Mr. Amela Helać*
J.U. Gimnazija „Vaso Pelagić“,
Brčko distrikt BiH

UDK 551.5
Originalni naučni rad
Primljen: 29. IV 2014.

RJEŠAVANJE PELOVE JEDNAČINE LAGRANŽOVOM METODOM

SAŽETAK: Pojmovi i iskazi iz teorije brojeva, pri površnom posmatranju mogu izgledati tako jednostavni i nekorisni za praksu. Međutim, ako im se priđe sa pozicije njihove stvarne geneze i njihove historijske evolucije, koji su bitno uslovljeni općom društvenom praksom i zahtjevima matematike kao nauke, a ovi pretpostavljaju indirektno ispoljavanje potreba i zahtjeva opće društvene prakse, onda se situacija mijenja u našim predstavama tih pojmova i iskaza, jer oni nastaju iz stalnog sudaranja čovjeka sa stvarnošću, bez kojeg bi ostali skriveni u čovjeku samo kao mogućnost.

Zato je u teoriji brojeva, kao i u matematici i u svakoj drugoj nauci, vrlo važno razmatrati „sadašnje“ u vezi sa „prošlim“, jer se „sadašnje“ razvilo iz „prošlog“, a isto tako „buduće“ će se razviti iz „sadašnjeg“. Proučavanje „prošlog“ u svakoj nauci, pa i u matematici, a samim tim i u teoriji brojeva, pretvara se u sredstvo kojim se shvata „sadašnje“ i predviđa „buduće“ i tako se osmišljava razvoj svakog matematičkog modela i njegove cjelovite teorije kao historijski proces u okvirima razvoja opće društvene prakse, odnosno u direktnoj ili indirektnoj vezi sa njom. Iz ovoga jasno proizilaze osnovni problemi, zadaci i ciljevi istraživanja kojim se bavi historija matematike.

Predmet istraživanja je rješavanje Pelove jednačine. Da bi smo ilustrovali moguću veličinu brojeva koji se pojavljuju pri rješavanju Pelove jednačine opisan je „Arhimedov problem o govedima“. Daju se i svojstva verižnih razlomaka, radi njihove primjene u rješavanju Pelove jednačine Lagranžovom metodom.

KLJUČNE RIJEČI: Diofant, Pelova jednačina, Arhimedov problem, Lagranžov metod, verižni razlomak, algoritam.

1. Uvod

Na značaj proučavanja historije jedne nauke radi ispoljavanja osobina potrebnih za „vještinu pronalaženja“ ukazivao je još Lajbnic (Leibniz). U jednom radu koji je ostao neobjavljen za njegova života nalaze se ovi redovi: „Veoma je korisno saznati pravo porijeklo izvanrednih pronalazaka, naročito onih do kojih se došlo ne slučajno već snagom ljudske misli. Ovo je korisno ne samo zbog toga što će historija svakome dati svoje i u isti mah probuditi druge da se bore za ista priznanja, već i zbog toga što će poznavanje metoda u izuzetnim primjerima doprinijeti razvoju – vještine pronalaženja.“ [1]

Pelovu jednačinu spominje još Diofant u svom zborniku radova *Aritmetika*, i ona spada u grupu kvadratnih Diofantovih jednačina. Diofant je stari grčki matematičar Helenističkog doba koji je živio u Aleksandriji između 200-214. godine i umro u periodu između 284-298. godine nove ere. Mnogi ga zovu „ocem algebre“.

Danas pod Diofantovom jednačinom smatramo jednačinu oblika

$$D(x_1, x_2, ..., x_n) = 0$$

gdje je D polinom sa cjelobrojnim koeficijentom, a promjenljive uzimaju vrijednosti iz skupa cijelih brojeva.

* amelahelac71@gmail.com

Ovakvim jednačinama i njihovim rješavanjem manje više bavili su se svi velikani matematičke misli od Al Horezmija, preko Ojlera i Lagranža, pa sve do Hilberta. Generalno gledano, iako ne postoji postupak za rješavanje bilo koje Diofantove jednačine, za neke klase jednačina postoje algoritmi rješavanja.[2]

2. Traženje algoritma za rješavanje Pelove jednačine

Definicija 4.2.1. Diofantska jednačina

$$x^2 - dy^2 = 1 \tag{1}$$

gdje $d \in N$ i d nije potpun kvadrat, zove se Pelova jednačina (J. Pell, 1610-1685) (iako J. Pel nije značajnije doprinio njezinom proučavanju). Jednačinu oblika

$$x^2 - dy^2 = N \tag{2}$$

gdje je d kao gore i $N \in ¥$, zovemo pelovska jednačina.

Neki specijalni primjeri Pelove jednačine pojavljuju se još u starogrčko doba. Jedan od primjera navešćemo ovdje. Metode rješavanja takvih jednačina razvijali su indijski matematičari Brahmagupta (Brahmagupta, 598 - oko 660) i Baskara (Bhaskara, 1114-1185).

U modernu matematiku jednačine ovakvog tipa uveo je Ferma (P. Fermat, 1601-1665), tako što je u jednom pismu engleskim matematičarima uputio „izazov“ rješavanja problema: „Za proizvoljan dati broj koji nije kvadrat postoji beskonačno mnogo kvadrata, takvih da ako se takav kvadrat pomnoži datim brojem i proizvodu doda jedinica, rezultat je ponovo kvadrat.“ Drugim riječima, on tvrdi da ako prirodan broj d nije potpun kvadrat, tada jednačina

$$dy^2 + 1 = x^2$$

ima beskonačno mnogo rješenja. Problem su pokušali da riješe engleski matematičari Braunker (W. Brouncker, 1620-1684) i Volis (J. Wallis, 1616-1703). U prvoj varijanti oni su „previdjeli“ uvjet da se rješenje traži u cijelim brojevima, već su jednačinu riješili za racionalne x i y :

$$x = \frac{dn^2 + m^2}{dn^2 - m^2}, \quad y = \frac{2mn}{dn^2 - m^2}, \quad m, n \in ¥ .$$

Ferma je odgovorio da on nikada ne bi postavio tako smiješno lak zadatak. Englezi su se žalili da on naknadno mijenja uvjete zadatka, ali su ipak poslije izvjesnog vremena poslali novo rješenje, koje je u suštini bilo kao i rješenje Baskare. Međutim, Ferma ni ovaj put nije bio zadovoljan, jer je tvrdio (s pravom) da ponuđeni metod rješavanja doduše dovodi do rješenja, ali samo ako se unaprijed pretpostavi da rješenje postoji. Pri tome je tvrdio da on zna dokaz egzistencije rješenja i da ga je izveo metodom „beskonačnog smanjivanja“ koji je koristio i u nekim drugim situacijama. Međutim, taj dokaz, kao ni većinu drugih svojih dokaza nikada nije objavio.

Ojler (L. Euller, 1707-1783) je, proučavajući Fermaovu zaostavštinu, naišao i na prepisku vezanu za navedeni problem i zainteresovao se za njega. Iz nekog razloga on je pogrešno smatrao da je u rješavanju učestvovao jedan drugi engleski matematičar, Pel, te je jednačinu nazvao po njemu. S obzirom na Ojlerov autoritet, taj naziv se zadržao i svi kasniji pokušaji da se jednačini da korektniji naziv nisu uspjeli. Tako se i mi u ovom radu držimo tradicionalne varijante Pelove jednačine.

Sam Ojler je u svojim radovima opisao algoritam za nalaženje rješenja Pelove jednačine, ali čak ni on nije naveo dokaz da taj algoritam uvijek dovodi do rješenja. Prvi dokaz je 1768. godine objavio Lagranž (J. L. Lagrange, 1736-1813). Dokaz je izveden korištenjem verižnih razlomaka i taj metod je i do danas ostao najpoznatiji.

Da bismo ilustrovali moguću veličinu brojeva koji se pojavljuju pri rješavanju Pelove jednačine, u kratkim crtama ćemo opisati dobro poznati „Arhimedov problem o govedima“, koji predstavlja jedan od prvih primjera jednačine ovog oblika, a potom Lagranžov metod za rješavanja Pelove jednačine korištenjem osobina verižnih razlomaka.[3]

2.1. Arhimedov problem o broju goveda

Njemački istraživač Lesing (Lessing, 1729-1821) je pronašao i 1773. godine objavio papirus za koji se smatra da sadrži Arhimedov (Arhimed, 287-212 p.n.e.) pismo Eratostenu iz Kirene (Eratosten, oko 276-194 p.n.e.). U pismu se, u stihovima, govori o tome da je bog Sunce na Siciliji imao krdo goveda. Pri tome su goveda bila od četiri različite vrste – bijela, crna, šarena i smeđa – i naravno, u svakoj vrsti bilo je i krava i volova. U daljem tekstu se daju uvjeti koje su zadovoljavali brojevi krava, odnosno volova u svakoj od tih vrsta. Prevedeno na savremene oznake, ako se sa x, y, z, t označe redom brojevi bijelih, crnih, šarenih i smeđih volova, a sa x', y', z', t' odgovarajući brojevi krava, Arhimedov zadatak je bio postavljen na slijedeći način.

ARHIMEDOV PROBLEM

(a) Odrediti cijele brojeve x, y, z, t kao x', y', z', t' koji zadovoljavaju slijedeći sistem $(3)-(4)$ od sedam linearnih jednačina

$$x = (\frac{1}{2}+\frac{1}{3})y + t, \qquad y = \left(\frac{1}{4}+\frac{1}{5}\right)z + t, \qquad (3)$$

$$z = \left(\frac{1}{6}+\frac{1}{7}\right)x + t$$

$$x' = \left(\frac{1}{3}+\frac{1}{4}\right)(y+y'), \qquad z' = \left(\frac{1}{5}+\frac{1}{6}\right)(t+t'),,$$

$$y' = \left(\frac{1}{4}+\frac{1}{5}\right)(z+z'), \qquad t' = \left(\frac{1}{6}+\frac{1}{7}\right)(x+x'). \qquad (4)$$

(b) Odrediti ono rješenje prethodnog sistema kod kojeg je $x+y$ kvadratni, a $z+t$ trougaoni broj.

Pri tome su, kao što je poznato, stari Grci prirodan broj p zvali trougaonim ako je on oblika $\frac{n(n+1)}{2}$, odnosno (ekvivalentno) ako je $8p+1$ potpun kvadrat.

Dio pod (a) Arhimedovog problema je, bar u principu, sasvim jednostavan. Poslije oslobađanja od razlomaka, imamo linearan diofantski sistem od sedam jednačina sa osam nepoznatih, koji se eliminacijom svodi na jednu jednačinu sa dvije nepoznate (treba paziti i da rješenja

budu prirodni brojevi). Mali problem predstavlja samo to što, bez obzira na jednostavne polazne koeficijente, tokom rada počinju da se dobijaju sve veći brojevi. (Uzgred, poznato je da je Arhimed i inače volio da postavlja i rješava probleme u kojima se pojavljuju
veoma veliki brojevi.) Tako se, rutinskom procedurom, dobija da sistem (3) zadovoljavaju četvorke prirodnih brojeva oblika

$$(x, y, z, t) = k \cdot (2226, 1602, 1580, 891), \quad k \in ¥ .$$

Da bi i sistem (4) imao prirodna rješenja mora biti $k = 4657 \cdot l, \quad l \in ¥$. Tada je

$$(x', y', z', t') = l \cdot (7206360, 4893246, 3515820, 5439213).$$

Stvari, dakle, počinju da izmiču kontroli. A najteže tek dolazi. Jer, dio zadatka pod (a) je za Arhimeda bilo tek „zagrijevanje"- glavni dio je bio zadatak pod (b) Treba, dakle, odrediti prirodan broj l (što je moguće manji) tako da broj

$$x + y = 4567 \cdot 3828 \cdot l \tag{5}$$

bude potpun kvadrat, a da broj

$$z + t = 4657 \cdot 2471 \cdot l \tag{6}$$

bude trougaoni. Kako je $4657 \cdot 3828 = 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657$ (broj 4657 je prost), uvjet (5) će biti ispunjen ako je $l = am^2$, gdje je $a = 3 \cdot 11 \cdot 29 \cdot 4657$, a m je cio broj. Da bi broj $z + t$ bio trougaoni, tj. da bi $8(z + t) + 1$ bio potpun kvadrat (npr. jednak n^2), mora biti, na osnovu (6),

$$n^2 = 8(z + t) + 1 = 8 \cdot 4657 \cdot 2471 \cdot am^2 + 1$$

pa tako za nalaženje brojeva m i n dobijamo Pelovu jednačinu

$$n^2 = dm^2 + 1,$$

gdje je

$$d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 \cdot (2 \cdot 4657)^2 = 410286423278424.$$

Ako se pozovemo na Lagranžov rezultat, znamo da ova jednačina ima beskonačno mnogo rješenja i da se sva ona mogu lako naći ako se prvo pronađe najmanje od njih. Ali kako doći do tog najmanjeg rješenja i koliko je ono? Skoro je sigurno da ni sam Arhimed to nije znao.

Naime, poslije Lesingovog otkrića, mnogi matematičari su, znajući i Laganžov metod verižnih razlomaka, pokušavali da to rješenje pronađu. Poslije više neuspješnih pokušaja tek je 1880. godine njemački matematičar Amtor (A. Amtor) uspio da dokaže da najmanje rješenje (tačnije, najmanji ukupan broj goveda), predstavljeno u dekadnom zapisu ima 206545 cifara! Amtor je pokušao i da nađe bar neke od tih cifara, ali je već četvrta bila pogrešna.

Tačan zapis ovog najmanjeg rješenja je nađen tek u eri računara i 1980. godine je objavljeno to rješenje koje u originalu zauzima 47 stranica kompjuterskog listinga. Navešćemo neke od cifara:

$$77602714...237983357...55081800,$$

gdje svaka od šest tačaka zamjenjuje 34420 izostavljenih cifara.
Kažu da su se neki od matematičara XIX vijeka „zabrinuli" da li je toliki broj goveda mogao da stane na ostrvo Siciliju. Lesing je i na to odgovorio: „Ako su ona pripadala bogu Sunca, valjda se on nekako potrudio da ih tamo smjesti."[4]

2.2. Lagranžov metod rješavanje Pelove jednačine korištenjem osobina verižnih razlomaka

Žozef-Luj Lagranž (fr. Joseph-Louis, comte de Lagrange, 1736-1813) je bio italijansko-francuski matematičar i astronom, koji je dao važan doprinos na svim poljima analize i teorije brojeva kao i klasične i nebeske mehanike. Smatra se najvećim matematičarem XVIII vijeka. Govorilo se da je mogao na svojim papirima da piše bez ijedne greške.

2.2.1. Diofantske aproksimacije

Definicija 2.2.1.1. Verižni razlomak je izraz oblika:

$$\alpha = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \mathrm{O}}}}$$

gdje su a_i, b_i proizvoljni izrazi. Jednostavan verižni razlomak je verižni razlomak kojem su svi b_i jednaki 1.

Neka je α proizvoljan realan broj. S $\lfloor \alpha \rfloor$ ćemo označavati najveći cijeli broj koji nije veći od α, a s $\{\alpha\}$ realan broj $\alpha - \lfloor \alpha \rfloor$. Stavimo: $a_0 = \lfloor \alpha \rfloor$. Ako je $a_0 \neq \alpha$, onda zapišemo α u obliku $\alpha = a_0 + \frac{1}{\alpha_1}$, tako da je $\alpha_1 > 1$, i stavimo $a_1 = \lfloor \alpha_1 \rfloor$. Ako je $a_1 \neq \alpha_1$, onda α_1 zapišemo u obliku $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, tako da je $\alpha_2 > 1$, i stavimo $a_2 = \lfloor \alpha_2 \rfloor$. Ovaj proces možemo nastaviti u nedogled, ukoliko nije $a_n = \alpha_n$ za neki n. Jasno je da ako je $a_n = \alpha_n$ za neki n, onda je α racionalan broj. Naime, tada je

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \mathrm{O}_{\frac{1}{a_n}}}}$$

Ovo ćemo kraće zapisivati u obliku $\alpha = [a_0, a_1, ..., a_n]$. Tako ćemo imati $a_0 \in ¢$ i $a_n \in ¥, n = 1, 2, ...$

Pretpostavimo sada da je $a_n \neq \alpha_n$ za sve n. Definirajmo racionalne brojeve $\frac{p_n}{q_n}$ sa

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

Teorema 2.2.1.1. Za sve $n \geq -1$ vrijedi: $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$

Dokaz: Teoremu dokazujemo indukcijom. Za $n = -1$ imamo:

$$q_{-1} p_{-2} - p_{-1} q_{-2} = 0 \cdot 0 - 1 \cdot 1 = (-1)^{-1}.$$

Pretpostavimo da tvrdnja vrijedi za $n-1$. Tada je:

$$q_n p_{n-1} - p_n q_{n-1} = \left(a_n q_{n-1} + q_{n-2}\right) p_{n-1} - \left(a_n p_{n-1} + p_{n-2}\right) q_{n-1} =$$
$$= -\left(q_{n-1} p_{n-2} - p_{n-1} q_{n-2}\right) = -\left(-1\right)^{n-1} = \left(-1\right)^n .$$

Definicija 2.2.1.2. Ako je a_0 cijeli broj, $a_1,...,a_n$ prirodni brojevi, te ako je $\alpha = \left[a_0, a_1,..., a_n\right]$, onda ovaj izraz zovemo razvoj broja α u konačni jednostavni verižni (neprekidni) razlomak; $\frac{p_i}{q_i} = \left[a_0,..., a_i\right]$ je i-ta konvergenta od α, a_i je i-ti parcijalni kvocijent od α, a $\alpha_i = \left[a_i, a_{i+1},..., a_n\right]$ je i-ti potpuni kvocijent od α.

Ako je α iracionalan broj, onda uvodimo oznaku $\lim_{n\to\infty}\left[a_0, a_1,..., a_n\right] = \left[a_0, a_1, a_2,...\right]$.

Ako je $\alpha = \left[a_0, a_1, a_2,...\right]$, onda ovaj izraz zovemo razvoj od α u (beskonačni) jednostavni verižni razlomak; $\frac{p_i}{q_i} = \left[a_0,..., a_i\right]$ je i-ta konvergenta od α, a_i je i-ti parcijalni kvocijent, a $\alpha_i = \left[a_i, a_{i+1},...\right]$ je i-ti potpuni kvocijent od α.

Teorema 2.2.1.2. Ležendr (Legendre) Neka su p, q cijeli brojevi takvi da je $q \geq 1$ i $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$ tada je $\frac{p}{q}$ neka konvergenta od α.

Dokaz: Izvedimo prvo jednu pomoćnu jednakost. Ako je $\alpha = \left[a_0, a_1,..., a_n, a_{n+1}\right]$

Važiće

$$q_n\alpha - p_n = q_n \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} - p_n = \frac{\left(-1\right)^n}{\alpha_{n+1} q_n + q_{n-1}}. \qquad (7)$$

Možemo pretpostaviti da je $\alpha \neq \frac{p}{q}$ inače je tvrdnja trivijalno zadovoljena. Tada možemo pisati $\alpha - \frac{p}{q} = \frac{\varepsilon\vartheta}{q^2}$, gdje je $0 < \vartheta < \frac{1}{2}$ i $\varepsilon = \pm 1$. Neka je $\frac{p}{q} = \left[b_0, b_1,..., b_{n-1}\right]$ razvoj od $\frac{p}{q}$ u jednostavni verižni razlomak, gdje je n izabran tako da vrijedi $\left(-1\right)^{n-1} = \varepsilon$. To uvijek možemo postići jer je $\left[a_0, a_1,..., a_m\right] = \left[a_0, a_1,..., a_m - 1, 1\right]$.

Definirajmo ω sa $\alpha = \frac{\omega p_{n-1} + p_{n-2}}{\omega q_{n-1} + q_{n-2}}$ tako da je $\alpha = \left[b_0, b_1,..., b_{n-1}, \omega\right]$.

Sada će zbog jednakosti (7) važiti

$$\frac{\varepsilon\vartheta}{q^2} = \alpha - \frac{p}{q} = \frac{1}{q_{n-1}}\left(\alpha q_{n-1} - p_{n-1}\right) = \frac{1}{q_{n-1}} \cdot \frac{\left(-1\right)^{n-1}}{\omega q_{n-1} + q_{n+2}}.$$

Rješavanjem ove relacije po ω dobijamo $\omega = \frac{1}{\vartheta} - \frac{q_{n-2}}{q_{n-1}}$. Odavdje slijedi da je $\omega > 2 - 1 = 1$. Razvijmo ω u (konačan ili beskonačan) jednostavan verižni razlomak $\omega = \left[b_n, b_{n+1}, b_{n+2},...\right]$. Budući da je $\omega > 1$, svi $b_j\ \left(j = n, n+1,...\right)$ su prirodni brojevi. Stoga je

$$\alpha = [b_0, b_1, ..., b_{n-1}, b_n, b_{n+1}, ...]$$

razvoj u jednostavni verižni razlomak od α i $\frac{p}{q} = \frac{p_{n-1}}{q_{n-1}} = [b_0, b_1, ..., b_{n-1}]$ je konvergenta od α, što je i trebalo dokazati.

Definicija 2.2.1.3. Za beskonačni verižni razlomak $[a_0, a_1, a_2, ...]$ kažemo da je periodski ako postoje cijeli brojevi $k \geq 0, m \geq 0$ takvi da je $a_{m+n} = a_n$ za sve $n \geq k$. U tom slučaju verižni razlomak pišemo u obliku

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

gdje „crta“ iznad brojeva $a_k, ..., a_{k+m-1}$ znači da se taj blok brojeva ponavlja u nedogled.

Definicija 2.2.1.4. Za iracionalan broj α kažemo da je kvadratna iracionalnost ako je α korijen kvadratne jednačine s racionalnim koeficijentima.

Teorema 2.2.1.3. (Ojler, Lagranž) Razvoj u jednostavni verižni razlomak realnog broja α je periodski ako i samo ako je α kvadratna iracionalnost.

Dokaz: Neka je $\alpha = \left[b_0, b_1, ..., b_{k-1}, \overline{a_0, a_1, ..., a_{m-1}}\right]$, te neka je $\beta = \left[\overline{a_0, a_1, ..., a_{m-1}}\right]$, tj. neka je β čisto periodski dio od α. Iz $\beta = [a_0, a_1, ..., a_{m-1}, \beta]$ slijedi da je

$$\beta = \frac{\beta p_{m-1} + p_{m-2}}{\beta q_{m-1} + q_{m-2}},$$

a to je kvadratna jednačina za β (s racionalnim koeficijentima). Budući da je β iracionalan (jer mu je razvoj beskonačan), to je β kvadratna iracionalnost.

Kako je $\alpha = [b_0, b_1, ..., b_{k-1}, \beta]$ biće $\alpha = \frac{\beta p + p'}{\beta p + q'}$, (8)

gdje su $\frac{p}{q}$ i $\frac{p'}{q'}$ zadnje dvije konvergente od $[b_0, b_1, ..., b_{k-1}]$. Međutim, β ima oblik $\frac{a + \sqrt{b}}{c}$ pa iz (8) slijedi da i α ima isti oblik, pa zaključujemo pošto je α iracionalan da je i α kvadratna iracionalnost. Prvi dio teoreme je dokazan.

Dokažimo sada obrnuto. Neka je α kvadratna iracionalnost, tj. neka je oblika $\frac{a + \sqrt{b}}{c}$, gdje $a, b, c \in ¢, b > 0, c \neq 0$ i b nije potpun kvadrat. Množeći brojnik i nazivnik od α sa $|c|$, dobijamo

$$\alpha = \frac{ac + \sqrt{bc^2}}{c^2} \quad \text{ili} \quad \alpha = \frac{-ac + \sqrt{bc^2}}{-c^2},$$

u zavisnosti da li je c pozitivan ili negativan broj. Stoga α možemo pisati u obliku $\alpha = \frac{s_0 + \sqrt{d}}{t_0}$, gdje su $s_0, t_0, d \in ¢, t_0 \neq 0, d$ nije potpun kvadrat i $t_0 \mid \left(d - s_0^2\right)$.

Sada ćemo opisati razvoj $[a_0, a_1, ...]$ u jednostavni verižni razlomak broja α.

Neka je $\alpha_0 = \alpha$, te neka je

$$\alpha_i = \lfloor \alpha_i \rfloor, \quad \alpha_i = \frac{s_i + \sqrt{d}}{t_i}, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i} \tag{9}$$

Važiće da je

$$\alpha_i - a_i = \frac{s_i + \sqrt{d}}{t_i} - a_i = \frac{s_i + \sqrt{d} - a_i t_i}{t_i} = \frac{\sqrt{d} - s_{i+1}}{t_i} = \frac{d - s_{i+1}^2}{t_i\left(\sqrt{d} + s_{i+1}\right)} = \frac{t_{i+1}}{\sqrt{d} + s_{i+1}} = \frac{1}{\alpha_{i+1}},$$

pa je zaista $\alpha = [a_0, a_1, ...]$.

Dokažimo sada matematičkom indukcijom da su s_i, t_i cijeli brojevi takvi da je $t_i \neq 0$ i $t_i \mid \left(d - s_i^2\right)$. Po pretpostavci tvrđenje je tačno za $i = 0$. Ako tvrdnja vrijedi za neko i, onda iz $s_{i+1} = a_i t_i - s_i$ slijedi da je broj s_{i+1} cijeli. Relacija

$$t_{i+1} = \frac{d - s_{i+1}^2}{t_i} = \frac{d - s_i^2}{t_i} + 2a_i s_i - a_i^2 t_i$$

pokazuje da je i t_{i+1} cijeli broj. Dalje će biti $t_{i+1} \neq 0$, jer bi u suprotnom bilo $d = s_{i+1}^2$, što nije moguće jer d nije potpun kvadrat. Konačno kako $t_i \in ¢$ i kako $t_i = \frac{d - s_{i+1}^2}{t_{i+1}}$ slijedi $t_{i+1} \mid \left(d - s_{i+1}^2\right)$.

Ostaje još da pokažemo da je verižni razlomak $[a_0, a_1, a_2, ...]$ periodičan. Sa α_i' označimo konjugat od α_i, tj. $\alpha_i' = \frac{s_i - \sqrt{d}}{t_i}$. Budući da je konjugat količnika jednak količniku konjugata, imamo: $\alpha_0' = \frac{\alpha_n' p_{n-1} + p_{n-2}}{\alpha_n' q_{n-1} + q_{n-2}}$.

Odavdje je $\alpha_n' = -\frac{q_{n-2}}{q_{n-1}}\left(\frac{\alpha_0' - \frac{p_{n-2}}{q_{n-2}}}{\alpha_0' - \frac{p_{n-1}}{q_{n-1}}}\right)$.

Kada n teži u ∞, $\frac{p_{n-1}}{q_{n-1}}$ i $\frac{p_{n-2}}{q_{n-2}}$ teže prema α_0, a $\alpha_0 \neq \alpha_0'$. Stoga izraz u zagradi teži prema 1, pa je zbog toga pozitivan za dovoljno velike n, recimo za $n > N$. Sada je za $n > N$ broj α_n' negativan. No, α_n je pozitivan za $n \geq 1$, pa je

$$\alpha_n - \alpha_n' = \frac{s_n + \sqrt{d}}{t_n} - \frac{s_n - \sqrt{d}}{t_n} = \frac{2\sqrt{d}}{t_n} > 0 .$$

Dakle, $t_n > 0$ za $n > N$.

Kako sada znamo da je za $n > N$ i $t_n \in N$ biće za $n > N$ tačna nejednakost:

$$t_n \leq t_n t_{n+1} = d - s_{i+1}^2 < d .$$

Stoga za $n > N$ t_n može poprimiti samo vrijednosti iz skupa $\{1, 2, ..., d-1\}$.

Nadalje, za $n > N$ imamo:

$$s_n^2 < s_n^2 + t_{n-1}t_n = d \Rightarrow |s_n| < \sqrt{d}\,,$$

dok iz $\alpha_n > 1$ i upravo dokazanog slijedi

$$t_n < s_n + \sqrt{d} < 2\sqrt{d}$$

Odavdje slijedi da uređeni parovi (s_n, t_n) mogu poprimiti samo konačno mnogo vrijednosti, pa postoje prirodni brojevi j, k, $j < k$ takvi da je $s_j = s_k, t_j = t_k$. Sada (9) povlači da je $\alpha_j = \alpha_k$, pa je $\alpha = \left[a_0, ..., a_{j-1}, \overline{a_j, a_{j+1}, ..., a_{k-1}}\right]$, što je i trebalo dokazati.

Teorema 2.2.1.4. Kvadratna iracionalnost α ima čisto periodski razvoj u jednostavni verižni razlomak ako i samo ako je $\alpha > 1$, te $-1 < \alpha' < 0$, gdje je α' konjugat od α. (Za takvu kvadratnu iracionalnost kažemo da je reducirana.)

Dokaz: Neka je $\alpha > 1$ i $-1 < \alpha' < 0$. Stavimo $\alpha_0 = \alpha$, te definirajmo α_i rekurzivno sa $\frac{1}{\alpha_{i+1}} = \alpha_i - a_i$. Tada je $\frac{1}{\alpha'_{i+1}} = \alpha'_i - a_i$. (10)

Sada je $a_i \geq 1$ za sve $i \geq 0$ (čak i za $i = 0$ zbog $\alpha > 1$). Zbog toga, ako je $\alpha'_i < 0$, onda je $\frac{1}{\alpha_{i+1}} < -1$, odnosno $-1 < \alpha'_{i+1} < 0$. Budući da je $-1 < \alpha'_0 < 0$, indukcijom slijedi da je $-1 < \alpha'_i < 0$ za sve $i \geq 0$. Sada iz (10) slijedi

$$0 < -\frac{1}{\alpha'_{i+1}} - a_i < 1, \quad \text{tj.} \quad a_i = \left\lfloor -\frac{1}{\alpha'_{i+1}} \right\rfloor.$$

Iz teoreme 2.2.1.3. slijedi da postoje prirodni brojevi takvi da je $j < k$ i $\alpha_j = \alpha_k$. Sada je $\alpha'_j = \alpha'_k$, te

$$a_{j-1} = \left\lfloor -\frac{1}{\alpha'_j} \right\rfloor = \left\lfloor -\frac{1}{\alpha'_k} \right\rfloor = a_{k-1},$$

$$\alpha_{j-1} = a_{j-1} + \frac{1}{\alpha_j} = a_{k-1} + \frac{1}{\alpha_k} = \alpha_{k-1}.$$

Dakle, $\alpha_j = \alpha_k$ povlači da je $\alpha_{j-1} = \alpha_{k-1}$. Primijenimo li ovu implikaciju j puta, dobijamo

$$\alpha_0 = \alpha_{k-j}, \text{ tj. } \alpha = \left[\overline{a_0, a_1, \ldots, a_{k-j}}\right].$$

Obrnuto, pretpostavimo da je razvoj od α čisto periodski, $\alpha = \left[\overline{a_0, a_1, \ldots, a_{n-1}}\right]$, $a_0, a_1, \ldots, a_{n-1} \in \mathrm{N}$ (zbog $a_0 = a_n$). Imamo: $\alpha > a_0 \geq 1$.

Također je $\alpha = [a_0, \ldots, a_{n-1}, \alpha] = \frac{\alpha p_{n-1} + p_{n-2}}{\alpha q_{n-1} + q_{n-2}}$.

Prema tome, α zadovoljava jednačinu

$$f(x) = x^2 q_{n-1} + x(q_{n-2} - p_{n-1}) - p_{n-2} = 0$$

Ova kvadratna jednačina ima dva korijena, α i α'. Budući da je $\alpha > 1$, dovoljno je provjeriti da $f(x)$ ima korijen između -1 i 0. To ćemo provjeriti tako da pokažemo da $f(-1)$ i $f(0)$ imaju različite predznake.

Najprije je $f(0) = -p_{n-2} < 0$, a potom $f(-1) = q_{n-1} - q_{n-2} + p_{n-1} - p_{n-2} > 0$. [5]

2.2.2. Rješavanja Pelove jednačine

Rekli smo već da diofantska jednačina

$$x^2 - dy^2 = 1,$$

gdje je $d \in \mathrm{N}$ i d nije potpun kvadrat, zove se Pelova jednačina.

Ako je d cijeli broj takav da je $d < 0$ ili je d potpun kvadrat, onda očito jednačine (1) i (2) imaju konačno mnogo rješenja. Koristeći razvoj u verižni razlomak broja $\sqrt{d}$ pokazat ćemo da Pelova jednačina uvijek ima beskonačno mnogo rješenja.

Teorema 2.2.2.1. Ako prirodan broj d nije potpun kvadrat, onda razvoj u jednostavni verižni razlomak od $\sqrt{d}$ ima oblik

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

gdje je $a_0 = \lfloor \sqrt{d} \rfloor$, a $a_1, \ldots, a_{r-1}$ su centralno simetrični, tj. $a_1 = a_{r-1}$, $a_2 = a_{r-2}$, ... Nadalje, u (11) uz $\alpha_0 = \sqrt{d}$, $t_0 = 1$, $s_0 = 0$, imamo $t_i \neq -1$, te $t_i = 1$ ako i samo ako $r \mid i$ (ovdje r označava duljinu najmanjeg perioda u razvoju od $\sqrt{d}$).

Dokaz: Promotrimo broj $\beta = \sqrt{d} + \lfloor \sqrt{d} \rfloor$. Očito je broj β reduciran, pa po teoremi 2.2.1.3. ima čisto periodičan razvoj

$$\sqrt{d} + \lfloor \sqrt{d} \rfloor = \left[\overline{b_0, b_1, \ldots, b_{r-1}}\right] = \left[b_0, \overline{b_1, \ldots, b_{r-1}, b_0}\right]. \qquad (11)$$

Razvoji od β i $\sqrt{d}$ se razlikuju samo u prvom članu, tj. $b_i = a_i$ za $i \geq 1$.

Uočimo da je $b_0 = \left\lfloor \sqrt{d} + \lfloor d \rfloor \right\rfloor = 2\left\lfloor \sqrt{d} \right\rfloor$. Sada je

$$\begin{aligned}\sqrt{d} &= -\lfloor \sqrt{d} \rfloor + \beta = -\lfloor \sqrt{d} \rfloor + \left[2\lfloor \sqrt{d} \rfloor, \overline{b_1, \ldots, b_{r-1}, b_0}\right] \\ &= \left[\lfloor \sqrt{d} \rfloor, \overline{b_1, \ldots, b_{r-1}, b_0}\right] = \left[a_0, \overline{a_1, \ldots, a_{r-1}, 2a_0}\right].\end{aligned}$$

Da bi smo dokazali centralnu simetričnost, uočimo da je $\beta = b_0 + \frac{1}{\beta_1}$, gdje je

$$\beta_1 = \left(\sqrt{d} - \lfloor \sqrt{d} \rfloor\right)^{-1} = -\frac{1}{\beta'} = -\frac{1}{\beta'_r} = (\text{zbog 10}) = \left[b_{r-1}, -\frac{1}{\beta'_{r-1}}\right] = \ldots$$

$$= \left[b_{r-1}, b_{r-2}, \ldots, b_0, -\frac{1}{\beta'}\right] = \left[\overline{b_{r-1}, b_{r-2}, \ldots, b_0}\right].$$

Dakle, $\beta = \left[b_0, \overline{b_{r-1}, b_{r-2}, \ldots, b_0}\right]$. Usporedimo li ovo s (11), dobijamo: $b_1 = b_{r-1}, b_{r-2}, \ldots$.

Budući da je r duljina najmanjeg perioda, imamo da je $\beta_i = \beta$ ako i samo ako $r \mid i$.

Ako sada primijenimo algoritam (9) na $\beta_0 = \sqrt{d} + \lfloor \sqrt{d} \rfloor$, $t_0 = 1$, $s_0 = \lfloor \sqrt{d} \rfloor$, onda za sve $j \geq 0$ imamo: $\frac{s_{jr} + \sqrt{d}}{t_{jr}} = \beta_{jr} = \beta_0 = \frac{s_0 + \sqrt{d}}{t_0} = \lfloor \sqrt{d} \rfloor + \sqrt{d}$,

odnosno $s_{jr} - t_{jr}\lfloor\sqrt{d}\rfloor = (t_{jr} - 1)\sqrt{d}$, pa je $t_{jr} = 1$ jer je $\sqrt{d}$ iracionalan.

Nadalje, $t_i \neq 1$ za sve ostale vrijednosti od i.

Zaista, $t_i = 1$ povlači $\beta_i = s_i + \sqrt{d}$. Međutim, β_i ima čisto periodski razvoj, pa je, po teoremi 2.2.1.4., $-1 < s_i - \sqrt{d} < 0$. Odavdje je $\sqrt{d} - 1 < s_i < \sqrt{d}$, tj. $s_i = \lfloor\sqrt{d}\rfloor$, pa je $\beta_i = \beta$, što povlači da $r \mid i$.

Neka je sada $t_i = -1$. Onda je $\beta = -s_i - \sqrt{d}$, pa teorema 2.2.1.4. povlači da je $-s_i - \sqrt{d} > 1$ i $-1 < -s_i + \sqrt{d} < 0$, pa je $\sqrt{d} < s_i < -\sqrt{d} - 1$, što je očito nemoguće.

Teorema 2.2.2.2. Ako je $\frac{p_n}{q_n}$ konvergenta u verižnom razvoju od $\sqrt{d}$ onda je

$p_n^2 - dq_n^2 = (-1)^{n+1} t_{n+1}$, za sve $n \geq -1$.

Dokaz: Iz (9) imamo:

$$\sqrt{d} = \alpha_0 = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} = \frac{(s_{n+1} + \sqrt{d}) p_n + t_{n+1} p_{n-1}}{(s_{n+1} + \sqrt{d}) q_n + t_{n+1} q_{n-1}}.$$

Budući da je $\sqrt{d}$ iracionalan, odavde slijedi

$$s_{n+1} q_n + t_{n+1} q_{n-1} - p_n = 0, \quad s_{n+1} p_n + t_{n+1} p_{n-1} - dq_n = 0.$$

Eliminirajući s_{n+1}, dobijamo

$$p_n^2 - dq_n^2 = (p_n q_{n-1} - p_{n-1} q_n) t_{n+1} = (-1)^{n-1} t_{n+1}$$

Teorema 2.2.2.3. Neka je d prirodan broj koji nije potpun kvadrat, te neka su $\frac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Neka je N cijeli broj, $|N| < \sqrt{d}$. Tada svako pozitivno rješenje $x = u$, $y = v$ jednačine $x^2 - dy^2 = N$, takvo da je $(u, v) = 1$, zadovoljava $u = p_n$, $v = q_n$ za neki $n \in \mathrm{N}$.

Dokaz: Neka su E i M prirodni brojevi takvi da je $(E, M) = 1$ i $E^2 - \rho M^2 = \sigma$, gdje je $\sqrt{\rho}$ iracionalan i $0 < \sigma < \sqrt{\rho}$. Ovdje su ρ i σ realni brojevi, ne nužno cijeli. Tada je

$\frac{E}{M} - \sqrt{\rho} = \frac{\sigma}{M\left(E + M\sqrt{\rho}\right)}$ pa je

$$0 < \frac{E}{M} - \sqrt{\rho} < \frac{\sqrt{\rho}}{M\left(E + M\sqrt{\rho}\right)} = \frac{1}{M^2\left(\frac{E}{M\sqrt{\rho}} + 1\right)} < \frac{1}{2M^2}.$$

Po teoremi 2.2.1.2., $\frac{E}{M}$ je konvergenta u razvoju od $\sqrt{\rho}$.

Ako je $N > 0$, uzmimo $\sigma = N$, $\rho = d$, $E = u$, $M = v$, pa dobijamo tvrdnju teoreme u ovom slučaju.

Ako je $N<0$, onda je $v^2-\frac{1}{d}u^2=-\frac{N}{d}$, pa možemo uzeti $\sigma=-\frac{N}{d}$, $\rho=\frac{1}{d}$, $E=v$, $M=u$. Dobijamo da je $\frac{v}{u}$ konvergenta u razvoju od $\frac{1}{\sqrt{d}}$. No, ako je $\frac{v}{u}$ n-ta konvergenta od $\frac{1}{\sqrt{d}}$, onda je $\frac{u}{v}$ $(n-1)$-va konvergenta od $\sqrt{d}$, pa je teorema dokazana i u ovom slučaju.

Iz teorema 2.2.2.1., 2.2.2.2. i 2.2.2.3. neposredno slijedi

Teorema 2.2.2.4. Sva rješenja u prirodnim brojevima jednačina $x^2-dy^2=\pm 1$ nalaze se među $x=p_n$, $y=q_n$, gdje su $\frac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$.

Neka je r duljina perioda u razvoju od $\sqrt{d}$.

Ako je r paran, onda jednačina $x^2-dy^2=-1$ nema rješenja, a sva rješenja od $x^2-dy^2=1$ su dana sa $x=p_{nr-1}$, $y=q_{nr-1}$ za $n\in \mathrm{N}$.

Ako je r neparan, onda su sva rješenja jednačine $x^2-dy^2=-1$ dana sa $x=p_{nr-1}$, $y=q_{nr-1}$ za n neparan, dok su sva rješenja jednačine $x^2-dy^2=1$ dana sa $x=p_{nr-1}$, $y=q_{nr-1}$ za n paran.

Teorema 2.2.2.5. Ako je (x_1, y_1) najmanje rješenje u prirodnim brojevima jednačine $x^2-dy^2=1$, onda su sva rješenja ove jednačine dana sa (x_n, y_n) za $n\in \mathrm{N}$, gdje su x_n i y_n prirodni brojevi definirani sa

$$x_n+y_n\sqrt{d}=\left(x_1+y_1\sqrt{d}\right)^n. \qquad (12)$$

Dokaz: Iz (12) slijedi $x_n-y_n\sqrt{d}=\left(x_1-y_1\sqrt{d}\right)^n$, pa je

$$x_n^2-dy_n^2=\left(x_1^2-dy_1^2\right)^n=1,$$

što znači da su (x_n, y_n) zaista rješenja.

Pretpostavimo sada da je (s,t) rješenje koje se ne nalazi u familiji $\{(x_n, y_n): n\in \mathrm{N}\}$.

Budući da je $x_1+y_1\sqrt{d}>1$ i $s+t\sqrt{d}>1$, to postoji $m\in \mathrm{N}$ takav da je

$$\left(x_1+y_1\sqrt{d}\right)^m<s+t\sqrt{d}<\left(x_1+y_1\sqrt{d}\right)^{m+1}. \qquad (13)$$

Pomnožimo li (13) sa $\left(x_1-y_1\sqrt{d}\right)^m$, dobijamo

$1<\left(s+t\sqrt{d}\right)\left(x_1-y_1\sqrt{d}\right)^m<x_1+y_1\sqrt{d}$.

Definirajmo $a, b\in \mathrm{Z}$ s $a+b\sqrt{d}=\left(s+t\sqrt{d}\right)\left(x_1-y_1\sqrt{d}\right)^m$. Imamo:

$a^2-db^2=\left(s^2-dt^2\right)\left(x_1^2-dy_1^2\right)^m=1$. Iz $a+b\sqrt{d}>1$ slijedi $0<a-b\sqrt{d}<1$, pa je

$2a=\left(a+b\sqrt{d}\right)+\left(a-b\sqrt{d}\right)>0$,

$2b\sqrt{d}=\left(a+b\sqrt{d}\right)-\left(a-b\sqrt{d}\right)>0$.

Stoga je (a,b) rješenje u prirodnim brojevima jednačine $x^2-dy^2=1$ i $a+b\sqrt{d}<x_1+y_1\sqrt{d}$ što je kontradikcija.

Teorema 2.2.2.6. Neka je (x_n, y_n), $n \in \mathrm{N}$ niz svih rješenja Pelove jednačine $x^2 - dy^2 = 1$ u prirodnim brojevima, zapisan u rastućem redoslijedu. Uzmimo da je $(x_0, y_0) = (1, 0)$. Tada vrijedi:

$x_{n+2} = 2x_1x_{n+1} - x_n$, $\quad y_{n+2} = 2x_1y_{n+1} - y_n$, $\quad n \geq 0$.

Dokaz: Vrijedi: $x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n$. Odavde je

$$\left(x_{n+1} + y_{n+1}\sqrt{d}\right)\left(x_1 + y_1\sqrt{d}\right) = x_{n+2} + y_{n+2}\sqrt{d},$$
$$\left(x_{n+1} + y_{n+1}\sqrt{d}\right)\left(x_1 - y_1\sqrt{d}\right) = x_n + y_n\sqrt{d}.$$

Sada imamo:

$$x_{n+2} = x_1x_{n+1} + dy_1y_{n+1},$$
$$x_n = x_1x_{n+1} - dy_1y_{n+1},$$

Odakle zbrajanjem dobijamo $x_{n+2} = 2x_1x_{n+1} - x_n$. Analogno je

$$y_{n+2} = x_1y_{n+1} + y_1x_{n+1},$$
$$y_n = x_1y_{n+1} - y_1x_{n+1},$$

pa ponovo zbrajanjem dobijamo $y_{n+2} = 2x_1y_{n+1} - y_n$. [5]

3. Zaključak

Generalno gledano, iako ne postoji jedinstven postupak za rješavanje bilo koje Diofantove jednačine, za neke klase jednačina postoje algoritmi rješavanja. U radu smo istraživali jednu od Diofantovih kvadratnih jednačina kod koje je moguće naći algoritam za njeno rješavanje. To je, takozvana, Pelova jednačina. Da bismo ilustrovali moguću veličinu brojeva koji se pojavljuju pri rješavanju Pelove jednačine, u kratkim crtama smo opisali dobro poznati „Arhimedov problem o govedima“, koji predstavlja jedan od prvih primjera jednačine ovog oblika. Kako bi smo došli do njenog rješenja koristili smo Lagranžov metod rješavanja, te zbog toga uveli pojam verižnih razlomaka. Na taj način smo došli do algoritma za rješavanje Pelove jednačine.

S tačke gledišta teorijskog matematičara, kada se dokaže da neki problem ima rješenje, i još se nađe algoritam kako se do tog rješenja dolazi, problem prestaje da bude interesantan. Međutim, u ovom slučaju ima još mnogo izazova koje postavlja rješavanje Pelove jednačine, a neki od njih bi mogli biti interesantni i „najtvrđim“ teoretičarima. Naime, čak i za relativno male brojeve *d*, rješenja, čak i najmanja, naše jednačine mogu biti prilično velika. Pogotovo je to tako ako je i samo *d* veliki broj. To postavlja problem nalaženja što efikasnijeg algoritma rješavanja koji bi u što kraćem (računarskom) vremenu doveo do rješenja, kao i procjene brzine takvog algoritma.

LITERATURA

[1] Gotfried W. Lajbnic: Matematische Schtiften Bd. V, Hall, 1858.
[2] www.hazu.hr/~duda/diofant.html
[3] Zoran Kadelburg: *Još jednom o Pelovoj jednačini*
(elib.mi.sanu.ac.rs/files/journals/nm/.../nm471203.pd...)

[4] H. W. Lenstra Jr., Solving the Pell equation, Notices of the American Mathematical Society 49,2 (2002), 182-192

[5] Andrej Dujella: *Uvod u teoriju brojeva*. Zagreb: PMF Matematički odjel Sveučilišta u Zagrebu.

(http://web.math.hr/~duje/utb/utblink.pdf)

Amela Helać. M.Sc.

SOLVING THE PELL EQUATION BY THE LAGRANGE'S THEOREM METHOD

Summary

The terms and expressions in the theory of numbers , at a superficial observation may seem so simple and useless in practice. However , if you look at them based on their actual positions of their historical genesis and evolution, which are essentially caused by the general social practices and the requirements of mathematics as a science, having in mind that these are the indirect expression of the needs and requirements of the general social practice, then the situation changes in terms of these concepts and statements and the way we see it, because they arise from the constant collision between the reality and the man, without which they would have been concealed in the man only as a possibility.

This is why in the theory of numbers, both in mathematics and every other science, it is very important to consider the "present" in connection with "the past", because the "present" developed from "the past", and also in the same way "the future" will develop from "the present". The study of "the past" in every science, even in mathematics, and thus also in the theory of numbers, becomes a means to understand "the present" and predict "the future". Therefore, this conceives the development of each of the mathematical models and its complete theory as a part of historical process within the general framework of the development of social practice, whether they are directly or indirectly related to it. This clearly causes the basic problems to appear along with all the tasks and objectives of the research that are normally dealt within the field of research of the history of mathematics.

The subject of the research is to solve the Pell's equation. In order to illustrate the possible size of the numbers that appear in resolving the Pell's equation, it is necessary to describe "the Archimedes' cattle problem." The properties of continued fractions have also been given, due to their application and use in solving the Pell's equation by using the Lagrange equations .

Key words: Diophantus, the Pell's equation, Archimedes problem, Lagrange's method, continued fraction, algoritam.

.