорији конгруенција разматрају само случајеви када је m природан број. Такође треба истакнути да је релација „бити конгруентан" релација еквиваленције на скупу $\mathbf{Z}$.

Наведимо неколико особина конгруенција које се врло често користе у примјенама.

Тврђење 1. *Нека су a, b, c, d цијели бројеви и нека је f полином с цјелобројним коефицијентима.*

1. $a \equiv b \pmod{m} \Leftrightarrow a - b \equiv 0 \pmod{m}$.
2. *Ако је* $a \equiv b \pmod{m}$ *и* $c \equiv d \pmod{m}$, *онда је* $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$ *и* $ac \equiv bd \pmod{m}$.
3. *Ако је* $a \equiv b \pmod{m}$ *и* $d \mid m$, *онда је* $a \equiv b \pmod{d}$.
4. *Ако је* $a \equiv b \pmod{m}$, *онда је* $ac \equiv bc \pmod{mc}$ *за сваки* $c \neq 0$.
5. *Ако је* $a \equiv b \pmod{m}$, *онда је* $f(a) \equiv f(b) \pmod{m}$.

Конгруенције имају много сличности с једначинама. Аналогно једначинама, рјешење конгруенције $f(x) \equiv 0 \pmod{m}$, гдје је $f(x)$ полином с цјелобројним коефицијентима, јесте сваки цијели број x који је задовољава. Ако је x_1 неко рјешење конгруенције $f(x) \equiv 0 \pmod{m}$, и $x_2 \equiv x_1 \pmod{m}$, онда је и x_2 такође рјешење те конгруенције. Нас интересују рјешења која нису међусобно конгруентна по модулу m, тј. нас интересују нееквивалентна рјешења. Два рјешења x_1 и x_2 сматрамо еквивалентним ако је $x_1 \equiv x_2 \pmod{m}$. Број рјешења конгруенције је број нееквивалентних рјешења.

Теорема 5. *Нека су a и m природни бројеви и нека је b цијели број. Конгруенција $ax \equiv b \pmod{m}$ има рјешења ако и само ако $d =$ НЗД(a, m) дијели b. Ако је овај услов испуњен, онда горња конгруенција има тачно d рјешења модуло m.*

Још једна карактеризација конгруентности је врло интересантна. Тако имамо да ако је $a \equiv b \pmod{m}$, тада постоји цијели број k такав да је $a = km + b$. Ту карактеризацију можемо искористити за рјешавање конгруенција облика $ax \equiv b \pmod{m}$. Ако та конгруенција има рјешења, онда $d =$ НЗД$(a, m) \mid b$ и постоји $k \in \mathbf{Z}$ тако да је $ax = mk + b$, тј. да је $ax + m(-k) = b$. Како $d =$ НЗД$(a, m) \mid b$ то диофантска једначина $ax + m(-k) = b$ има рјешење, па наведене рекурзије и

поступак за њено рјешавање можемо искористити и за рјешавање конгруенција облика $ax \equiv b \pmod{m}$.

Пример 6. Ријешити конгруенцију $224x \equiv 1 \pmod{319}$.

Рјешење. Примијенимо Еуклидов алгоритам да одредимо НЗД$(319, 224)$.

$$\begin{aligned} 319 &= 224 \cdot 1 + 95 \\ 224 &= 95 \cdot 2 + 34 \\ 95 &= 34 \cdot 2 + 27 \\ 34 &= 27 \cdot 1 + 7 \\ 27 &= 7 \cdot 3 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ 6 &= 1 \cdot 6 \end{aligned}$$

Добили смо да је НЗД$(319, 224) = 1$. Како $1 \mid 1$, то дата конгруенција има рјешење. До рјешења се може лако доћи примјеном рекурзивне релације

$$y_{-1} = 0, \quad y_0 = 1; \quad y_i = y_{i-2} - q_i y_{i-1}, \quad i = 1, 2, \ldots, k,$$

гдје је k индекс посљедњег остатка у Еуклидовом алгоритму који је различит од 0. У том случају рјешење конгруенције је $x \equiv y_k \pmod{319}$.

i	-1	0	1	2	3	4	5	6
q_i			1	2	2	1	3	1
y_i	0	1	-1	3	-7	10	-37	-47

Дакле, рјешење конгруенције $224x \equiv 1 \pmod{319}$ је $x \equiv 47 \pmod{319}$.

Пример 6. Ријешити конгруенцију $255x \equiv 145 \pmod{370}$.

Рјешење. Примијенимо ли Еуклидов алгоритам добијамо $d =$ НЗД$(255, 370) = 5$, а како $d = 5 \mid 145$ то конгруенција има рјешење. Подијелимо ли 255, 145 и 370 с $d = 5$, добијамо 51, 29 и 74 па рјешавамо конгруенцију $51y \equiv 29 \pmod{74}$. Како је сада НЗД$(51, 74) = 1$, искористимо ли q_i-ове из Еуклидовог алгоритма за одређивање НЗД$(255, 370)$ (напоменимо да су q_i-ови из Еуклидовог алгоритма за одређивање НЗД$(51, 74)$ једнаки q_i-овима из Еуклидовог алгоритма за одређивање НЗД$(255, 370)$), имамо да је $u \equiv 45 \pmod{74}$ рјешење конгруенције $51u \equiv 1 \pmod{74}$. Из тога слиједи да је

$$y \equiv 29 \cdot 45 \equiv 1305 \equiv 47 \pmod{74}$$

рјешење конгруенције $51y \equiv 29 \pmod{74}$. На крају добијамо да су рјешења полазне конгруенције

$$x \equiv 47 + k \cdot 74 \pmod{370}, \quad k = 0, 1, 2, 3, 4 = d - 1 = \text{НЗД}(255, 370) - 1,$$

тј.

$$x \equiv 47, 121, 195, 269, 343 \pmod{370}.$$

4. Мултипликативни инверз у коначном пољу

Ако за прост број p посматрамо просто коначно поље $\mathbf{Z}_p$ чији су елементи остаци при дијељењу бројем p, а операције сабирање и множење модуло p, тада се поставља питање шта представља инверз елемента a у том пољу. Према дефиницији инверза важи да је $x \in \mathbf{Z}_p$ инверз од a ако је x рјешење конгруенције $ax \equiv 1 \pmod{p}$. Тако добијамо да се одређивање мултипликативног инверза a^{-1} елемента a своди на рјешавање линеарне конгруенције. Напоменимо да је и у скупу $\mathbf{Z}_n$, гдје је n природан сложен број, такође могуће на исти начин одредити мултипликативни инверз елемента a. Како је $\text{НЗД}(a, n) \mid 1$ услов да конгруенција $ax \equiv 1 \pmod{n}$ има рјешење, то слиједи да је елемент $a \in \mathbf{Z}_n$ инвертибилан ако је $\text{НЗД}(a, n) = 1$.

Примјер 8. Одредити мултипликативни инверз броја 37 у скупу $\mathbf{Z}_{233}$.

Рјешење. Одредити мултипликативни инверз $37^{-1} \bmod 233$ броја 37 у скупу $\mathbf{Z}_{233}$ значи да треба ријешити конгруенцију $37x \equiv 1 \pmod{233}$. Због тога можемо у потпуности примијенити претходно описани алгоритам.

$$\begin{aligned} 233 &= 37 \cdot 6 + 11 \\ 37 &= 11 \cdot 3 + 4 \\ 11 &= 4 \cdot 2 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 \end{aligned}$$

Добили смо да је $\text{НЗД}(37, 233) = 1$, а како $1 \mid 1$, то наша конгруенција има рјешење па га тражимо помоћу претходно дане рекурзивне релације.

i	-1	0	1	2	3	4
q_i			6	3	2	1
y_i	0	1	-6	19	-44	63

Рјешење конгруенције $37x \equiv 1 \pmod{233}$ је $x \equiv 63 \pmod{233}$, па закључујемо да је 63 мултипликативни инверз броја 37 у скупу $\mathbf{Z}_{233}$, тј. $37^{-1} \equiv 63 \pmod{233}$.

5. Верижни разломци

Дефиниција 4. Нека је q_0 цијели број и нека су $q_1, q_2, \ldots, q_n$ природни бројеви. Тада се израз

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \; q_{n-1} + \cfrac{1}{q_n}}}}$$

назива развој броја α у *коначни једноставни верижни разломак*. Краћи запис је облика $\alpha = [q_0; q_1, \ldots, q_n]$.

Ако је α цијели број, онда постоје тачно два развоја од α у једноставни верижни разломак и то $\alpha = [\alpha]$ и $\alpha = [\alpha - 1, 1]$. Ако је α рационалан, али не цијели број, онда постоје тачно два развоја од α у једноставни верижни разломак и то $\alpha = [q_0; q_1, \ldots, q_n]$, гдје је $q_n \geq 2$, а други је $\alpha = [q_0; q_1, \ldots, q_{n-1}, q_n - 1, 1]$.

Теорема 6. *Сваки рационалан број a/b може бити представљен на јединствен начин у облику једноставног верижног разломка $[q_0; q_1, \ldots, q_n]$, гдје су q_i количници из Еуклидовог алгоритма за одређивање* НЗД(a, b) *и $q_n \neq 1$. Важи и обрат, тј. сваки коначни верижни разломак можемо замијенити њему једнаким рационалним бројем.*

Примјер 9. Одредити развој броја $\dfrac{233}{37}$ у једноставни верижни разломак.

Рјешење. Искористимо ли Еуклидов алгоритам из претходног примјера, добијамо рјешење.

$$\frac{233}{37} = 6 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3}}}}$$

Краћи запис је $\dfrac{233}{37} = [6; 3, 2, 1, 3]$.

Примјер 10. Одредити рационалан број којем одговара једноставни верижни разломак $[0; 2, 1, 5]$.

Рјешење.

$$[0; 2, 1, 5] = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{5}}} = \cfrac{1}{2 + \cfrac{5}{6}} = \frac{6}{17}.$$

На сљедећем примјеру ћемо показати једну примјену верижних разломака за врло једноставно рјешавање једног облика диофантских једначина. Задатак се појавио на математичком такмичењу за 10. разред у Русији [1].

Примјер 11. Ријешити у скупу природних бројева једначину

$$x + \cfrac{1}{y + \cfrac{1}{z}} = \frac{10}{7}.$$

Рјешење. Развијмо број $10/7$ у једноставни верижни разломак.

$$\begin{aligned} 10 &= 7 \cdot 1 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 \end{aligned}$$

Добили смо да важи

$$\frac{10}{7} = 1 + \cfrac{1}{2 + \cfrac{1}{3}} = x + \cfrac{1}{y + \cfrac{1}{z}} = \frac{10}{7}.$$

Како је овај развој јединствен, то је рјешење једначине $(x, y, z) = (1, 2, 3)$.

ЛИТЕРАТУРА

1. I. L. Babinskaja, *Zadaci s ruskih matematičkih natjecanja*, Element, Zagreb, 1999.
2. B. Ibrahimpaxić, *Kriptografija kroz primjere*, Pedagoški fakultet, Bihać, 2011.
3. В. Мићић, З. Каделбург, Д. Ђукић, *Увод у теорију бројева*, ДМС, Београд, 2004.
4. S. Y. Yan, *Number Theory for Computing*, Springer-Verlag, Berlin, 2002.
5. А. Золић, *Верижни разломци и примјене*, Настава математике, XLV 3–4 (2000), 23–30.

Др Бернадин Ибрахимпашић, Педагошки факултет, Универзитет у Бихаћу, Луке Марјановића бб, 77000 Бихаћ, Босна и Херцеговина

E-mail: bernadin@bih.net.ba

Др Ариф Золић, Математички факултет, Универзитет у Београду, Студентски трг 16, 11000 Београд, Србија

E-mail: azolic@diginaut.com