Diofantske jednadžbe

Andrej Dujella

Poslijediplomski kolegij 2006/2007

Sadržaj

Poglavlje 1

Pellovske jednadžbe

1.1 Jednadžbe $\mathbf{x^2 - dy^2 = \pm 1, \pm 4}$

Diofantska jednadžba oblika

$$x^2 - dy^2 = 1, \tag{1.1}$$

gdje je d prirodan broj koji nije potpun kvadrat, naziva se *Pellova jednadžba*. Slučaj kad je d potpun kvadrat isključujemo jer je tada očito da jednadžba (1.1) ima samo trivijalna rješenja $x = \pm 1$, $y = 0$. Zaista, ako je $d = \delta^2$, onda iz $(x - \delta y)(x + \delta y) = 1$ slijedi $x - \delta y = x + \delta y = \pm 1$. Jednadžba je dobila ime po engleskom matematičaru Johnu Pellu, kojem je Euler, po svemu sudeći pogrešno, pripisao zasluge za njezino rješavanje. Neke pojedinačne jednadžbe ovog tipa nalaze se u tekstovima starogrčkih matematičara (Arhimed, Diofant), no prvi su ih sustavno proučavali srednjevjekovni indijski matematičari (Brahmagupta). Od europskih matematičara, metode za rješavanje Pellovih jednadžbi dali su Brouncher, Fermat, Euler i Lagrange, koji je prvi dao i striktan dokaz korektnosti predložene metode.

Kao prvi korak u proučavanju Pellove jednadžbe, dokazat ćemo da ona ima beskonačno mnogo rješenja u prirodnim brojevima. Koristit ćemo Dirichletov teorem iz diofantskih aproksimacija koji kaže da za svaki iracionalan broj α postoji beskonačno mnogo racionalnih brojeva $\frac{p}{q}$ sa svojstvom

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{1.2}$$

Za dokaz vidjeti npr. skriptu iz *Uvoda u teoriju brojeva*, Teorem 6.1 i Korolar 6.2 (na skriptu ćemo se ubuduće pozivati sa [UTB]). Ideja dokaza je za dani prirodan broj Q promotriti $Q + 1$ brojeva

$$0,\ 1,\ \{\alpha\} = \alpha - \lfloor\alpha\rfloor,\ \{2\alpha\},\ \ldots,\ \{(Q-1)\alpha\}$$

iz segmenta $[0, 1]$ i podjelu tog segmenta na Q disjunktnih podintervala širine $1/Q$, te po Dirichletovom principu zaključiti da postoji podinterval koji sadrži barem dva, od promatranih $Q + 1$ brojeva.

Lema 1.1. *Neka je d prirodan broj koji nije potpun kvadrat. Tada postoji cijeli broj k, $|k| < 1 + 2\sqrt{d}$, sa svojstvom da jednadžba*

$$x^2 - dy^2 = k \tag{1.3}$$

ima beskonačno mnogo rješenja u prirodnim brojevima.

Dokaz: Po Dirichletovom teoremu, postoji beskonačno mnogo parova prirodnih brojeva (x, y) sa svojstvom

$$\left|\sqrt{d} - \frac{x}{y}\right| < \frac{1}{y^2}, \quad \text{tj.} \quad \left|x - y\sqrt{d}\right| < \frac{1}{y}.$$

Za svaki takav par (x, y) vrijedi

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

pa je

$$|x^2 - dy^2| = |x - y\sqrt{d}| \cdot |x + y\sqrt{d}| < 1 + 2\sqrt{d}.$$

Budući da parova (x, y) s navedenim svostvo ima beskonačno, a cijelih brojeva koji su po modulu manji od $1+2\sqrt{d}$ samo konačno, to postoji neki cijeli broj k, takav da je $|k| < 1 + 2\sqrt{d}$, za kojeg jednadžba (1.3) ima beskonačno mnogo rješenja. □

Teorem 1.1. *Pellova jednadžba $x^2 - dy^2 = 1$ ima barem jedno rješenje u prirodnim brojevima x i y.*

Dokaz: Beskonačno mnogo rješenja jednadžbe (1.3) možemo podijeliti u k^2 klasa, stavljajući rješenja (x_1, y_1) i (x_2, y_2) u istu klasu akko je $x_1 \equiv x_2 \pmod{k}$ i $y_1 \equiv y_2 \pmod{k}$. Tada neka od tih klasa sadrži barem dva (u stvari beskonačno) različitih rješenja (x_1, y_1), (x_2, y_2) (x_1, x_2 su različiti prirodni brojevi). Stavimo

$$x = \frac{x_1x_2 - dy_1y_2}{k}, \quad y = \frac{x_1y_2 - x_2y_1}{k}$$

("podijelimo rješenja" $x_2 + y_2\sqrt{d}$ i $x_1 + y_1\sqrt{d}$). Tvrdimo da je $x, y \in \mathbb{Z}$, $y \neq 0$ i $x^2 - dy^2 = 1$. Imamo: $x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv k \equiv 0 \pmod{k}$, $x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{k}$, pa su $x, y \in \mathbb{Z}$. Pretpostavimo da je $y = 0$, tj. $x_1y_2 = x_2y_1$. Tada je

$$k = x_2^2 - dy_2^2 = x_2^2 - d \cdot \frac{x_2^2y_1^2}{x_1^2} = \frac{x_2^2}{x_1^2}(x_1^2 - dy_1^2) = \frac{x_2^2}{x_1^2} \cdot k,$$

tj. $x_1^2 = x_2^2$, što je u suprotnosti s pretpostavkom da su x_1 i x_2 različiti prirodni brojevi. Konačno,

$$\begin{aligned} x^2 - dy^2 &= \frac{1}{k^2}\left[(x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2\right] \\ &= \frac{1}{k^2}(x_1^2x_2^2 + d^2y_1^2y_2^2 - dx_1^2y_2^2 - dx_2^2y_1^2) \\ &= \frac{1}{k^2}(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = \frac{1}{k^2}\cdot k\cdot k = 1. \end{aligned}$$

□

Za najmanje rješenja (x, y) u prirodnim brojevima Pellove jednadžbe (1.1) kažemo da je njeno *fundamentalno rješenje*. Označavamo ga sa (x_1, y_1), a često također i sa $x_1 + y_1\sqrt{d}$.

Teorem 1.2. *Pellova jednadžba $x^2 - dy^2 = 1$ ima beskonačno mnogo rješenja. Ako je (x_1, y_1) fundamentalno rješenje, onda su sva rješenja (u prirodnim brojevima) ove jednadžbe dana formulom*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{N}, \tag{1.4}$$

tj.

$$\begin{aligned} x_n &= x_1^n + \binom{n}{2}dx_1^{n-2}y_1^2 + \binom{n}{4}d^2x_1^{n-4}y_1^4 + \cdots, \\ y_n &= nx_1^{n-1}y_1 + \binom{n}{3}dx_1^{n-3}y_1^3 + \binom{n}{5}d^2x_1^{n-5}y_1^5 + \cdots. \end{aligned}$$

Dokaz: Iz (1.4) slijedi $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, pa množenjem dobivamo

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

što znači da su (x_n, y_n) zaista rješenja (i ima ih beskonačno mnogo).

Pretpostavimo sada da je (s, t) rješenje koje nije oblika (x_n, y_n), $n \in \mathbb{N}$. Budući da je $x_1 + y_1\sqrt{d} > 1$ i $s + t\sqrt{d} > 1$, to postoji $m \in \mathbb{N}$ takav da je

$$(x_1 + y_1\sqrt{d})^m < s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1}. \tag{1.5}$$

Pomnožimo li (1.5) sa $(x_1 + y_1\sqrt{d})^{-m} = (x_1 - y_1\sqrt{d})^m$, dobivamo

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

Definirajmo $a, b \in \mathbb{Z}$ s $a + b\sqrt{d} = (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m$. Imamo: $a^2 - db^2 = (s^2 - dt^2)(x_1^2 - dy_1^2)^m = 1$. Iz $a + b\sqrt{d} > 1$ slijedi $0 < a - b\sqrt{d} < 1$, pa je $a > 0$ i $b > 0$. Stoga je (a, b) rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$ i $a + b\sqrt{d} < x_1 + y_1\sqrt{d}$, što je kontradikcija. □

Napomena 1.1. Iz (1.4) se lako dobije (vidi [UTB, Teorem 7.12]) da nizovi (x_n) i (y_n) zadovoljavaju rekurzije

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

gdje je (x_1, y_1) fundamentalno rješenje od (1.1), dok je $(x_0, y_0) = (1, 0)$ "trivijalno rješenje".

O metodama za nalaženje fundamentalnog rješenja govorit ćemo malo kasnije, i vidjet ćemo da to nije sasvim jednostavan problem. No, za neke d-ove specijalnog oblika fundamentalno rješenje je vrlo lako odrediti.

Propozicija 1.1. *Ako je $a + b\sqrt{d}$ rješenje jednadžbe $x^2 - dy^2 = 1$ i vrijedi $a > \frac{1}{2}b^2 - 1$, onda je to fundamentalno rješenje. Specijalno, ako su u, v prirodni brojevi i $d = u(uv^2 + 2)$, onda je $1 + uv^2 + v\sqrt{d}$ fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$.*

Dokaz: Ako je $b = 1$, onda je tvrdnja očito točna. Neka je $b > 1$, te $x_1 + y_1\sqrt{d}$ fundamentalno rješenje od (1.2). Pretpostavimo da je $b > y_1$. Tada iz

$$d = \frac{a^2 - 1}{b^2} = \frac{x_1^2 - 1}{y_1^2}$$

slijedi $x_1^2b^2 - y_1^2a^2 = b^2 - y_1^2 = \delta$, za neki $\delta \in \mathbb{N}$. Dakle, $x_1b + y_1a = \delta_1$, $x_1b - y_1a = \delta_2$, gdje je $\delta_1\delta_2 = \delta$. Sada je

$$a = \frac{\delta_1 - \delta_2}{2y_1} \leq \frac{\delta - 1}{2y_1} = \frac{b^2 - y_1^2 - 1}{2y_1} \leq \frac{b^2}{2} - 1,$$

kontradikcija.

Specijalni slučaj slijedi iz

$$(1 + uv^2)^2 - u(uv^2 + 2)v^2 = 1 \quad \text{i} \quad 1 + uv^2 > \frac{v^2}{2} - 1.$$

□

Do sada smo se bavili samo jednom od četiri jednadžbe navedene u naslovu ovog odjeljka. Da bismo motivirali proučavanje i preostale tri jednadžbe, navest ćemo neke pojmove i činjenice o kvadratnim poljima. Ti će pojmovi biti kasnije poopćeni i sustavnije obrađeni kad budemo govorili o primjeni alata iz algebarske teorije brojeva na rješavanje diofantskih jednadžbi.

Neka je d cijeli broj koji nije potpun kvadrat. Skup svih brojeva oblika $u + v\sqrt{d}$, $u, v \in \mathbb{Q}$, uz uobičajene operacije zbrajanja i množenja kompleksnih brojeva, čini polje, koje označavamo s $\mathbb{Q}(\sqrt{d})$ i zovemo *kvadratno polje*. Očito je $\mathbb{Q}(\sqrt{dm^2}) = \mathbb{Q}(\sqrt{d})$ za $m \in \mathbb{Q}$, $m \neq 0$, pa možemo bez smanjenja općenitosti pretpostaviti da je d kvadratno slobodan. Svaki element

α od $\mathbb{Q}(\sqrt{d})$ je nultočka jedinstvenog normiranog kvadratnog polinoma s racionalnim koeficijentima (kojeg zovemo minimalni polinom od α). Ako su koeficijenti tog polinoma cjelobrojni, onda kažemo da je α *cijeli* (algebarski broj). Cijeli elementi u $\mathbb{Q}(\sqrt{d})$ čine prsten, koji označavamo sa $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Vrijedi (vidi [UTB, Teorem 8.2]):

- ako je $d \equiv 2$ ili $3 \pmod 4$, onda je $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \{u + v\sqrt{d} : u, v \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{d}]$,
- ako je $d \equiv 1 \pmod 4$, onda je $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \{\frac{u+v\sqrt{d}}{2} : u, v \in \mathbb{Z}, u \equiv v \pmod 2\} = \mathbb{Z}[(1+\sqrt{d})/2]$.

Invertibilni elementi prstena $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ zovu se *jedinice* polja $\mathbb{Q}(\sqrt{d})$.

Norma elementa $\alpha = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ definira se kao $N(\alpha) = \alpha \cdot \overline{\alpha} = (u + v\sqrt{d})(u - v\sqrt{d}) = u^2 - dy^2$. Osnovna svojstva norme su (vidi [UTB, Teorem 8.3]):

1) $N(\alpha\beta) = N(\alpha)N(\beta)$,
2) $N(\alpha) = 0 \Leftrightarrow \alpha = 0$,
3) $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \Rightarrow N(\alpha) \in \mathbb{Z}$,
4) $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ je jedinica $\Leftrightarrow N(\gamma) = \pm 1$.

Primijetimo da svojstvo 4) slijedi iz relacije $N(\gamma) \cdot N(\frac{1}{\gamma}) = N(1) = 1$ i svojstva 3).

Vidimo da je problem pronalaženja jedinica u realnim kvadratnim poljima (s $d > 0$) usko povezan s Pellovim jednadžbama. Preciznije:

- ako je $d \equiv 2$ ili $3 \pmod 4$, tada je $u + v\sqrt{d}$ jedinica u $\mathbb{Q}(\sqrt{d})$ ako i samo ako vrijedi $u^2 - dy^2 = \pm 1$,
- ako je $d \equiv 1 \pmod 4$, tada je $\frac{u+v\sqrt{d}}{2}$ jedinica u $\mathbb{Q}(\sqrt{d})$ ako i samo ako vrijedi $u^2 - dy^2 = \pm 4$.

Stoga se uz (običnu) Pellovu jednadžbu $x^2 - dy^2 = 1$ promatraju i jednadžbe $x^2 - dy^2 = -1, 4, -4$ (često se i one nazivaju Pellovim jednadžama).

Uočimo da za razliku od obične Pellove jednadžbe (1.1), jednadžba

$$x^2 - dy^2 = -1 \tag{1.6}$$

ne mora imati rješenja u cijelim brojevima. Npr. očito je da jednadžba $x^2 - 3y^2 = -1$ nema rješenja (jer je lijeva strana kongruentna 0 ili 1 modulo 3). Nužan uvjet za rješivost jednadžbe (1.6) je da d nema prostih djelitelja oblika $4k+3$ (jer -1 mora biti kvadratni ostatak modulo d). No, vidjet ćemo uskoro da taj uvjet nije i dovoljan. Ako jednadžba (1.6) ima rješenja, onda najmanje njezino rješenje u prirodnim brojevima zovemo *fundamentalno rješenje*.

Teorem 1.3. *Pretpostavimo da jednadžba* $x^2-dy^2=-1$ *ima rješenja, te da joj je* $x_1+y_1\sqrt{d}$ *fundamentalno rješenje. Tada je* $(x_1+y_1\sqrt{d})^2$ *fundamentalno rješenje jednadžbe* $x^2-dy^2=1$. *Ako definiramo* $x_n+y_n\sqrt{d}=(x_1+y_1\sqrt{d})^n$, *tada su* $x_{2n}+y_{2n}\sqrt{d}$ *sva rješenja jednadžbe* $x^2-dy^2=1$, *a* $x_{2n+1}+y_{2n+1}\sqrt{d}$ *sva rješenja jednadžbe* $x^2-dy^2=-1$ *u prirodnim brojevima.*

Dokaz: Imamo: $x_n-y_n\sqrt{d}=(x_1-y_1\sqrt{d})^n$, pa je $x_n^2-dy_n^2=(x_1^2-dy_1^2)^n=(-1)^n$. Dakle, zaista je $x_{2n}+y_{2n}\sqrt{d}$ rješenje od $x^2-dy^2=1$, a $x_{2n+1}+y_{2n+1}\sqrt{d}$ rješenje od $x^2-dy^2=-1$. Pretpostavimo da za fundamentalno rješenje $a+b\sqrt{d}$ jednadžbe (1.1) vrijedi

$$1<a+b\sqrt{d}<(x_1+y_1\sqrt{d})^2.$$

Iz $(x_1+y_1\sqrt{d})(-x_1+y_1\sqrt{d})=1$, slijedi $0<-x_1+y_1\sqrt{d}<1$. Stoga je

$$-x_1+y_1\sqrt{d}<(a+b\sqrt{d})(-x_1+y_1\sqrt{d})=s+t\sqrt{d}<x_1+y_1\sqrt{d},$$

gdje je $s=-ax_1+dby_1$, $t=ay_1-bx_1$ i vrijedi $s^2-dt^2=-1$. Zbog $s+t\sqrt{d}>0$ i $s-t\sqrt{d}<0$, jasno je da je $t>0$. Ako je $s<0$, onda iz $-x_1+y_1\sqrt{d}<s+t\sqrt{d}$ dobivamo $x_1+y_1\sqrt{d}>-s+t\sqrt{d}$. Prema tome, zaključujemo da je $|s|+t\sqrt{d}$ rješenje od (1.6), koje je manje od fundamentalnog, što je kontradikcija.

Pretpostavimo sada da je $u+v\sqrt{d}$ neko rješenje od (1.6) koje nije sadržano u nizu $(x_{2n+1}+y_{2n+1}\sqrt{d})$. Tada postoji $m\in\mathbb{N}$ takav da je

$$(x_1+y_1\sqrt{d})^{2n-1}<u+v\sqrt{d}<(x_1+y_1\sqrt{d})^{2n+1}.$$

Množeći ove nejednakosti sa $(x_1-y_1\sqrt{d})^{2n}$, dobivamo

$$-x_1+y_1\sqrt{d}<\sigma+\tau\sqrt{d}<x_1+y_1\sqrt{d},$$

gdje je $\sigma^2-d\tau^2=-1$. No, već smo dokazali da takvi σ i τ ne mogu postojati. □

Propozicija 1.2. *Ako je* p *prost broj i* $p\equiv 1 \pmod 4$, *onda jednadžba* $x^2-py^2=-1$ *ima rješenja.*

Dokaz: Neka je (x_1,y_1) fundamentalno rješenje jednadžbe $x^2-py^2=1$. Tada je $x_1^2-y_1^2\equiv 1 \pmod 4$, pa je x_1 neparan, a y_1 paran. Iz

$$\frac{x_1-1}{2}\cdot\frac{x_1+1}{2}=p\cdot\left(\frac{y_1}{2}\right)^2 \quad \text{i} \quad \left(\frac{x_1-1}{2},\frac{x_1+1}{2}\right)=1$$

slijedi da postoje $u,v\in\mathbb{N}$ takvi da je

$$\frac{x_1\pm 1}{2}=pu^2, \quad \frac{x_1\mp 1}{2}=v^2, \quad \frac{y_1}{2}=uv.$$

Odavde je $v^2-pu^2=\mp 1$. No, iz $u<y_1$ i minimalnosti od (x_1,y_1), slijedi da ovdje ne možemo imati predznak $+$, tj. da vrijedi $v^2-pu^2=-1$.

(Uočimo da je po Teoremu 1.3, $u+v\sqrt{p}$ fundamentalno rješenje od $x^2-py^2=-1$ i vrijedi $(u+v\sqrt{p})^2=u^2+pv^2+2uv\sqrt{p}=x_1+y_1\sqrt{pd}$.) □

Primjer 1.1. *Jednadžba* $x^2 - 34y^2 = -1$ *nema rješenja (iako kongruencija* $x^2 - 34y^2 \equiv -1 \pmod{m}$ *ima rješenja za svaki* $m \in \mathbb{N}$*).*

Rješenje: Fundamentalno rješenje jednadžbe $x^2 - 34y^2 = 1$ je $35 + 6\sqrt{34}$ (iz Propozicije 1.1, ili uvrštavanjem $y = 1, 2, 3, \ldots$). Ako bi jednadžba $x^2 - 34y^2 = -1$ bila rješiva, za njezino fundamentalno rješenje $x_1 + y_1\sqrt{34}$ bi, po Teoremu 1.3, trebalo vrijediti

$$x_1^2 + 34y_1^2 = 35, \quad 2x_1y_1 = 6.$$

Očito je da ovaj sustav nema cjelobrojnih rješenja. ♢

Jednadžba

$$x^2 - dy^2 = 4 \tag{1.7}$$

(d je i dalje prirodan broj koji nije potpun kvadrat) naravno uvijek ima rješenja u prirodnim brojevima, jer ako je (u, v) rješenje jednadžbe $u^2 - dy^2 = 1$, onda je $x = 2u$, $y = 2v$ rješenje jednadžbe $x^2 - dy^2 = 4$. No, vidjet ćemo da za neke d-ove mogu postojati i neka rješenja koja se ne dobivaju na ovaj način. Potpuno analogno Teoremu 1.2, dokazuje se sljedeći teorem:

Teorem 1.4. *Sva rješenja jednadžbe* $x^2 - dy^2 = 4$ *u prirodnim brojevima dana su sa*

$$\frac{x_n + y_n\sqrt{d}}{2} = \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^n, \quad n \in \mathbb{N},$$

gdje je (x_1, y_1) *fundamentalno (tj. najmanje) rješenje te jednadžbe.*

Promotrimo sada slučajeve koji mogu nastupiti u ovisnosti o parnosti ili neparnosti brojeva x_1 i y_1. Jasno je da ne može biti da je y_1 neparan, a x_1 paran, pa stoga imamo tri slučaja:

- Ako su x_1, y_1 oba parni, onda su x_n, y_n također parni za svaki n i $\frac{x_1}{2} + \frac{y_1}{2}\sqrt{d}$ predstavlja fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$.
- Ako je x_1 paran, a y_1 neparan, onda $4|d$, tj. $d = 4d'$. Sada je $\frac{x_1}{2} + y_1\sqrt{d'}$ fundamentalno rješenje jednadžbe $x^2 - d'y^2 = 1$.
- Preostao je najzanimljiviji slučaj kada su x_1, y_1 neparni, u kojem nemamo odmah tako direktnu vezu s (običnom) Pellovom jednadžbom. U tom slučaju mora vrijediti $d \equiv dy_1^2 \equiv x_1^2 - 4 \equiv 5 \pmod 8$. Dakle, nužan uvjet da bi jednadžba $x^2 - dy^2 = 4$ imala rješenja u neparnim brojevima jest da je $d \equiv 5 \pmod 8$. Primjerice, za $d = 5, 13, 21, 29$ jednadžba (1.7) ima rješenja u neparnim brojevima. Npr. za $d = 5$, fundamentalno rješenje je $(x_1, y_1) = (3, 1)$. No, uvjet $d \equiv 5 \pmod 8$ nije i dovoljan, što pokazuje primjer $d = 37$, gdje je $x_1 = 146$, $y_1 = 24$, pa su sva rješenja parna.

Propozicija 1.3. *Ako jednadžba $x^2 - dy^2 = 4$ ima rješenja u neparnim brojevima i ako je $x_1 + y_1\sqrt{d}$ njezino fundamentalno rješenje, onda je*

$$\left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^3 = \frac{1}{8}(x_1^3 + 3dx_1y_1^2) + \frac{1}{8}(3x_1^2y_1 + dy_1^3)\sqrt{d}$$

fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$.

Dokaz: Budući da su x_1, y_1 neparni i $d \equiv 5 \pmod 8$, vrijedi

$$x_1^2 + 3dy_1^2 \equiv 1 + 15 \equiv 0 \pmod 8, \quad 3x_1^2 + dy_1^2 \equiv 3 + 5 \equiv 0 \pmod 8,$$

pa su brojevi $u_1 = \frac{1}{8}(x_1^3 + 3dx_1y_1^2)$ i $v_1 = \frac{1}{8}(3x_1^2y_1 + dy_1^3)$ cijeli. Nadalje, $u_1^2 - dv_1^2 = \left(\frac{x_1^2 - dy_1^2}{4}\right)^3 = 1$.

Pretpostavimo da $u_1 + dv_1$ nije fundamentalno rješenje jednadžbe (1.1), te neka je $s_1 + t_1\sqrt{d}$ to fundamentalno rješenje. To znači da je

$$1 < s_1 + t_1\sqrt{d} < \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^3.$$

Uočimo da ne može biti $s_1 + t_1\sqrt{d} < (x_1 + y_1\sqrt{d})/2$, jer bi tada $2s_1 + 2t_1\sqrt{d}$ bilo rješenje od (1.7) koje je manje od $x_1 + y_1\sqrt{d}$. Također, ne može biti $s_1 + t_1\sqrt{d} = \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^2$, jer broj $(x_1^2 + dy_1^2)/4$ nije cijeli. Zato je

$$\left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^i < s_1 + t_1\sqrt{d} < \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^{i+1} \tag{1.8}$$

za $i = 1$ ili $i = 2$. Množeći nejednakosti u (1.8) sa $\left(\frac{x_1 - y_1\sqrt{d}}{2}\right)^i$, dobivamo

$$1 < \frac{a + b\sqrt{d}}{2} < \frac{x_1 + y_1\sqrt{d}}{2},$$

gdje je $a^2 - db^2 = 4$, što je u kontradikciji s minimalnošću od (x_1, y_1). □

Primjer 1.2. Fundamentalno rješenje jednadžbe

$$x^2 - 5y^2 = 4 \tag{1.9}$$

je $3 + \sqrt{5}$, pa je fundamentalno rješenje jednadžbe

$$x^2 - 5y^2 = 1 \tag{1.10}$$

jednako $\left(\frac{3+\sqrt{5}}{2}\right)^3 = 9 + 4\sqrt{5}$. Koristeći rekurzivne relacije analogne ovima iz Napomene 1.1, može se dokazati da su sva rješenja jednadžbe (1.9) dana

sa $x = L_{2n}$, $y = F_{2n}$, a sva rješenje jednadžbe (1.10) sa $x = \frac{1}{2}L_{6n}$, $y = \frac{1}{2}F_{6n}$, gdje su F_n i L_n Fibonaccijevi i Lucasovi brojevi, definirani sa

$$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n,$$
$$L_0 = 2,\ L_1 = 1,\ L_{n+2} = L_{n+1} + L_n.$$

Konačno, promotrimo još i jednadžbu

$$x^2 - dy^2 = -4. \tag{1.11}$$

Ona ne mora imati rješenja. Ako jednadžba $x^2 - dy^2 = -1$ ima rješenja, onda i jednadžba (1.11) ima rješenja (u parnim brojevima). No, jednadžba (1.11) može imati rješenja i u neparnim brojevima. To je npr. slučaj za $d = 5$ (rješenje je $x = y = 1$), $d = 13, 29, 53$. Ponovo je nužan uvjet za postojanje neparnih rješenja $d \equiv 5 \pmod 8$. Analogno Teoremu 1.3 se dokazuje sljedeći rezultat:

Teorem 1.5. *Pretpostavimo da jednadžba $x^2 - dy^2 = -4$ ima rješenja, te da je $x_1 + y_1\sqrt{d}$ njezino fundamentalno rješenje. Tada su sva rješenja te jednadžbe dana sa*

$$\frac{x_n + y_n\sqrt{d}}{2} = \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^n, \quad n \text{ neparan.}$$

Nadalje, $\left(\frac{x_1+y_1\sqrt{d}}{2}\right)^2$ je fundamentalno rješenje jednadžbe $x^2 - dy^2 = 4$.

Rezultate iz ovog odjeljka o jednadžbama $x^2 - dy^2 = \pm 1, \pm 4$ ćemo sumirati i interpretirati u terminima jedinica u realnim kvadratnim poljima, što nam je i bila jedna od motivacija za njihovo proučavanje. Sljedeći korolar je direktna posljedica Teorema 1.2, 1.3, 1.4 i 1.5 u kojima je dana struktura skupa svih rješenja Pellovih jednadžbi.

Korolar 1.1. *Grupa jedinica u realnom kvadratnom polju $\mathbb{Q}(\sqrt{d})$ ima dva generatora: -1 i ϵ_d, gdje je $\epsilon_d = a + b\sqrt{d}$ ili $\frac{a+b\sqrt{d}}{2}$, dok je $a + b\sqrt{d}$ fundamentalno rješenje jedne od Pellovih jednadžbi $x^2 - dy^2 = \pm 1, \pm 4$. Dakle, svaka se jedinica može napisati u obliku $\pm\epsilon_d^n$, $n \in \mathbb{Z}$. Generator ϵ_d se zove* fundamentalna jedinica *kvadratnog polja $\mathbb{Q}(\sqrt{d})$. Ako je $x_1 + y_1\sqrt{d}$ fundamentalno rješenje Pellove jednadžbe $x^2 - dy^2 = 1$, onda je $x_1 + y_1\sqrt{d} = (a + b\sqrt{d})^\nu$, gdje je $\nu \in \{1, 2, 3, 6\}$.*

Preciznije informacije o eksponentu ν su dane u sljedećoj tablici, pomoću koje ν možemo odrediti iz kongruencijskih svojstava brojeva a, b, d.

d	$a^2 - db^2$	b	a	ν	primjer
$\equiv 3 \pmod 4$	1			1	$d = 3$
$\equiv 1, 2 \pmod 4$	1	$\equiv 0 \pmod 2$		1	$d = 6$
$\equiv 1, 2 \pmod 4$	-1	$\equiv 1 \pmod 2$		2	$d = 2$
$\equiv 5 \pmod{16}$	4	$\equiv 1 \pmod 2$	$\equiv \pm 3b \pmod 8$	3	$d = 21$
$\equiv 5 \pmod{16}$	-4	$\equiv 1 \pmod 2$	$\equiv \pm b \pmod 8$	6	$d = 5$
$\equiv 13 \pmod{16}$	4	$\equiv 1 \pmod 2$	$\equiv \pm b \pmod 8$	3	$d = 45$
$\equiv 13 \pmod{16}$	-4	$\equiv 1 \pmod 2$	$\equiv \pm 3b \pmod 8$	6	$d = 13$

Tablica 1.1: Veza fundamentalnih rješenja i fundamentalnih jedinica

1.2 Verižni razlomci i Pellova jednadžbe

Teorem 1.2 i Napomena 1.1 nam pokazuju kako možemo generirati sva rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ ukoliko znamo njeno fundamentalno (najmanje) rješenje. No, ostaje pitanje kako naći to fundamentalno rješenje. Ponekad rješenje možemo naći uvrštavajući redom $y = 1, 2, 3, \ldots$ i provjeravajući je li $dy^2 + 1$ kvadrat. Međutim, već i za relativno male d-ove fundamentalno rješenje može biti vrlo veliko, npr. za $d = 94$, fundamentalno rješenje je $2143295 + 221064\sqrt{94}$. Stoga je potrebno naći efikasniji način za njegovo nalaženje.

Jedan relativno efikasan algoritam za nalaženje fundamentalog rješenja dobit ćemo iz veze Pellovih jednadžbi s diofantskim aproksimacijama, te preko njih s verižnim razlomcima. Naime, svako netrivijano rješenje jednadžbe $x^2 - dy^2 = 1$ inducira jako dobru racionalnu aproksimaciju iracionalnog broja $\sqrt{d}$. Zaista,

$$\left|\sqrt{d} - \frac{x}{y}\right| = \frac{1}{y|x + y\sqrt{d}|} < \frac{1}{2\sqrt{d}y^2}. \tag{1.12}$$

Poznato je da se sve jako dobre racionalne aproksimacije realnog broja mogu dobiti iz njegovog razvoja u verižni razlomak.

Neka je $\alpha \in \mathbb{R}$. Izraz oblika

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

gdje je $a_0 \in \mathbb{Z}$, te $a_1, a_2, \ldots \in \mathbb{N}$, zove se razvoj broja α u *jednostavni verižni (ili neprekidni) razlomak*. Verižni razlomak kraće zapisujemo kao $[a_0; a_1, a_2, \ldots]$. Brojevi $a_0, a_1, a_2, \ldots$ se zovu *parcijalni kvocijenti*, a definiraju se na sljedeći način:

$$a_0 = \lfloor \alpha \rfloor, \quad \alpha = a_0 + \frac{1}{\alpha_1}, \quad a_1 = \lfloor \alpha_1 \rfloor, \quad \alpha_1 = a_1 + \frac{1}{\alpha_2}, \quad a_2 = \lfloor \alpha_2 \rfloor, \ldots.$$

Postupak se nastavlja sve dok je $a_k \neq \alpha_k$. Razvoj u jednostavni verižni razlomak broja α je konačan ako i samo ako je α racionalan broj. Ako je $\alpha = \frac{m}{n}$, brojevi $a_0, a_1, a_2, \ldots$ su upravo kvocijenti iz Euklidovog algoritma primjenjenog na brojeve m i n.

Racionalne brojeve

$$\frac{p_k}{q_k} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_k}}} = [a_0; a_1, \ldots, a_k]$$

zovemo *konvergente verižnog razlomka*. Brojnici i nazivnici konvergenti zadovoljavaju sljedeće rekurzije:

$$p_{n+2} = a_{n+2}p_{n+1} + p_n, \quad p_0 = a_0, \quad p_1 = a_0a_1 + 1, \quad (p_{-1} = 1,\ p_{-2} = 0),$$
$$q_{n+2} = a_{n+2}q_{n+1} + q_n, \quad q_0 = 1, \quad q_1 = a_1, \quad (q_{-1} = 0,\ q_{-2} = 1).$$

Indukcijom se lako dokazuje sljedeća važna relacija koja povezuje konvergente sa susjednim indeksima:

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n. \tag{1.13}$$

Relacija (1.13) povlači da je $\frac{p_{2k}}{q_{2k}} \leq \alpha$ i $\alpha \leq \frac{p_{2k+1}}{q_{2k+1}}$ za svaki k. Nadalje, može se dokazati da ako je α pozitivan, onda vrijede sljedeće nejednakosti:

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots \leq \alpha \leq \cdots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

Ako je α iracionalan, onda je $\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$ (za detalje vidjeti [UTB, Poglavlje 6]).

Postavlja se pitanje koliko dobro konvergente aproksimiraju α. Odgovor je dan u sljedećim nejednakostima:

$$\frac{1}{q_n(q_n + q_{n+1})} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}\,. \tag{1.14}$$

Vrijedi i svojevrsni obrat ove činjenice (Legendreov teorem): ako je $\frac{p}{q}$ racionalan broj koji zadovoljava nejednakost $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$, onda je $\frac{p}{q}$ konvergenta od α. Mi ćemo dokazati nešto općenitiju tvrdnju (Worley [1981], Dujella [2004]).

Teorem 1.6. *Neka je α proizvoljan realan broj, te c pozitivan realan broj. Ako racionalan broj $\frac{p}{q}$ zadovoljava nejednakost*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}, \tag{1.15}$$

tada je

$$\frac{p}{q} = \frac{rp_n \pm sp_{n-1}}{rq_n \pm sq_{n-1}},$$

za neke nenegativne cijele brojevi n, r, s takve da je $rs < 2c$ (i izbor predznaka).

Dokaz: Pretpostavit ćemo da je $\alpha < \frac{p}{q}$. U slučaju $\alpha > \frac{p}{q}$, dokaz je analogan. Također ćemo pretpostaviti da je α iracionalan (za α racionalan potrebna je mala modifikacija dokaza). Neka je n najveći neparan broj takav da je

$$\alpha < \frac{p}{q} \leq \frac{p_n}{q_n}.$$

(Ako je $\frac{p}{q} > \frac{p_1}{q_1}$, onda uzimamo $n = -1$.) Definirajmo brojeve r i s sa:

$$p = rp_{n+1} + sp_n,$$
$$q = rq_{n+1} + sq_n.$$

Prema relaciji (1.13), determinanta ovog sustava je ± 1, pa su r, s cijeli brojevi, a kako je $\frac{p_{n+1}}{q_{n+1}} < \frac{p}{q} \leq \frac{p_n}{q_n}$, vrijedi $r \geq 0$ i $s > 0$.

Zbog minimalnosti od n, imamo

$$\left|\frac{p_{n+2}}{q_{n+2}} - \frac{p}{q}\right| < \left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}.$$

Nadalje,

$$\left|\frac{p_{n+2}}{q_{n+2}} - \frac{p}{q}\right| = \frac{(a_{n+2}q_{n+1} + q_n)(rp_{n+1} + sp_n) - (a_{n+2}p_{n+1} + p_n)(rq_{n+1} + sq_n)}{qq_{n+2}}$$
$$= \frac{sa_{n+2} - r}{qq_{n+2}}.$$

Stoga je

$$q(sa_{n+2} - r) < cq_{n+2} = \frac{c}{s}((sa_{n+2} - r)q_{n+1} + q),$$

tj.

$$(sa_{n+2} - r)(q - \frac{c}{s}q_{n+1}) < \frac{c}{s}\,q.$$

Dalje imamo

$$\frac{1}{sa_{n+2} - r} > \frac{q - \frac{c}{s}q_{n+1}}{\frac{c}{s}q} = \frac{s}{c} - \frac{1}{r + \frac{sq_n}{q_{n+1}}} \geq \frac{s}{c} - \frac{1}{r}.$$

Tako smo dobili nejednakost (kvadratnu nejednadžbu po r):

$$r^2 - sra_{n+2} + ca_{n+2} > 0. \tag{1.16}$$

Razlikujemo sada dva slučaja:

1) $s^2a_{n+2} \geq 4c$

   Uz ovu pretpostavku je $s^4a_{n+2}^2 - 4cs^2a_{n+2} \geq (s^2a_{n+2} - 4c)^2$, pa za rješenje nejednadžbe (1.16) vrijedi da je

$$r < \frac{1}{2s}\left(s^2a_{n+2} - \sqrt{s^4a_{n+2}^2 - 4cs^2a_{n+2}}\right) \leq \frac{2c}{s},$$

   ili

$$r > \frac{1}{2s}\left(s^2a_{n+2} + \sqrt{s^4a_{n+2}^2 - 4cs^2a_{n+2}}\right) \geq \frac{1}{s}(s^2a_{n+2} - 2c).$$

Prva mogućnost povlači $rs < 2c$. Ako je nastupila druga mogućnost, uvodimo supstituciju $t = sa_{n+2} - r$. Broj t je prirodan i vrijedi

$$p = rp_{n+1} + sp_n = (sa_{n+2} - t)p_{n+1} + sp_n = sp_{n+2} - tp_{n+1},$$
$$q = sq_{n+2} - tq_{n+1}$$

i $st = s^2a_{n+2} - rs < 2c$.

1) $s^2a_{n+2} < 4c$

Ako je $r < \frac{1}{2}sa_{n+2}$, onda $rs < \frac{1}{2}s^2a_{n+2} < 2c$. Ako je $\frac{1}{2}sa_{n+2} \leq r < sa_{n+2}$, onda ponovo definiramo $t = sa_{n+2} - r$ i vrijedi $st \leq \frac{1}{2}s^2a_{n+2} < 2c$.

□

Iz nejednakosti (1.12) i Teorema 1.6 (ustvari, već iz Legendreovog teorema koji je specijalni slučaj Teorema 1.6 za $c = 1/2$) zaključujemo da za svako rješenje Pellove jednadžbe $x^2 - dy^2 = 1$ vrijedi da je $\frac{x}{y}$ neka konvergenta u razvoju od $\sqrt{d}$. Broj $\sqrt{d}$ je kvadratna iracionalnost, pa mu je razvoj periodičan ([UTB, Teorem 6.14]). Štoviše, broj $\sqrt{d}+\lfloor\sqrt{d}\rfloor$ je reduciran (veći je od 1, a konjugat $-\sqrt{d} + \lfloor\sqrt{d}\rfloor$ mu je iz $\langle -1, 0\rangle$), pa mu je razvoj čisto periodičan ([UTB, Teorem 6.15]). Odavde slijedi da $\sqrt{d}$ ima razvoj oblika:

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{\ell-1}, 2a_0}],$$

gdje je $a_0 = \lfloor\sqrt{d}\rfloor$. Nadalje, može se pokazati da vrijedi "palindromno svojstvo": $a_1 = a_{\ell-1}$, $a_2 = a_{\ell-2}$, ... ([UTB, Teorem 7.7]).

Sada ćemo navesti algoritam za razvoj kvadratnih iracionalnosti u verižni razlomak (za dokaz korektnosti algoritma, vidjeti [UTB, dokaz Teorema 6.14]). Neka je α kvadratna iracionalnost. Prikažemo je u obliku $\alpha = \frac{s_0+\sqrt{d}}{t_0}$, gdje su $d, s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$, $d \neq \square$ i $t_0|(d - s_0^2)$. Ako je $\alpha = \sqrt{d}$, onda je jednostavno $s_0 = 0$, $t_0 = 1$. Sada brojeve a_i (tzv. parcijalne kvocijente) računamo rekurzivno na slijedeći način:

$$a_i = \lfloor\frac{s_i + a_0}{t_i}\rfloor, \quad s_{i+1} = a_it_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}. \tag{1.17}$$

Uočimo da, iako je α iracionalan broj, ovaj algoritam radi samo s cijelim brojevima. Pokazuje se da su nizovi (s_i) i (t_i) ograničeni. Preciznije, dobije se da za dovoljno velike indekse i vrijedi

$$0 < s_i < \sqrt{d}, \quad 0 < t_i < s_i + \sqrt{d} < 2\sqrt{d}.$$

Na taj način se upravo i zaključuje da razvoj mora biti periodičan (jer moraju postojati različiti indeksi j, k takvi da je $(s_j, t_j) = (s_k, t_k)$). Odavde

direktno dobivamo ocjenu za duljinu perioda u razvoju od $\sqrt{d}$: $\ell(d) < \sqrt{d} \cdot 2\sqrt{d} = 2d$. Preciznijom analizom odnosa između s_i i t_i (posebno kongruencije $s_i^2 \equiv d \pmod{t_i}$), dobije se ocjena $\ell(d) = \mathcal{O}(\sqrt{d}\ln d)$. Najbolji poznati rezultat toga tipa je $\ell(d) < \frac{7}{2\pi^2}\sqrt{d}\ln d$ za dovoljno velike d ([Cohn 1977]), a slutnja je (povezana s čuvenom Riemannovom slutnjom) da vrijedi $\ell(d) = \mathcal{O}(\sqrt{d}\ln\ln d)$.

Izjednačavanjem racionalnih i iracionalnih dijelova u jednakosti

$$\sqrt{d} = \frac{\frac{s_{n+1}+\sqrt{d}}{t_{n+1}}p_n + p_{n-1}}{\frac{s_{n+1}+\sqrt{d}}{t_{n+1}}q_n + q_{n-1}},$$

dobiva se relacija

$$p_n^2 - dq_n^2 = (-1)^{n+1}t_{n+1}, \quad \text{za sve } n \geq -1. \tag{1.18}$$

Ona nam pokazuje da rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ odgovaraju onim n-ovima za koje je $(-1)^{n+1}t_{n+1} = 1$. Nije teško za vidjeti da je $t_i = 1$ ako i samo ako $\ell | i$ (ℓ je duljina perioda). Zato vrijedi

Teorem 1.7. *Neka je ℓ duljina perioda u razvoju od $\sqrt{d}$.*

Ako je ℓ paran, onda jednadžba $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja od $x^2 - dy^2 = 1$ su dana sa $(x, y) = (p_{n\ell-1}, q_{n\ell-1})$, $n \in \mathbb{N}$. Posebno, fundamentalno rješenje je $(p_{\ell-1}, q_{\ell-1})$.

Ako je ℓ neparan, onda su sva rješenja jednadžbe $x^2 - dy^2 = -1$ dana sa $(x, y) = (p_{(2n-1)\ell-1}, q_{(2n-1)\ell-1})$, a sva rješenja jednadžbe $x^2 - dy^2 = 1$ sa $(x, y) = (p_{2n\ell-1}, q_{2n\ell-1})$, $n \in \mathbb{N}$. Posebno, fundamentalno rješenje od $x^2 - dy^2 = 1$ je $(p_{2\ell-1}, q_{2\ell-1})$.

Primjer 1.3. *Nađimo fundamentalno rješenje jednadžbe $x^2 - 113y^2 = 1$.*

Rješenje: Razvijmo $\sqrt{113}$ u verižni razlomak koristeći algoritam (1.17):

$$\begin{aligned}
&a_0 = 10,\ s_1 = a_0t_0 - s_0 = 10,\ t_1 = \frac{d - s_1^2}{t_0} = 13;\\
&a_1 = \left\lfloor \frac{s_1 + 10}{t_1} \right\rfloor = 1,\ s_2 = 3,\ t_2 = 8; \quad a_2 = 1,\ s_3 = 5,\ t_3 = 11;\\
&a_3 = 1,\ s_4 = 6,\ t_4 = 7; \quad a_4 = 2,\ s_5 = 8,\ t_5 = 7.
\end{aligned}$$

Možemo nastaviti dalje s algoritmom sve dok ne dobijemo $(s_k, t_k) = (s_1, t_1)$. No, možemo i uočiti da vrijedi $t_4 = t_5$. Ovo "djelomično" ponavljanje nam indicira da smo došli do polovice punog perioda. Naime, vrijedi slijedeće:

- ako je $s_n = s_{n+1}$, onda je $\ell = 2n$;
- ako je $t_n = t_{n+1}$, onda je $\ell = 2n + 1$.

U našem slučaju je $\ell = 9$, pa nam svojstvo palidromnosti i činjenica da je zadnji član u periodu jednak $2a_0$, omogućava da rekonstruiramo razvoj:

$$\sqrt{113} = [10; \overline{1, 1, 1, 2, 2, 1, 1, 1, 20}].$$

Da bi izračunali fundamenalno rješenje jednadžbe $x^2 - 113y^2 = 1$, dovoljno je naći fundamentalno rješenje jednadžbe $x^2 - 113y^2 = -1$ (a to je (p_8, q_8)) i kvadrirati ga (Teorem 1.3).

i	-1	0	1	2	3	4	5	6	7	8
a_i		10	1	1	1	2	2	1	1	1
p_i	1	10	11	21	32	85	202	287	489	776
q_i	0	1	1	2	3	8	19	27	46	73

Traženo fundamentalno rješenje jednadžbe $x^2 - 113y^2 = 1$ je

$$(776 + 73\sqrt{113})^2 = 1204353 + 113296\sqrt{113}.$$

♢

1.3 Jednadžba $x^2 - dy^2 = N$

Jednadžba oblika

$$x^2 - dy^2 = N, \tag{1.19}$$

gdje je d prirodan broj koji nije potpun kvadrat i N cijeli broj različit od 0, naziva se *pellovska jednadžba*. Jasno je da ovakva jednadžba ne mora imati cjelobrojnih rješenja. No, ukoliko ima barem jedno rješenje, onda ih ima beskonačno mnogo. Zaista, ako je $x + y\sqrt{d}$ rješenje jednadžbe 1.19, a $u + v\sqrt{d}$ rješenje pripadne Pellove jednadžbe $x^2 - dy^2 = 1$, onda je

$$(x + y\sqrt{d})(u + v\sqrt{d}) = (ux + dvy) + (uy + vx)\sqrt{d} \tag{1.20}$$

također rješenje jednadžbe (1.19), jer je

$$(ux + dvy)^2 - d(uy + vx)^2 = (x^2 - dy^2)(u^2 - dv^2) = N \cdot 1 = N.$$

Budući da Pellova jednadžba ima beskonačno mnogo rješenja, to iz (1.20) slijedi da i jednadžba (1.19) ima beskonačno rješenja (uz pretpostavku da ima barem jedno).

Za dva rješenja $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ jednadžbe (1.19) kažemo da su *asocirana* ako se jedno iz drugog može dobiti množenjem s nekim rješenjem Pellove jednadžbe kao u formuli (1.20). Lako se provjerava da je na ovaj način uvedena relacija ekvivalencije na skupu svih rješenja jednadžbe (1.19) (podsjetimo se da je $(u+v\sqrt{d})^{-1} = u - v\sqrt{d}$, što povlači simetričnost). Reći ćemo da međusobno asocirana rješenja tvore jednu *klasu rješenja*. Nije teško za vidjeti da su $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ asocirani ako i samo ako vrijedi

$$xx' \equiv dyy' \pmod{N}, \quad xy' \equiv x'y \pmod{N}$$

(pogledati dokaz Teorema 1.1).

Neka je $\mathbf{K}$ jedna klasa rješenja, te neka su njeni elementi $x_i + y_i\sqrt{d}$, $i = 1, 2, 3, \ldots$. Tada klasu koja se sastoji od rješenja $x_i - y_i\sqrt{d}$ označavamo s $\bar{\mathbf{K}}$ i kažemo da je *konjugirana* klasi $\mathbf{K}$. Ako vrijedi da je $\mathbf{K} = \bar{\mathbf{K}}$, onda kažemo da je klasa $\mathbf{K}$ *dvoznačna*.

Među svim elementima klase $\mathbf{K}$ odabrat ćemo jedan, $x^* + y^*\sqrt{d}$, kojeg ćemo zvati *fundamentalno rješenje jednadžbe* $x^2 - dy^2 = N$ *u klasi* $\mathbf{K}$. Biramo ga tako da y^* poprimi najmanju moguću nenegativnu vrijednost među svim elementima $x+y\sqrt{d}$ u klasi $\mathbf{K}$. Ovim je zahtjevom i x^* jednoznačno određen, osim u slučaju kada je $\mathbf{K}$ dvoznačna. Ako je $\mathbf{K}$ dvoznačna, onda izabiremo x^* tako da zadovolji i dodatni uvjet da je $x^* \geq 0$. Uočimo da $|x^*|$ poprima najmanju moguću vrijednost unutar klase $\mathbf{K}$.

Teorem 1.8. *Neka je* $u+v\sqrt{d}$ *fundamentalno rješenje jednadžbe* $x^2 - dy^2 = 1$. *Tada za svako fundamentalno rješenje* $x^* + y^*\sqrt{d}$ *jednadžbe* $x^2 - dy^2 = N$

vrijede nejednakosti:

$$0 \le y^* \le \frac{v}{\sqrt{2(u+\varepsilon)}}\sqrt{|N|},$$
$$|x^*| \le \sqrt{\frac{1}{2}(u+\varepsilon)|N|},$$

gdje je $\varepsilon = 1$ *ako je* $N > 0$, *a* $\varepsilon = -1$ *ako je* $N < 0$. *Posebno, fundamentalnih rješenja (pa i klasa rješenja) ima konačno mnogo.*

Dokaz: Dokazat ćemo tvrdnju za $N < 0$. Dokaz za $N > 0$ je analogan. Definirajmo cijele brojeve x', y' sa $x' + y'\sqrt{d} = (x^* + y^*\sqrt{d})(u - \delta v\sqrt{d})$, gdje je $\delta = 1$ ako je $x^* \ge 0$, a $\delta = -1$ ako je $x^* < 0$. Tada $x' + y'\sqrt{d}$ pripada istoj klasi kao i $x^* + y^*\sqrt{d}$, pa zbog minimalnosti od y^* zaključujemo da je

$$y' = uy^* - \delta v x^* \ge y^*,$$

što povlači $v|x^*| \le (u-1)y^*$. Kvadriranjem dobivamo

$$v^2(dy^{*2} + N) \le (u^2 - 2u + 1)y^{*2},$$

tj. $y^{*2}(2u-2) \le |N| \cdot v^2$, pa dobivamo traženu nejednakost za y^*. Sada je

$$x^{*2} = dy^{*2} + N \le \frac{-dNv^2}{2u-2} + N = \frac{-N(u^2-2u+1)}{2u-2} = \frac{|N| \cdot (u-1)}{2}.$$

□

Primjer 1.4. *Riješimo jednadžbu* $x^2 - 6y^2 = -29$.

Rješenje: Fundamentalno rješenje pripadne Pellove jednadžbe $x^2 - 6y^2 = 1$ je $5 + 2\sqrt{6}$. Stoga za fundamentalna rješenja polazne jednadžbe vrijede nejednakosti $0 \le y^* \le 3$, $|x^*| \le 7$. Lako se provjeri da su jedina rješenja koja zadovoljavaju te nejednakosti $5+3\sqrt{6}$ i $-5+3\sqrt{6}$ (i ona nisu asocirana). Dakle, sva rješenja su dana sa

$$x + y\sqrt{6} = \pm(5+3\sqrt{6})(5+2\sqrt{6})^n \quad \text{ili} \quad x + y\sqrt{6} = \pm(-5+3\sqrt{6})(5+2\sqrt{6})^n,$$

za $n \in \mathbb{Z}$. To znači da imamo dva niza rješenja (u prirodnim brojevima):

$$x_0 = 5,\ y_0 = 3;\ x_1 = 61,\ y_1 = 25;\ x_{n+2} = 10x_{n+1} - x_n,\ y_{n+2} = 10y_{n+1} - y_n,$$
$$x'_0 = -5,\ y'_0 = 3;\ x'_1 = 11,\ y'_1 = 5;\ x'_{n+2} = 10x'_{n+1} - x'_n,\ y'_{n+2} = 10y'_{n+1} - y'_n.$$

♢

Propozicija 1.4. *Pretpostavimo da je* $|N| < \sqrt{d}$. *Ako je* $x + y\sqrt{d}$ *rješenje jednadžbe* $x^2 - dy^2 = N$, *onda je* $\frac{x}{y}$ *neka konvergenta u razvoju u verižni razlomak od* $\sqrt{d}$.

Dokaz: Pretpostavimo najprije da je $N > 0$. Tada je $x > y\sqrt{d}$, pa je

$$0 < \frac{x}{y} - \sqrt{d} = \frac{N}{y(x + y\sqrt{d})} < \frac{N}{2\sqrt{d}y^2} < \frac{1}{2y^2}.$$

Iz Legendreovog teorema slijedi da je $\frac{x}{y}$ neka (neparna) konvergenta od $\sqrt{d}$.

Neka je sada $N < 0$. Tada je $x < y\sqrt{d}$, pa imamo

$$0 < \frac{y}{x} - \frac{1}{\sqrt{d}} = \frac{|N|}{x\sqrt{d}(x + y\sqrt{d})} < \frac{|N|}{2\sqrt{d}x^2} < \frac{1}{2x^2}.$$

Zaključujemo da je $\frac{y}{x}$ neka konvergenta od $\frac{1}{\sqrt{d}}$. No, ako je $\frac{y}{x}$ i-ta konvergenta od $\frac{1}{\sqrt{d}}$, onda je $\frac{x}{y}$ $(i-1)$-va konvergenta od $\sqrt{d}$. □

Dakle, rješivost jednadžbe $x^2 - dy^2 = N$ u relativno prostim cijelim brojevima x, y, ako je $|N| < \sqrt{d}$, možemo ustanoviti tako da $\sqrt{d}$ razvijemo u verižni razlomak, te provjerimo zadovoljava li neka od prvih 2ℓ konvergenti relaciju

$$p_i^2 - dq_i^2 = (-1)^{i+1}t_{i+1} = N.$$

Ako $|N|$ nije puno veći od $\sqrt{d}$ (npr. $|N| < 4\sqrt{d}$), onda možemo koristiti Teorem 1.6 umjesto Legendreovog teorema. Pritom koristimo relaciju

$$(rp_i \pm sp_{i-1})^2 - d(rq_i \pm sq_{i-1})^2 = (-1)^{i+1}(r^2t_{i+1} - s^2t_i \mp 2rss_{i+1}). \quad (1.21)$$

Za rješenje $x_0 + y_0\sqrt{d}$ kažemo da je *primitivno* ako su x_0 i y_0 relativno prosti. Ako je $(x_0, y_0) = g$, onda je $\frac{x_0}{g} + \frac{y_0}{g}\sqrt{d}$ primitivno rješenje jednadžbe $x^2 - dy^2 = \frac{N}{g^2}$.

Primjer 1.5. *Neka je k prirodan broj. Odrediti sve prirodne brojeve N takve da je $N < 4k$ i da jednadžba*

$$x^2 - (k^2 + 1)y^2 = N$$

ima primitivno rješenje.

Rješenje: Imamo da je

$$0 < \frac{x}{y} - \sqrt{k^2 + 1} < \frac{N}{2\sqrt{k^2 + 1}y^2} < \frac{2k}{\sqrt{k^2 + 1}y^2} < \frac{2}{y^2}.$$

Po Teoremu 1.6, brojevi x i y imaju oblik $x = rp_i \pm sp_{i-1}$, $y = rq_i \pm sq_{i-1}$, gdje je $rs < 4$. Broj $\sqrt{k^2 + 1}$ ima vrlo jednostavan razvoj u verižni razlomak:

$$\sqrt{k^2 + 1} = [k; \overline{2k}].$$

Nadalje, $s_i = k$, $t_i = 1$ za svaki $i \geq 1$. Zato je u formulu (1.21) dovoljno uvrstiti $i = 1$, te $(r, s) = (1, 0), (1, 1), (1, 2), (2, 1), (1, 3), (3, 1)$. Dobivaju se sljedeće vrijednosti od N koje zadovoljavaju uvjet $0 < N < 4k$:

$$N = 1,\ 2k,\ 4k - 3 \quad (\text{za svaki } k \in \mathbb{N}),$$

te još dodatno $N = 10$ za $k = 3$ (što je jednako $6k - 8$). $\diamondsuit$

Opisat ćemo opći algoritam kojim se rješavanje jednadžbe $x^2 - dy^2 = N$ za $|N| < \sqrt{d}$ može svesti na rješavanje jednadžbe $x^2 - dy^2 = N'$, gdje je $|N'| > \sqrt{d}$. Konstrukcija koja se pritom koristi dat će nam i novi dokaz konačnosti broja klasa rješenja, te ocjenu za broj klasa koja neće ovisi o veličini fundamentalnog rješenja pripadne Pellove jednadžbe.

Lema 1.2. *Ako je $x_0 + y_0\sqrt{d}$ primitivno rješenje jednadžbe $x^2 - dy^2 = N$, onda postoji cijeli broj k, $|k| \leq \frac{|N|}{2}$, sa svojstvom*

$$\begin{aligned} x_0 &\equiv ky_0 \pmod{N}, \\ k^2 &\equiv d \pmod{N}. \end{aligned}$$

U tom slučaju kažemo da rješenje $x_0 + y_0\sqrt{d}$ pripada broju k.

Dokaz: Budući da su x_0 i y_0 relativno prosti, to su i y_0 i N također relativno prosti. Stoga postoji $k \in \mathbb{Z}$ takav da je $ky_0 \equiv x_0 \pmod{N}$. Broj k možemo izabrati iz bilo kojeg potpunog sustava ostataka modulo N, a tako i iz onog s najmanjim ostacima po apsolutnoj vrijednosti, koji sadrži ostatke koji su $\leq \frac{|N|}{2}$. Nadalje,

$$x_0^2 - dy_0^2 \equiv (k^2 - d)y_0^2 \equiv 0 \pmod{N},$$

pa je $k^2 \equiv d \pmod{N}$. $\square$

Lema 1.3. *Dva primitivna rješenja jednadžbe $x^2 - dy^2 = N$ su asocirana ako i samo ako pripadaju istom broju.*

Dokaz: Neka su $x_0 + y_0\sqrt{d}$ i $x_1 + y_1\sqrt{d}$ dva primitivna asocirana rješenja jednadžbe $x^2 - dy^2 = N$. Tada postoji rješenje $u + v\sqrt{d}$ jednadžbe $x^2 - dy^2 = 1$ tako da je

$$x_1 = x_0u + dy_0v, \quad y_1 = x_0v + y_0u.$$

Ako $x_0 + y_0\sqrt{d}$ pripada broju k, onda vrijedi

$$y_1k \equiv x_0vk + y_0uk \equiv y_0vk^2 + x_0u \equiv dy_0v + x_0u \equiv x_1 \pmod{N},$$

pa i $x_1 + y_1\sqrt{d}$ pripada broju k.

Dokažimo sada obrat. Pretpostavimo da rješenja $x_0 + y_0\sqrt{d}$ i $x_1 + y_1\sqrt{d}$ pripadaju istom broju k. Tada je

$$x_0x_1 \equiv k^2y_0y_1 \equiv dy_0y_1 \pmod{N} \quad \text{i} \quad x_0y_1 \equiv ky_0y_1 \equiv y_0x_1 \pmod{N},$$

pa su rješenja asocirana. $\square$

Korolar 1.2. *Neka je N kvadratno slobodan cijeli broj. Broj klasa rješenja jednadžbe $x^2 - dy^2 = N$ je $\leq 2^{\omega(N)}$, gdje je $\omega(N)$ broj prostih faktora od N.*

Dokaz: Budući da je N kvadratno slobodan, sva rješenja su primitivna. Po Lemi 1.3, broj klasa je manji ili jednak broju mogućih k-ova, tj. broju rješenja kongruencije $x^2 \equiv d \pmod N$. Neka je $N = p_1 p_2 \cdots p_{\omega(N)}$. Za svaki $i = 1, 2, \ldots, \omega(N)$, kongruencija $x^2 \equiv d \pmod{p_i}$ ima najviše dva rješenja, pa je (po Kineskom teoremu o ostacima) broj rješenja kongruencije $x^2 \equiv d \pmod N$ manji ili jednak $2^{\omega(N)}$. □

Napomena 1.2. U općem slučaju, kada je $N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$, može se pokazati da je broj rješenja jednadžbe $x^2 - dy^2 = N$ odozgo omeđen s $\prod_{i=1}^{m}(\alpha_i + 1)$. Naime, ovdje treba uzeti u obzir i neprimitivna rješenja. Tako, npr. kada je $N = p^{2\beta+1}$, onda promatramo jednadžbe $x^2 - dy^2 = p^{2\gamma+1}$ za $0 \le \gamma \le \beta$. Svaka od njih ima najviše dvije klase primitivnih rješenja, pa je ukupan broj klasa $\le 2(\beta+1)$. Ako je $N = p^{2\beta}$, onda promatramo jednadžbe $x^2 - dy^2 = p^{2\gamma}$ za $0 \le \gamma \le \beta$. Za $\gamma = 0$ imamo točno jednu klasu rješenja, a za $\gamma \ge 1$ najviše dvije klase primitivnih rješenja, pa je ukupan broj klasa $\le 1 + 2\beta$.

Neka je $k^2 \equiv d \pmod N$. Definirajmo $M = \frac{k^2 - d}{N}$. Može se pokazati da jednadžba $x^2 - dy^2 = N$ ima rješenje koje pripada broju k ako i samo ako jednadžba $X^2 - dY^2 = M$ ima rješenje koje pripada broju k. Nadalje, veza među rješenjima ovih dviju jednadžbi je dana sa:

$$x = \left| \frac{dY \pm kX}{M} \right|, \quad y = \left| \frac{X \pm kY}{M} \right| \tag{1.22}$$

(ovdje predznak izabiremo tako da brojnici budu djeljivi s M). Pretpostavimo da je $|N| > \sqrt{d}$. Ako je $k^2 - d > 0$, onda je

$$|M| < \frac{k^2}{|N|} \le \frac{N^2/4}{|N|} = \frac{|N|}{4},$$

a ako je $k^2 - d < 0$, onda je

$$|M| \le \frac{d}{|N|} < \frac{d}{\sqrt{d}} = \sqrt{d}.$$

Stoga u konačno mnogo koraka dolazimo do jednadžbe oblika $x^2 - dy^2 = M'$ u kojoj $|M'| < \sqrt{d}$, koja se može riješiti pomoću verižnih razlomaka (Propozicija 1.4).

Primjer 1.6. *Dokažimo da jednadžba* $x^2 - 13y^2 = 53$ *ima rješenja.*

Rješenje: Promotrimo kongruenciju $k^2 \equiv 13 \pmod{53}$. Ona ima rješenja $k = \pm 15$. Pripadni M je jednak 4, a pripadna jednadžba je $X^2 - 13Y^2 = 4$. Znamo da ova jednadžba mora imati rješenja, a najmanje je $X + Y\sqrt{d} = 11 + 3\sqrt{13}$. Stoga i polazna jednadžba ima rješenja. Koristeći formule (1.22), dobivamo da je jedno rješenje

$$x = \left| \frac{13 \cdot 3 + 11 \cdot 15}{4} \right| = 51, \quad y = \left| \frac{11 + 15 \cdot 3}{4} \right| = 14.$$

♢

Poglavlje 2

Ternarne kvadratne forme

2.1 Legendreov teorem

Promatrat ćemo *ternarne kvadratne forme*

$$Q(x,y,z) = Ax^2 + Bxy + Cxz + Dy^2 + Eyz + Fz^2 \tag{2.1}$$

s racionalnim koeficijentima (tj. homogene polinome drugog stupnja u tri varijable). Zanimaju nas kriteriji za određivanje ima li jednadžba $Q(x,y,z) = 0$ netrivijalnih racionalnih rješenja (x,y,z) (rješenje $(x,y,z) = (0,0,0)$ ćemo zvati trivijalnim). Jasno je da je za ovakvu (homogenu) jednadžbu rješivost u racionalnim brojevima ekvivalentna rješivosti u relativno prostim cijelim brojevima (množimo sa zajedničkim nazivnikom; dijelimo sa zajedničkim faktorom).

Neka je $\mathcal{A} = [\alpha_{ij}]$ nesingularna 3×3 matrica s racionalnim koeficijentima. Tada za formu

$$g(x,y,z) = f(\alpha_{11}x + \alpha_{12}y + \alpha_{13}z, \alpha_{21}x + \alpha_{22}y + \alpha_{23}z, \alpha_{31}x + \alpha_{32}y + \alpha_{33}z)$$

kažemo da je ekvivalentna formi f. Na taj način očito dobivamo relaciju ekvivalencije. Nadalje, vrijedi da jednadžba $f(x,y,z) = 0$ ima netrivijalno rješenje ako i samo ako jednadžba $g(x,y,z) = 0$ ima netrivijalno rješenje (zato ćemo i za te dvije jednadžbe govoriti da su ekvivalentne).

Lema 2.1. *Jednadžba $Q(x,y,z) = 0$ ekvivalentna je nekoj jednadžbi oblika*

$$ax^2 + by^2 + cz^2 = 0,$$

gdje su a,b,c cijeli brojevi. Ako je $abc \neq 0$, onda se a,b,c mogu izabrati tako da budu kvadratno slobodni i u parovima relativno prosti.

Dokaz: Možemo pretpostaviti da je $A \neq 0$. U protivnom, polaznu formu možemo zamijeniti njoj ekvivalentnom formom koja će imati to svojstvo. Zaista, neka je $Q(x_0,y_0,z_0) = \alpha \neq 0$. Postoji nesingularna matrica $\mathcal{A}$ kojoj

je prvi stupac x_0, y_0, z_0. Primijenimo li supstituciju s matricom $\mathcal{A}$ na formu Q, dobivamo formu oblika $\alpha x^2 + \cdots$. Dakle, imamo $A \neq 0$. Sada supstitucija $x \mapsto x - \frac{By+Cz}{2A}$ eliminira članove uz xy i xz, tj. dobivamo jednadžbu oblika

$$A'x^2 + D'y^2 + E'yz + F'z^2 = 0.$$

Ako D', E', F' nisu svi jednaki 0, onda slično kao gore možemo pretpostaviti da je $D' \neq 0$. Primjenom supstitucije $y \mapsto y - \frac{E'z}{2D'}$ eliminiramo član uz yz i dobivamo jednadžbu oblika

$$ax^2 + by^2 + cz^2 = 0, \tag{2.2}$$

$a, b, c \in \mathbb{Q}$. Množeći sa zajedničkim nazivnikom, možemo pretpostaviti da su $a, b, c \in \mathbb{Z}$.

Ako sada npr. a nije kvadratno slobodan (i različit je od 0), tj. $a = a'a''^2$, onda supstitucijom $x \mapsto \frac{x}{a''}$ dobivamo jednadžbu oblika (2.2) u kojoj je a kvadratno slobodan. Dakle, možemo postići da su a, b, c kvadratno slobodni. Dijeleći sa zajedničkim faktorom, možemo postići da je $(a, b, c) = 1$. Pretpostavimo da a, b, c nisu u parovima relativno prosti. Neka je npr. p prost broj koji dijeli b i c, tj. $b = pb'$, $c = pc'$. Supstitucijom $x \mapsto px$ dobivamo jednadžbu

$$pax^2 + b'y^2 + c'z^2 = 0.$$

Na ovaj način možemo ukloniti sve eventualne zajedničke faktore dvaju od brojeva a, b, c, te postići da na kraju a, b, c budu u parovima relativno prosti. □

U daljnjem ćemo promatrati forme oblika $ax^2+by^2+cz^2$, gdje a, b, c zadovoljavaju uvjete iz Leme 2.1. Ti uvjeti se mogu objediniti tako da tražimo da je abc kvadratno slobodan. Također ćemo pretpostavljati da je forma negenerirana, što znači da je $abc \neq 0$. (Ako je $a = 0$, onda jednadžba $by^2 + cz^2 = 0$ ima netrivijalno rješenje ako i samo ako je $-bc$ kvadrat cijelog broja. A ako su b i c kvadratno slobodni i relativno prosti, to je moguće samo za $bc = -1$.)

Teorem 2.1 (Legendre)**.** *Neka su a, b, c cijeli brojevi različiti od 0, takvi da je broj abc kvadratno slobodan. Nužan i dovoljan uvjet da bi jednadžba $ax^2 + by^2 + cz^2 = 0$ imala netrivijalno rješenje u racionalnim brojevima je da*

1) brojevi a, b, c nisu svi pozitivni niti svi negativni;

2) broj $-bc$ je kvadratni ostatak modulo a,
broj $-ac$ je kvadratni ostatak modulo b,
broj $-ab$ je kvadratni ostatak modulo c.

Dokažimo najprije dvije leme. Prva govori o tome kako linearna homogena kongruencija uvijek ima relativno mala netrivijalna rješenja, dok

druga govori o tome kako možemo kombinirati faktorizacije kvadratne forme na linearne faktore po različitim modulima. Mi ćemo to iskoristiti da bi našu formu (2.2) faktorizirali modulo abc, te pomoću dobivenih linearnih faktora našli "malo" rješenje promatrane kongruencije. Bude li to rješenje dovoljno malo, kongruenciju ćemo moći zamjeniti jednakošću i time dokazati teorem.

Lema 2.2. *Neka su λ, μ, ν pozitivni realni brojevi takvi da je $\lambda\mu\nu = m \in \mathbb{Z}$. Tada kongruencija*

$$\alpha x + \beta y + \gamma z \equiv 0 \pmod{m}$$

(s cjelobrojnim koeficijentima) ima netrivijano rješenje x, y, z takvo da je $|x| \leq \lambda$, $|y| \leq \mu$, $|z| \leq \nu$.

Dokaz: Neka x prolazi skupom $\{0, 1, \ldots, \lfloor\lambda\rfloor\}$, y skupom $\{0, 1, \ldots, \lfloor\mu\rfloor\}$, a z skupom $\{0, 1, \ldots, \lfloor\nu\rfloor\}$. Tako dobivamo $(1 + \lfloor\lambda\rfloor)(1 + \lfloor\mu\rfloor)(1 + \lfloor\nu\rfloor)$ različitih trojki (x, y, z). Kako je $(1 + \lfloor\lambda\rfloor)(1 + \lfloor\mu\rfloor)(1 + \lfloor\nu\rfloor) > \lambda\mu\nu = m$, po Dirichletovom principu postoje dvije različite trojke (x_1, y_1, z_1) i (x_2, y_2, z_2) za koje vrijedi

$$\alpha x_1 + \beta y_1 + \gamma z_1 \equiv \alpha x_2 + \beta y_2 + \gamma z_2 \pmod{m}.$$

Sada je

$$\alpha(x_1 - x_2) + \beta(y_1 - y_2) + \gamma(z_1 - z_2) \equiv 0 \pmod{m},$$

te $|x_1 - x_2| \leq \lfloor\lambda\rfloor \leq \lambda$, $|y_1 - y_2| \leq \mu$, $|z_1 - z_2| \leq \nu$. □

Lema 2.3. *Neka je $(m, n) = 1$. Ako se $ax^2+by^2+cz^2$ faktorizira na linearne faktore modulo m i modulo n, onda se faktorizira na linearne faktore modulo mn.*

Dokaz: Po pretpostavci je

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv (\alpha_1 x + \beta_1 y + \gamma_1 z)(\alpha_2 x + \beta_2 y + \gamma_2 z) \pmod{m}, \\ ax^2 + by^2 + cz^2 &\equiv (\alpha_3 x + \beta_3 y + \gamma_3 z)(\alpha_4 x + \beta_4 y + \gamma_4 z) \pmod{n}, \end{aligned}$$

gdje su $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}$.

Po Kineskom teoremu o ostacima, postoje $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in \mathbb{Z}$ sa svojstvima:

$$\begin{aligned} \alpha &\equiv \alpha_1 \pmod{m}, & \alpha &\equiv \alpha_3 \pmod{n}; \\ \beta &\equiv \beta_1 \pmod{m}, & \beta &\equiv \beta_3 \pmod{n}; \\ \gamma &\equiv \gamma_1 \pmod{m}, & \gamma &\equiv \gamma_3 \pmod{n}; \\ \alpha' &\equiv \alpha_2 \pmod{m}, & \alpha' &\equiv \alpha_4 \pmod{n}; \\ \beta' &\equiv \beta_2 \pmod{m}, & \beta' &\equiv \beta_4 \pmod{n}; \\ \gamma' &\equiv \gamma_2 \pmod{m}, & \gamma' &\equiv \gamma_4 \pmod{n}. \end{aligned}$$

Tada kongruencija

$$ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z)$$

vrijedi i modulo m i modulo n, pa vrijedi i modulo mn. □

Dokaz Teorema 2.1:

Nužnost: Ako $ax^2 + by^2 + cz^2 = 0$ ima cjelobrojno rješenje $(x_0, y_0, z_0) \neq (0, 0, 0)$, onda je jasno da a, b, c ne mogu svi biti pozitivni (jer bi tada bilo $ax_0^2 + by_0^2 + cz_0^2 > 0$), niti svi negativni. Dijeleći s (x_0, y_0, z_0) ako je potrebno, možemo pretpostaviti da su x_0, y_0, z_0 relativno prosti.

Dokažimo sada da je $(c, x_0) = 1$. Pretpostavimo da prost broj p dijeli c i x_0. Tada $p|by_0^2$, ali $p \nmid b$, pa mora biti $p|y_0$. No, tada $p^2|cz_0^2$, pa jer je c kvadratno slobodan, imamo da $p|z_0$. To je kontradikcija s $(x_0, y_0, z_0) = 1$. Dakle, zaista je $(c, x_0) = 1$.

Zato postoji $u \in \mathbb{Z}$ takav da je $ux_0 \equiv 1 \pmod{c}$. Promotrimo kongruenciju

$$ax_0^2 + by_0^2 \equiv 0 \pmod{c}.$$

Množeći ju s $u^2 b$, dobivamo $(uby_0)^2 \equiv -ab \pmod{c}$, što upravo znači da je $-ab$ kvadratni ostatak modulo c. Sasvim na isti način se dokazuju analogne tvrdnje za $-ac$ i $-bc$.

Dovoljnost: Bez smanjenja općenitosti možemo pretpostaviti da je $a > 0$ i $b, c < 0$ (uočimo da ako a, b, c zadovoljavaju uvjete teorema, onda ih zadovoljavaju i $-a, -b, -c$).

Neka je $r^2 \equiv -ab \pmod{c}$, te $aa_1 \equiv 1 \pmod{c}$ (r i a_1 postoje po pretpostavkama na a, b, c). Tada je

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv ax^2 + by^2 \equiv aa_1(ax^2 + by^2) \equiv a_1(a^2x^2 + aby^2) \\ &\equiv a_1(a^2x^2 - r^2y^2) \equiv a_1(ax - ry)(ax + ry) \\ &\equiv (x - a_1 ry)(ax + ry) \pmod{c}. \end{aligned}$$

Dakle, $ax^2 + by^2 + cz^2$ je produkt linearnih faktora modulo c, a sasvim analogno i modulo a i modulo b. Primijenimo li Lemu 2.3 (dvaput), dobivamo da vrijedi

$$ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z) \pmod{abc}. \tag{2.3}$$

Sada ćemo primijeniti Lemu 2.2 na kongruenciju

$$\alpha x + \beta y + \gamma z \equiv 0 \pmod{abc} \tag{2.4}$$

uz $\lambda = \sqrt{bc}$, $\mu = \sqrt{|ac|}$, $\nu = \sqrt{|ab|}$. Zaključujemo da postoji netrivijalno rješenje (x_1, y_1, z_1) kongruencije (2.4) koje zadovoljava $|x_1| \leq \sqrt{bc}$, $|y_1| \leq \sqrt{|ac|}$, $|z_1| \leq \sqrt{|ab|}$. Uočimo da $\sqrt{bc}$ može biti cijeli broj samo ako je $bc = 1$, tj. $b = c = -1$. Sličan zaključak imamo i za preostala dva korijena. Stoga smo dobili slijedeće:

$x_1^2 \leq bc$ i jednakost vrijedi samo za $b = c = -1$;

$y_1^2 \leq -ac$ i jednakost vrijedi samo za $a = 1$, $c = -1$;

$z_1^2 \leq -ab$ i jednakost vrijedi samo za $a = 1$, $b = -1$.

Promotrimo najprije slučaj $b = c = -1$. Sada uvjet teorema postaje da je -1 kvadratni ostatak modulo a. No, dobro je poznato (vidi [UTB, Teorem 4.7]) da se tada a može zapisati kao suma dva kvadrata: $a = y_0^2 + z_0^2$, pa jednadžba $ax^2 + by^2 + cz^2 = ax^2 - y^2 - z^2 = 0$ ima netrivijalno rješenje $(x, y, z) = (1, y_0, z_0)$.

Dakle, sada možemo pretpostaviti da nije $b = c = -1$. U tom slučaju imamo

$$ax_1^2 + by_1^2 + cz_1^2 \leq ax_1^2 < abc,$$

$$ax_1^2 + by_1^2 + cz_1^2 \geq by_1^2 + cz_1^2 > b(-ac) + c(-ab) = -2abc,$$

tj. $-2abc < ax_1^2 + by_1^2 + cz_1^2 < abc$. No, zbog (2.3) i (2.4) vrijedi i $ax_1^2 + by_1^2 + cz_1^2 \equiv 0 \pmod{abc}$. To znači da imamo samo dvije mogućnosti (samo su dva višekratnika od abc u intervalu $\langle -2abc, abc\rangle$):

$$ax_1^2 + by_1^2 + cz_1^2 = 0 \quad \text{ili} \quad ax_1^2 + by_1^2 + cz_1^2 = -abc.$$

Ako je nastupio prvi slučaj, onda smo našli netrivijalno rješenje promatrane jednadžbe i dokaz je gotov. U drugom slučaju ćemo modificirati trojku (x_1, y_1, z_1) da bi pomoću nje ipak dobili rješenje promatrane jednadžbe. Definirajmo: $x_2 = -by_1 + x_1z_1$, $y_2 = ax_1 + y_1z_1$, $z_2 = z_1^2 + ab$. Imamo $c(z_1^2 + ab) = -ax_1^2 - by_1^2$, pa je

$$cz_2^2 = -(ax_1^2+by_1^2)(z_1^2+ab) = -a(-by_1+x_1z_1)^2-b(ax_1+y_1z_1)^2 = -ax_2^2-by_2^2.$$

Dakle, (x_2, y_2, z_2) je traženo rješenje. Treba još samo provjeriti što se događa u slučaju kada je ovo rješenje trivijalno. Tada je $z_1^2 = -ab$, pa jer je ab kvadratno slobodan, mora biti $a = 1$, $b = -1$. Dakle, imamo jednadžbu $x^2 - y^2 + cz^2 = 0$, koja očito ima netrivijalno rješenje $(x, y, z) = (1, 1, 0)$. □

Primjer 2.1. *Ispitajmo ima li diofantska jednadžba*

$$Q(x, y, z) = x^2 + 3y^2 + 5z^2 + 7xy + 9yz + 11xz = 0$$

netrivijalnih cjelobrojnih rješenja.

Rješenje: Želimo dobiti ekvivalentnu jednadžbu oblika $ax^2 + by^2 + cz^2 = 0$, pa postupamo kao u dokazu Leme 2.1. Najprije iz

$$Q(x, y, z) = \left(x + \frac{7}{2}y + \frac{11}{2}z\right)^2 - \frac{37}{4}y^2 - \frac{101}{4}z^2 - \frac{41}{4}yz$$

dobivamo ekvivalentnu jednadžbu

$$g(x,y,z) = 4x^2 - 37y^2 - 101z^2 - 41yz = 0,$$

a potom iz $g(x,y,z) = 4x^2 - 37\left(y + \frac{41}{74}z\right)^2 - \frac{13267}{148}z^2$ dobivamo jednadžbu $37 \cdot (4x)^2 - (74y)^2 - 13267z^2 = 0$. Konačno, eliminacijom kvadratnih faktora dolazimo do jednadžbe

$$h(x,y,z) = 37x^2 - y^2 - 13267z^2 = 0$$

na koju možemo primijeniti Legendreov teorem.

Vidimo da koeficijenti nisu istog predznaka. Nadalje, brojevi 37 i 13267 su prosti, pa još samo treba provjeriti da su Legendreovi simboli $\left(\frac{37}{13267}\right)$ i $\left(\frac{-13267}{37}\right)$ jednaki 1. Oba ova simbola su jednaka $\left(\frac{13267}{37}\right)$, pa računamo

$$\left(\frac{13267}{37}\right) = \left(\frac{21}{37}\right) = \left(\frac{37}{21}\right) = \left(\frac{16}{21}\right) = 1.$$

Prema tome, polazna jednadžba ima netrivijalno rješenje. U idućem poglavlju ćemo vidjeti kako se to rješenje može naći. ♢

2.2 Algoritmi za nalaženje netrivijalnih rješenja

Kao što smo vidjeli u prethodnom poglavlju, Legendreov teorem nam daje relativno efikasnu metodu za ispitivanje postojanja netrivijalnih nultočaka ternarne kvadratne forme. Preciznije, algoritam koji koristi Legendreov teorem ima subeksponencijalnu složenost, jer je njegov najzahtjevniji dio faktorizacija brojeva a, b, c na proste faktore, koja je nužna da bi mogli testirati jesu li zadovoljeni uvjeti s kvadratnim ostacima.

Postavlja se pitanje, nakon što smo ustanovili postojanje netrivijalnog rješenja, kako pronaći barem jedno takvo rješenje (ili čak sva rješenja).

Prikazat ćemo dva algoritma za nalaženje jednog netrivijalnog rješenja. Prvi algoritam je zasnovan na preciznim ocjenama (preciznijim od onih koje slijede iz gornjeg dokaza Teorema 2.1) koje mora zadovoljiti barem jedno netrivijalno rješenje.

Teorem 2.2 (Holzer)**.** *Neka je broj abc kvadratno slobodan, te $a > 0$ i $b, c < 0$. Ako jednadžba*

$$ax^2 + by^2 + cz^2 = 0 \tag{2.5}$$

ima netrivijalno rješenje, onda postoji barem jedno netrivijalno rješenje koje zadovoljava nejednakosti

$$|x| \leq \sqrt{bc}, \quad |y| \leq \sqrt{|ac|}, \quad |z| \leq \sqrt{|ab|}.$$

Dokaz: Neka je (x_0, y_0, z_0) rješenje od (2.5) u relativno prostim brojevima. Pretpostavimo da je $|x_0| > \sqrt{bc}$. Pokazat ćemo da tada postoji rješenje (x, y, z) od (2.5) u kojem je $|x| < |x_0|$. Nastavljajući isti postupak, dolazimo do zaključka da mora postojati rješenje u kojem je $|x| \leq \sqrt{bc}$. No, tada je $|b|y^2 \leq ax^2 \leq abc$, pa je $|y| \leq \sqrt{|ac|}$, a slično i $|z| \leq \sqrt{|ab|}$.

Pokažimo dakle kako se može dobiti rješenje u kojem je $|x| < |x_0|$. Stavimo

$$x = x_0 + tX, \quad y = y_0 + tY, \quad z = z_0 + tZ, \tag{2.6}$$

gdje su X, Y, Z cijeli brojevi koje ćemo na prikladan način izabrati malo kasnije. Može se reći da smo povukli (projektivni) pravac kroz (projektivnu) racionalnu točku na (projektivnoj) koniki. Zato očekujemo da će se pravac i konika sjeći u još jednoj točki. Zaista, uvrštavanjem (2.6) u (2.5), te kraćenjem s t (slobodni član je jednak nula jer je (x_0, y_0, z_0) rješenje), dobivamo

$$t = -\frac{2(ax_0X + by_0Y + cz_0Z)}{aX^2 + bY^2 + cZ^2}.$$

Stoga je

$$\begin{aligned}
\delta x &= x_0(aX^2 + bY^2 + cZ^2) - 2X(ax_0X + by_0Y + cz_0Z), \\
\delta y &= y_0(aX^2 + bY^2 + cZ^2) - 2Y(ax_0X + by_0Y + cz_0Z), \\
\delta z &= z_0(aX^2 + bY^2 + cZ^2) - 2Z(ax_0X + by_0Y + cz_0Z).
\end{aligned}$$

gdje je δ zajednički djelitelj triju izraza na desnoj strani.

Pretpostavimo sada da $\delta|a$ i $\delta|(y_0Z - z_0Y)$. Pokazat ćemo da su tada x, y, z cijeli brojevi. Dovoljno je dokazati da $\delta|(bY^2+cZ^2)$ i $\delta|(by_0Y+cz_0Z)$. Iz $ax_0^2+by_0^2+cz_0^2 = 0$ i pretpostavke da su x_0, y_0, z_0 relativno prosti, te a, b, c kvadratno slobodni i u parovima relativno prosti, slijedi da je $(\delta, bcy_0z_0) = 1$. Sada imamo:

$$\begin{aligned} bY^2 + cZ^2 &\equiv y_0^{-2}Y^2(by_0^2 + cz_0^2) \equiv -ax_0^2y_0^{-2}Y^2 \equiv 0 \pmod{\delta}, \\ by_0Y + cz_0Z &\equiv y_0^{-1}Y(by_0^2 + cz_0^2) \equiv 0 \pmod{\delta}, \end{aligned}$$

čime smo dokazali da su stvarno x, y, z cijeli brojevi. Želimo izabrati δ, X, Y, Z tako da $|x|$ bude što manji. Imamo:

$$-\frac{\delta x}{ax_0} = \left(X + \frac{by_0Y + cz_0Z}{ax_0}\right)^2 + \frac{bc}{a^2x_0^2}(y_0Z - z_0Y)^2. \tag{2.7}$$

Odaberimo sada Y i Z kao rješenja linearne kongruencije $y_0Z - z_0Y = \delta$. Dalje se dokaz malo razlikuje u ovisnosti o parnosti od a. Neka je najprije a paran. Tada stavljamo $\delta = \frac{a}{2}$, a za X izabiremo najbliži cijeli broj broju $-\frac{by_0Y+cz_0Z}{ax_0}$ (da bi minimizirali prvi pribrojnik na desnoj strani u (2.7)). Tada iz (2.7) dobivamo

$$\frac{1}{2}\frac{|x|}{|x_0|} \leq \frac{1}{4} + \frac{bc}{4x_0^2} < \frac{1}{2},$$

tj. $|x| < |x_0|$, što se i tražilo.

U slučaju kada je a neparan, potrebna je malo modifikacija da bi dobili isti zaključak. Sada je δ neparan. Ako su desne strane u jednakostima za δx, δy i δz parne, onda su djeljive s 2δ, a to znači da u (2.7) možemo δ zamijeniti s 2δ. Stavljamo $\delta = a$, te X izabiremo kao najbliži cijeli broj broju $-\frac{by_0Y+cz_0Z}{ax_0}$ koji zadovoljava dodatno svojstvo da je broj $aX+bY+cZ$ paran. Dobivamo $2\frac{|x|}{|x_0|} < 1 + 1$, te ponovo $|x| < |x_0|$. □

Holzerov teorem nam daje mogućnost nalaženja netrivijalnog rješenja jednadžbe (2.5) testiranjem svih parova x, y takvih da je $0 \leq x \leq \sqrt{|bc|}$, $0 \leq y \leq \sqrt{|ac|}$ i ispitivanjem je li broj $-\frac{ax^2+by^2}{c}$ kvadrat cijelog broja. O algoritmima za efikasno testiranje je li dani prirodni broj kvadrat može se naći u skripti iz kolegija *Teorija brojeva u kriptografiji*, Poglavlje 2.8. No, parova koje treba ispitati ima približno $|c|\sqrt{|ab|}$, pa ovo daje prilično neefikasan (eksponencijalni) algoritam na nalaženje rješenja. Prikazat ćemo dva efikasnija algoritma. Prvi koristi Holzerov teorem i opću ideju za nalaženje rješenja jednadžbe oblika $y^2 = f(x_1, \ldots, x_n)$. Ona se sastoji u tome da se za dovoljan broj prostih brojeva p eliminiraju ("prosiju") vrijednosti ($x_1 \bmod p, \ldots, x_n \bmod p$) za koje $f(x_1, \ldots, x_n)$ nije kvadrat modulo p. Relativna

efikasnost ove metode leži u činjenici da su samo pola elemenata iz reduciranog sustava ostataka modulo p kvadratni ostaci modulo p (vidi [UTB, Teorem 3.1]).

Bez smanjenja općenitosti možemo pretpostaviti da je $|a| \leq |b| \leq |c|$. Tada je $|y| \leq c$, pa je y u potpunosti određen s $y \bmod c$, a to povlači da je y skoro u potpunosti određen s x. Zaista, ako je $y \equiv rx \pmod{|c|}$, onda je r rješenje kongruencije $br^2 \equiv -a \pmod{|c|}$. Ova je kongruencija sigurno rješiva po Legendreovom teoremu, a broj rješenja joj ovisi o broju prostih faktora od $|c|$. Kongruenciju možemo efikasno riješiti u koliko nam je poznata faktorizacija broja $|c|$ na proste faktore. Sljedeći algoritam sito $(x_0,\ M,\ r)$ nalazi rješenje (rješive) jednadžbe $ax^2 + by^2 + cz^2 = 0$, koje zadovoljava granice iz Holzerovog teorema, te dodatne uvjete da je $x \equiv x_0 \pmod{M}$, $y \equiv rx \pmod{|c|}$. Poziva se sa sito $(0,\ 1,\ r)$ za sve r koji su rješenje kongruencije $br^2 \equiv -a \pmod{c}$.

Rekurzivni algoritam sita za $ax^2 + by^2 + cz^2 = 0$

sito $(x_0,\ M,\ r)$ =
  p najmanji prost broj koji ne dijeli $M \cdot c$
  for $x_1 = x_0$ to $\max(p \cdot M, \sqrt{|bc|})$ step M,
  $y_1 = r \cdot x \bmod |c|$
  if $(p \nmid x_1$ and $p \nmid y_1)$ then
  if $(-(a \cdot x_1^2 + b \cdot y_1^2) \cdot c^{-1}$ je kvadrat modulo $p)$ then
    if $(p \cdot M > \sqrt{|bc|})$ then
      $z_2 = -(a \cdot x_1^2 + b \cdot y_1^2)/c$
      if (z_2 je kvadrat) then print $(x_1,\ y_1,\ \sqrt{z_2})$
    else sito $(x_1,\ p \cdot M,\ r)$

Druga metoda koju ćemo prikazati naziva se *metoda silaska* i analogna je metodi za rješavanje pellovskih jednadžbi koju smo opisali na kraju Poglavlja 1.3. Ovdje je ideja polaznu jednadžbu zamijeniti s jednadžbom koja ima manje koeficijente, te taj postupak ("silazak") nastaviti sve dok ne dođemo do jednadžbe koja ima očito rješenje.

Ponovo krećemo od jednadžbe $ax^2 + by^2 + cz^2 = 0$ u kojoj su a, b, c kvadratno slobodni i u parovima relativno prosti, te zadovoljavaju uvjete "lokalne rješivosti" iz Legendreovog teorema. Množenjem jednadžbe sa c, te supstitucijom $z \mapsto \frac{w}{c}$, dobivamo jednadžbu oblika

$$w^2 = Ax^2 + By^2, \tag{2.8}$$

gdje je $A = -ac$, $B = -bc$, pa su A, B kvadratno slobodni. Možemo pretpostaviti da je $|A| \leq |B|$, a također i da je $|B| \neq 1$ (jer ako je $B = 1$, onda imamo očito rješenje $(x, y, w) = (0, 1, 1)$, a ako je $B = -1$, onda je $A = 1$, pa imamo očito rješenje $(x, y, w) = (1, 0, 1)$).

Izaberimo sada $0 \leq r \leq \frac{|B|}{2}$ tako da je $r^2 \equiv A \pmod{|B|}$. Takav r postoji jer je po pretpostavci $-ac$ kvadratni ostatak modulo b, pa postoji r_1 takav da je $r_1^2 \equiv A \pmod{|b|}$. Sada izaberemo r tako da vrijedi $r \equiv r_1 \pmod{|b|}$ i $r \equiv 0 \pmod{|c|}$. Stavimo $r^2 - A = BQ = BB'd^2$, gdje je B' kvadratno slobodan. Tada je

$$|B'| = \left|\frac{r^2 - A}{Bd^2}\right| \leq \left|\frac{r^2 - A}{B}\right| \leq \left|\frac{r^2}{B}\right| + \left|\frac{A}{B}\right| \leq \frac{|B|}{4} + 1 < |B|.$$

Uz supstituciju

$$x = \frac{rX - W}{r^2 - A}, \quad y = \frac{Y}{Bd}, \quad w = \frac{-AX + rW}{r^2 - A},$$

jednadžba (2.8) postaje

$$W^2 = AX^2 + B'Y^2. \tag{2.9}$$

Zaista,

$$B'Y^2 = B'B^2d^2y^2 = (r^2 - A)By^2 = (r^2 - A)(w^2 - Ax^2) = W^2 - AX^2.$$

Dakle, dobili smo jednadžbu istog oblika, ali s manjim koeficijentima (po apsolutnoj vrijednosti). Postupak nastavljamo sve dok ne dobijemo $A = 1$ ili $B = 1$.

Algoritam silaska za $w^2 = Ax^2 + By^2$

silazak $(A,\ B) =$
  if $(|A| > |B|)$ then $(y, x, w) =$ silazak $(B,\ A)$
  if $(A = 1)$ then return $(1, 0, 1)$
  if $(B = 1)$ then return $(0, 1, 1)$
  naći $r \in [0, 1, \ldots, |B|/2]$ takav da je $r^2 \equiv A \pmod{|B|}$
  neka je d_2 najveći kvadrat koji dijeli $Q = (r^2 - A)/B$
  $B' = Q/d_2$, $d = \sqrt{d_2}$
  $(X, Y, W) =$ silazak $(A,\ B')$
  $y = B'dY$, $x = rX - W$, $w = -AX + rW$
  return (x, y, w)

Opisani algoritam silaska daje prilično efikasnu metodu na nalaženje netrivijalnih rješenja promatrane jednadžbe. Budući da za dovoljno veliki $|B|$ (već za $|B| > 12$) vrijedi $|B'| < \frac{|B|}{3}$, broj koraka u algoritmu je $O(\log |B|)$. No, ovo ipak nije polinomijalni algoritam, već samo subeksponencijalni jer

- moramo faktorizirati $|B|$ da bismo mogli efikasno riješiti kvadratnu kongruenciju i naći r;
- moramo faktorizirati $|Q|$ da bismo mogli odrediti njegov kvadratno slobodni faktor B'.

Primjer 2.2. *Nađimo jedno netrivijalno rješenje jednadžbe*

$$w^2 = 37x^2 - 13267y^2$$

iz Primjera 2.1 (promijenili smo nazive varijabli da bi slijedili notaciju iz algoritma silaska).

Rješenje: Primijenit ćemo algoritam silaska. Najprije treba riješiti kongruenciju $r^2 \equiv 37 \pmod{13267}$. Jer je 13267 prost broj i $13267 \equiv 3 \pmod 4$, imamo (vidi [UTB, Primjer 3.6]) da je $r \equiv \pm 37^{(13267+1)/4} \pmod{13267}$, pa uzimamo $r = 3167$. Sada je $r^2 - A = B \cdot (-756) = B \cdot (-21) \cdot 6^2$, pa je $B' = -21$. Dakle, nova jednadžba je

$$W^2 = 37X^2 - 21Y^2.$$

Postupak bi mogli nastaviti, ali sada se sasvim očito da je $(1, 1, 4)$ rješenje zadnje jednadžbe. Iz njega dobivamo jedno rješenje polazne jednadžbe: $x = 3163$, $y = 126$, $z = 12631$. ♢

Konačno, postavlja se pitanje kako iz jednog netrivijalnog rješenja dobiti sva ostala (cjelobrojna ili racionalna) rješenja, i je li to uopće moguće. Odgovor je potvrdan, a metoda vrlo slična dokazu Holzerovog teorema.

Neka je (x_0, y_0, z_0) netrivijalno rješenje jednadžbe

$$Q(x, y, z) = Ax^2 + Bxy + Cxz + Dy^2 + Eyz + Fz^2 = 0.$$

Opće rješenje tražimo u obliku

$$x = rx_0, \quad y = ry_0 + s, \quad z = rz_0 + t, \tag{2.10}$$

gdje su r, s, t racionalni parametri. Uvrštavanjem u jednadžbu dobivamo:

$$r^2 Q(x_0, y_0, z_0) - r(c_1 s + c_2 t) + (c_3 s^2 + c_4 st + c_5 t^2) = 0,$$

za neke konstante $c_1, \ldots, c_5$. Budući da je po pretpostavci $Q(x_0, y_0, z_0) = 0$, dobivamo $r = \frac{c_3 s^2 + c_4 st + c_5 t^2}{c_1 s + c_2 t}$. Ako nas zanimaju samo racionalna rješenja, onda uvrštavanjem ove vrijednosti za r u (2.10), dobivamo formule za sva racionalna rješenja jednadžbe $Q(x, y, z) = 0$.

Slučaj s cjelobrojnim rješenjima je nešto kompliciraniji. Naime, uvrštavanjem, te rješavanjem nazivnika i zajedničkih faktora od s i t, dobivamo da postoje $g \in \mathbb{Z}$, te $\alpha_{ij} \in \mathbb{Z}$ tako da vrijedi

$$\begin{aligned} gx &= a_{11}s^2 + a_{12}st + a_{13}t^2, \\ gy &= a_{21}s^2 + a_{22}st + a_{23}t^2, \\ gz &= a_{31}s^2 + a_{32}st + a_{33}t^2. \end{aligned}$$

Pokazat ćemo da g može poprimiti samo konačno mnogo vrijednosti, te time u principu riješiti problem. Zapišimo gornji sustav matrično:

$$g\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A\begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix}.$$

Odavde je

$$g\,\mathrm{adj}(A)\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \det A\begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix}.$$

Budući da su s i t relativno prosti (podijelili smo ih sa zajedničkim faktorom), zaključujemo da $g|\det A$. Ostaje još samo vidjeti da je $\det A \neq 0$, no direktnim računom se provjeri da to vrijedi za svaku nedegeneriranu formu (uvjet $\det A = 0$ je ekvivalentan uvjetu da je diskriminanta forme jednaka 0).

Ilustrirat ćemo upravo opisani postupak na sljedećoj propoziciji.

Propozicija 2.1. *Neke je $|p|$ neparan prost broj. Sva rješenja jednadžbe*

$$x^2 + py^2 = z^2 \tag{2.11}$$

u relativno prostim cijelim brojevima dana su s jednom od sljedećih dvaju parametrizacija:

1) $x = \pm(s - pt^2)$, $y = 2st$, $z = \pm(s^2 + pt^2)$,
gdje su s, t relativno prosti cijeli brojevi različite parnosti i $p \nmid s$;

2) $x = \pm\left(\frac{p-1}{2}(s^2 + t^2) + (p+1)st\right)$, $y = s^2 - t^2$,
$z = \pm\left(\frac{p+1}{2}(s^2 + t^2) + (p-1)st\right)$,
gdje su s, t relativno prosti cijeli brojevi različite parnosti i $s \not\equiv t \pmod p$.

Dokaz: Koristimo očito (ali netrivijalno u smislu definicije trivijalnosti) rješenje od (2.11): $(x, y, z) = (1, 0, 1)$. Imamo transformaciju:

$$x = r, \quad y = t, \quad z = r + s.$$

Uvrštavanjem u (2.11), dobivamo $r^2 + pt^2 = r^2 + 2rs + s^2$, odnosno $2rs = pt^2 - s^2$, tj. $r = \frac{pt^2 - s^2}{2s}$. Dakle, postoji $g \in \mathbb{Z}$ takav da je

$$\begin{aligned} gx &= pt^2 - s^2, \\ gy &= 2st, \\ gz &= s^2 + pt^2. \end{aligned}$$

Ovdje možemo pretpostaviti da su s i t relativno prosti. Matrica A je ovdje

$$\begin{pmatrix} -1 & 0 & p \\ 0 & 2 & 0 \\ 1 & 0 & p \end{pmatrix}$$

i imamo $\det A = -4p$. Dakle, $g|4p$.

Ako $p \nmid s$, onda je $g = \pm 1$, ± 2 ili ± 4. Zadnji slučaj otpada jer bi tada s i t bili oba parni. Za $g = \pm 1$ dobivamo upravo parametrizaciju 1). Ako je $g = \pm 2$, onda su s i t oba neparni, pa su $s_1 = \frac{s+t}{2}$ i $t_1 = \frac{t-s}{2}$ relativno prosti brojevi različite parnosti i $s_1 \not\equiv t_1 \pmod{p}$. Uvrštavanjem dobivamo upravo parametrizaciju 2).

Ako $p|s$, onda stavimo $g = pg'$ i kraćenjem s p svodimo ovaj slučaj na prethodni (uz zamjenjenu ulogu od s i t). □

2.3 Princip Hassea i Minkowskoga

Neka je $f(x_1, \ldots, x_n)$ polinom s cjelobrojnim koeficijentima. Ako jednadžba $f(x_1, \ldots, x_n) = 0$ ima cjelobrojnih rješenja, onda je jasno da kongruencija $f(x_1, \ldots, x_n) \equiv 0 \pmod{m}$ ima rješenja za svaki cijeli broj m. Zanima nas vrijedi li obrat ove tvrdnje (i uz koje uvjete na f).

Dokažimo najprije sljedeću posljedicu Legendreovog teorema 2.1:

Teorem 2.3. *Neka su a, b, c cijeli brojevi koji nisu svi istog predznaka, te takvi da je abc kvadratno slobodan. Tada jednadžba*

$$ax^2 + by^2 + cz^2 = 0 \tag{2.12}$$

ima netrivijalno rješenje ako i samo ako za svaki cijeli broj m kongruencija

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{m} \tag{2.13}$$

ima rješenje takvo da je $(x, y, z, m) = 1$.

Dokaz: Očito je da ako (2.12) ima netrivijalno rješenje (x, y, z), onda ta trojka zadovoljava i kongruenciju (2.13), a možemo pretpostaviti da su x, y, z relativno prosti. Dokažimo drugi smjer u teoremu. Prema Legendreovom teoremu, zbog simetrije, dovoljno je dokazati da je $-ab$ kvadratni ostatak modulo c. Neka je p neki prosti faktor od c. Stavimo $m = p^2$ i promotrimo rješenje od (2.13) koje zadovoljava uvjet $(x, y, z, p) = 1$. Ako $p|y$, onda $p|x$, pa $p^2|cz^2$, te dobivamo da i $p|z$, što je kontradikcija s $(x, y, z, p) = 1$. Dakle, $p \nmid y$ i analogno $p \nmid x$. Sada iz kongruencije $ax^2 + by^2 \equiv 0 \pmod{p}$ dobivamo $-ab \equiv (byx^{-1})^2 \pmod{p}$, pa je $-ab$ kvadratni ostatak modulo p. Kako to vrijedi za svaki prosti faktor p od c, zaključujemo da je $-ab$ kvadratni ostatak modulo c. □

Jasno je, po Kineskom teoremu o ostacima, da je općenito uvjet

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{m}$$

dovoljno provjeriti za sve module oblika $m = p^k$, p prost, $k \in \mathbb{N}$. U slučaju kongruencije (2.13), prema Legendreovom teoremu, to je dovoljno provjeriti samo za proste brojeve p sa svojstvom $p|abc$. Dat ćemo još jedno objašnjenje tog fenomena.

Teorem 2.4 (Chevalley)**.** *Neka je $f(x_1, \ldots, x_n)$ polinom stupnja $d < n$. Ako je kongruencija*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p} \tag{2.14}$$

rješiva, onda ona ima barem dva rješenja.

Dokaz: Dokazat ćemo da je broj M n-torki $(x_1, \ldots, x_n) \in \mathbb{F}_p^n$ za koje je $f(x_1, \ldots, x_n) \not\equiv 0 \pmod{p}$ djeljiv s p. Tada će i broj rješenja kongruencije (2.14) biti djeljiv s p (jer je broj svih n-torki p^n), odakle će slijediti tvrdnja teorema.

Po Malom Fermatovom teoremu je

$$M \equiv \sum_{x_1,\ldots,x_n \in \mathbb{F}_p} f(x_1, \ldots, x_n)^{p-1} \pmod{p}.$$

Posljednja suma se može shvatiti kao suma pribrojnika oblika $x_1^{\delta_1} \cdots x_n^{\delta_n}$, gdje je $\delta_1 + \cdots \delta_n \leq d(p-1) < n(p-1)$. Dakle, u svakom pribrojniku je barem jedan eksponenent δ_j manji od $p-1$. Zato je dovoljno dokazati da za svaki δ, takav da je $0 \leq \delta < p-1$, vrijedi

$$S(\delta) := \sum_{x=0}^{p-1} x^\delta \equiv 0 \pmod{p}.$$

Za $\delta = 0$ imamo $S(0) = p \equiv 0 \pmod{p}$. Neka je $1 \leq \delta < p-1$, te neka je g primitivni korijen modulo p (za dokaz egzistencije primitivnog korijena vidjeti npr. [UTB, Teorem 2.19]). Tada je $g^\delta \not\equiv 1 \pmod{p}$, pa iz

$$S(\delta) = \sum_{x=0}^{p-1} x^\delta \equiv \sum_{x=0}^{p-1} (gx)^\delta \equiv g^\delta S(\delta) \pmod{p},$$

tj. $S(\delta)(1 - g^\delta) \equiv 0 \pmod{p}$, slijedi $S(\delta) \equiv 0 \pmod{p}$. □

Primijenimo li teorem 2.4 na kongruenciju

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}, \tag{2.15}$$

kod koje je $d = 2$ i $n = 3$, zaključujemo da ona ima netrivijalno rješenje za svaki p (ima trivijalno rješenje $(0, 0, 0)$, pa mora imati barem još jedno).

Neka sada $p \nmid 2abc$ (slučaj $p = 2$ ćemo diskutirati kasnije). Tada pomoću Henselove leme (vidi [UTB, Teorem 2.16]), rješenje modulo p možemo "podići" do rješenja modulo p^k. Zaista, neka je (x_0, y_0, z_0) netrivijalno rješenje kongruencije (2.15), te neka je npr. $x_0 \not\equiv 0 \pmod{p}$. Tada funkcija $f(x) = ax^2 + by_0^2 + cz_0^2$ zadovoljava uvjete Henselove leme. Naime, $f(x_0) \equiv 0 \pmod{p}$ i $f'(x_0) = 2ax_0 \not\equiv 0 \pmod{p}$ (tj. x_0 nije "dvostruki" korijen). Zato za svaki $k \in \mathbb{N}$ postoji rješenje kongruencije $f(x) \equiv 0 \pmod{p^k}$ takvo da je $x \equiv x_0 \pmod{p}$.

Vratimo se još jednom na Legendreov teorem. Vidimo da u njemu postoje (barem na prvi pogled) dva tipa uvjeta. Prvi govori o predznaku koeficijenata i njega se može interpretirati kao uvjet da jednadžba ima (netrivijalno) rješenje u $\mathbb{R}$. Upravo smo vidjeli da se drugi tip uvjeta može shvatiti kao zahtjev za rješivost pripadnih kongruencija modulo p^k. Postoji način da se

ova dva tipa uvjeta objedine, a za to nam treba pojam p-adskih brojeva. Naime, skup (polje) $\mathbb{R}$ možemo shvatiti kao upotpunjenje polja $\mathbb{Q}$ s obzirom na standardnu (arhimedsku) normu $|x|_\infty := |x|$, koja je obična apsolutna vrijednost. No, postoje i drugi (važni) načini za uvođenje norme na $\mathbb{Q}$. Neka je p prost broj. Tada svaki $x \in \mathbb{Q}$, $x \neq 0$, ima jedinstven prikaz u obliku

$$x = \frac{a}{b} \cdot p^{\nu_p(x)}, \quad p \nmid ab, \quad \nu_p(x) \in \mathbb{Z}.$$

Funkcija $x \mapsto \nu_p(x)$ se zove *p-adska valuacija*, a funkcija

$$|x|_p = \begin{cases} p^{-\nu_p(x)}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

p-adska norma (p-adska apsolutna vrijednost). U ovoj normi je broj "blizu" nule, ako je djeljiv s "velikom" potencijom od p, što je u skladu s time da je 0 djeljiva s proizvoljno velikom potencijom od p. Lako se vidi da funkcije $|\ |_p$ imaju svojstva norme. Što se tiče nejednakosti trokuta, one je zadovoljavaju u "jačoj" formi: $|x+y|_p \leq \max\{|x|_p, |y|_p\}$, pa se ove norme nazivaju nearhimedske, a metrički prostori koje induciraju ultrametrički (u njima su svi trokuti jednakokračni). Za dvije norme se kaže da su *ekvivalentne* ako induciraju istu topologiju (otvoreni skupovi im se podudaraju). Prema poznatom teoremu Ostrowskoga, svaka norma na $\mathbb{Q}$ je ekvivalentna nekoj od gore navedenih normi $|\ |_p$, za p prost ili $p = \infty$.

Polje $\mathbb{Q}$ nije potpuno u odnosu na normu $|\ |_p$ (kao što nije bilo ni u odnosu na $|\ |_\infty$). Njegovim upotpunjenjem, analogno kao kod konstrukcije polja $\mathbb{R}$, dobivamo polja $\mathbb{Q}_p$. To znači da se norma $|\ |_p$ može proširiti sa $\mathbb{Q}$ na $\mathbb{Q}_p$, $\mathbb{Q}_p$ je potpun u odnosu na $|\ |_p$ i $\mathbb{Q}$ je gust u $\mathbb{Q}_p$. Slično kao u slučaju skupa $\mathbb{R}$, postoji i spretnija interpetacija elemenata od $\mathbb{Q}_p$ od one koja se dobije po definiciji (kao klase Cauchyjevih nizova). Naime, svaki $\alpha \in \mathbb{Q}_p$ se može na jedinstven način zapisati u obliku

$$\alpha = \sum_{k \geq \nu_p(\alpha)} a_k p^k,$$

gdje je $\nu_p(\alpha) \in \mathbb{Z}$, a za "znamenke" a_k vrijedi $0 \leq a_k < p$. Elemente od $\mathbb{Q}_p$ zovemo *p-adski brojevi*. Elemente od $\mathbb{Q}_p$ za koje je $|\alpha|_p \leq 1$, tj. $\nu_p(\alpha) \geq 0$, zovemo *p-adski cijeli brojevi* i skup svih takvih elemenata označavamo sa $\mathbb{Z}_p$. Dakle, elementi od $\mathbb{Z}_p$ su oblika $\alpha = p^k \cdot \varepsilon$, gdje je $k \geq 0$, a

$$\varepsilon = e_0 + e_1 p + e_2 p^2 + \cdots, \quad 0 \leq e_i < p, \ e_0 \neq 0, \tag{2.16}$$

i ε je invertibilni element (jedinica) u prstenu $\mathbb{Z}_p$.

Lema 2.4. *Broj $\alpha = p^{2k} \cdot \varepsilon$, gdje je ε oblika (2.16), je kvadrat u $\mathbb{Z}_p$ ako i samo ako*

i) e_0 *je kvadratni ostatak modulo* p*, u slučaju kada je* $p \neq 2$*;*

ii) $\varepsilon \equiv 1 \pmod 8$*, u slučaju* $p = 2$

Dokaz:

i) Ako je $\alpha = (p^k\eta)^2$, gdje je $\eta = n_0 + n_1 p + \cdots$ jedinica, onda je $e_0 \equiv n_0^2 \pmod p$, pa je e_0 kvadratni ostatak modulo p.

Obratno, neka je $e_0 \equiv b^2 \pmod p$. Primijenimo Henselovu lemu na polinom $f(x) = x^2 - \varepsilon$. Iz $f(b) \equiv 0 \pmod p$ i $f'(b) = 2b \not\equiv 0 \pmod p$ slijedi da postoji $\eta \in \mathbb{Z}_p$ takav da je $f(\eta) = 0$ i $\eta \equiv b \pmod p$. Tada je $\varepsilon = \eta^2$.

ii) Nužnost slijedi iz činjenice da je kvadrat neparnog cijelog broja kongruentan 1 modulo 8. Za dovoljnost, promotrimo ponovo polinom $f(x) = x^2 - \varepsilon$. Za njega sada vrijedi $f(1) \equiv 0 \pmod 8$ i $f'(1) = 2 \not\equiv 0 \pmod 4$. Slično kao u dokazu Henselove leme, pokazuje se da postoji $\eta \in \mathbb{Z}_p$ takav da je $f(\eta) = 0$ i $\eta \equiv 1 \pmod 4$. Tada je $\varepsilon = \eta^2$.

Sada uvjete na rješivost kongruencija modulo p^k, $k \in \mathbb{N}$, možemo zamjeniti s jednim uvjetom da je jednadžba rješiva u p-adskim cijelim brojevima.

Teorem 2.5 (Hasse-Minkowski)**.** *Kvadratna forma s racionalnim koeficijentima ima netrivijalno rješenje u* $\mathbb{Q}$ *ako i samo ako ima netrivijalno rješenje u* $\mathbb{R}$ *i u* $\mathbb{Q}_p$ *za svaki prost broj* p*.*

Za funkcije koje zadovoljavaju tvrdnju iz Teorema 2.5 kažemo da zadovoljavaju *lokalno-globalni princip* (ako imaju rješenja u "lokalnim" poljima $\mathbb{R}$, $\mathbb{Q}_p$, onda imaju rješenje i u "globalnom" polju $\mathbb{Q}$) ili *princip Hassea i Minkowskoga*.

Mi smo Teorem 2.5 dokazali u slučaju ternarnih kvadratnih formi, tj. u slučaju $n = 3$. Slučaj $n = 1$ je trivijalan, a slučaj $n = 2$ vrlo jednostavan. Zaista, dovoljno je promatrati jednadžbe oblika $x^2 + dy^2 = 0$. Iz rješivosti u $\mathbb{R}$ slijedi da je $d < 0$. Neka je $d = -p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Iz rješivosti u $\mathbb{Q}_{p_i}$ slijedi da je α_i paran. Zato je $-d$ kvadrat prirodnog broja, pa jednadžba ima rješenja u $\mathbb{Q}$.

No, ne zadovoljavaju sve funkcije lokalno-globalni princip. Među najpoznatije kontraprimjere spadaju $3x^3 + 4y^3 - 5z^3$ (pronašao ga je Selmer) i $x^4 - 17 = 2y^2$ (pronašli su ga Lind i Reichardt). Dakle, već za kubne ternarne forme taj princip ne vrijedi. Mi ćemo pokazati primjer koji je jednostavniji, ali i specijalniji, jer je forma reducibilna.

Primjer 2.3. *Pokažimo da jednadžba*

$$(x^2 - 2y^2)(x^2 - 17y^2)(x^2 - 34y^2) = 0$$

ima netrivijalna rješenja u $\mathbb{R}$ *i* $\mathbb{Q}_p$ *za svaki* p*, ali nema u* $\mathbb{Q}$*.*

Rješenje: Očito je da jednadžba ima rješenja u $\mathbb{R}$, a nema u $\mathbb{Q}$.

Neka je $p \neq 2, 17$. Tada je $\left(\frac{2}{p}\right)\left(\frac{17}{p}\right)\left(\frac{34}{p}\right) = 1$, pa je barem jedan od ovih Legendreovih simbola jednak 1. To znači da je $x_0^2 \equiv a \pmod{p}$ za neki $a \in \{2, 17, 34\}$, pa po Henselovoj lemi x_0 možemo podići do rješenja u $\mathbb{Z}_p$.

Za $p = 17$, imamo kongruenciju $x^2 \equiv 2 \pmod{17}$, koja ima rješenja jer je $\left(\frac{2}{17}\right) = 1$, pa imamo rješenje u $\mathbb{Z}_{17}$.

Za $p = 2$, po Lemi 2.4 znamo da jednadžba $x^2 = 17$ ima rješenje u $\mathbb{Z}_p$ jer je $17 \equiv 1 \pmod{8}$. Pokažimo kako se to rješenje može konstruirati. Kao što smo rekli u dokazu Leme 2.4, slijedi se dokaz Henselove leme. Prematramo kongruencije $x^2 \equiv 17 \pmod{2^k}$. Ova kongruencija očito ima rješenja za $k = 1, 2, 3, 4$ (možemo uzeti $x = 1$). Za $k = 5$, promatramo x-eve u obliku $x = \pm(1+8t_5)$. Dobivamo uvjet $1+16t_5+64t_5^2 \equiv 17 \pmod{32}$, tj. $t_5 = 1+2t_6$. Sada za $k = 6$ tražimo x u obliku $x = \pm(9 + 16t_6)$, i nastavljamo postupak, te dobivamo rješenje u $\mathbb{Z}_2$. ♢

Definicija 2.1. *Za $\alpha, \beta \in \mathbb{Q}_p \setminus \{0\}$ definiramo* Hilbertov simbol $\left(\frac{\alpha,\beta}{p}\right)$ *tako da je $\left(\frac{\alpha,\beta}{p}\right) = 1$ ako jednadžba $\alpha x^2 + \beta y^2 - z^2 = 0$ ima rješenje u $\mathbb{Q}_p$, a $\left(\frac{\alpha,\beta}{p}\right) = -1$, inače.*

Definicija Hilbertovog simbola ima smisla i za $p = \infty$, tj. $\mathbb{Q}_p = \mathbb{R}$. Tada je $\left(\frac{\alpha,\beta}{\infty}\right) = 1$ ako je $\alpha > 0$ ili $\beta > 0$.

Pokazuje se da Hilbertovi simboli za različite p-ove nisu sasvim neovisni. Naime, za $a, b \in \mathbb{Q}$, vrijedi *produktna formula*

$$\prod_p \left(\frac{a, b}{p}\right) = 1. \tag{2.17}$$

Posebno, ako su svi faktori u formuli (2.17), osim možda jednog, jednaki 1, onda i taj preostali mora biti jednak 1. To znači da ako ternarna kvadratna forma f (netrivijalno) reprezentira 0 u svakom polju $\mathbb{Q}_p$ (p prost ili $p = \infty$) osim možda u jednom polju $\mathbb{Q}_q$, onda f reprezentira 0 i u $\mathbb{Q}_q$.

Ovo objašnjava zašto u našoj prvoj verziji Legendreovog teorema nije bilo nikakvog uvjeta na rješivost kongruencija modulo 2^k, tj. na rješivost u $\mathbb{Q}_2$. Da smo dodali takav uvjet, mogli smo recimo izbaciti uvjet na predznake koeficijenata, tj. na rješivost u $\mathbb{R}$.

Dokaz Teorema 2.5 za $n = 4$ Slično kao kod slučaja ternarnih kvadratnih formi, možemo pretpostaviti da je forma dijagonalna, te da su joj koeficijenti relativno prosti (štoviše, da nikoja tri nemaju zajednički faktor) i kvadratno slobodni. Dakle, promatramo formu

$$f(x_1.x_2, x_3, x_4) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2.$$

Zbog rješivosti u $\mathbb{R}$, brojevi a_1, a_2, a_3, a_4 nisu istog predznaka, pa smijemo prepostaviti da je $a_1 > 0$ i $a_4 < 0$. Neka je

$$g(x_1, x_2) = a_1x_1^2 + a_2x_2^2, \quad h(x_3, x_4) = -a_3x_3^2 - a_4x_4^2.$$

Želimo pokazati da postoji cijeli broj a koji se može (netrivijalno) reprezentirati i pomoću g i pomoću h.

Neka su $p_1, \ldots, p_s$ neparni prosti djelitelji od $a_1a_2a_3a_4$. Za prost broj $p \in \{2, p_1, \ldots, p_s\}$ postoji $b_p \in \mathbb{Z}_p$ koji je prikaziv u obliku

$$b_p = a_1y_1^2 + a_2y_2^2 = -a_3y_3^2 - a_4y_4^2, \quad y_i \in \mathbb{Z}_p,$$

i brojevi y_i nisu svi 0. Štoviše, možemo pretpostaviti da su svi različiti od 0. Zaista, kada bi npr. bilo $y_4 = 0$, onda za proizvoljni $y_4' \neq 0$ možemo naći t tako da za $y_1' = ty_1 + z_1$, $y_2' = ty_2 + z_2$, $y_3' = ty_3 + z_3$ vrijedi $a_1y_1'^2 + a_2y_2'^2 + a_3y_3'^2 + a_4y_4'^2 = 0$ (dobivamo linearnu jednadžbu u t; analogno se pokazuje opći rezultat da ako kvadratna forma reprezentira nulu, onda reprezentira i svaki drugi element iz pripadnog polja). Nadalje, možemo pretpostaviti da je $b_p \neq 0$, jer ako je $b_p = 0$, onda, kao što smo upravo rekli, g i h reprezentiraju sve elemente iz $\mathbb{Q}_p$.

Neka je $v_p(b_p) = \lambda_p$. Odaberimo prirodan broj a tako da vrijedi

$$a \equiv b_2 \pmod{2^{\lambda_2+3}}, \quad a \equiv b_p \pmod{p^{\lambda_p+1}}, \ p = p_1, \ldots, p_s. \tag{2.18}$$

Broj a je jedinstveno određen modulo $m = 2^{\lambda_2+3}p_1^{\lambda_{p_1}+1} \cdots p_s^{\lambda_{p_s}+1}$. Iz $b_p \not\equiv 0 \pmod{p^{\lambda_p+1}}$ slijedi da je $b_pa^{-1} \equiv 1 \pmod{p}$, pa je prema Lemi 2.4 b_pa^{-1} kvadrat u $\mathbb{Q}_p$. Slično je $b_pa^{-1} \equiv 1 \pmod{8}$, pa je b_pa^{-1} kvadrat u $\mathbb{Q}_2$. Dakle, dobili smo da jednadžbe

$$-ax_0^2 + a_1x_1^2 + a_2x_2^2 = 0 \quad \text{i} \quad -ax_0^2 - a_3x_3^2 - a_4x_4^2 = 0$$

imaju rješenje u $\mathbb{Q}_p$ za $p = 2, p_1, \ldots, p_s$. Zbog $a_1 > 0$, $a_4 < 0$, one imaju rješenja i u $\mathbb{R}$, a iz Chevalleyovog teorema i Henselove leme znamo da imaju rješenja u $\mathbb{Q}_p$ za $p \nmid 2aa_1a_2a_3a_4$. Dakle, ostaje još samo pitanje prostih brojeva p koji dijele a. No, vidjeli smo da jedan prost broj ne predstavlja problem, tj. da ako jednadžba ovakvog tipa (ternarna kvadratna forma) ima rješenja za svaki p prost ili $p = \infty$, osim eventualno jednog, onda ima rješenja za sve p. Zato želimo izabrati a tako da ima samo jedan prosti faktor različit od $2, p_1, \ldots, p_s$. To nam omogućava Dirichletov teorem o prostim brojevima u aritmetičkom nizu. Neka je a' bilo koji prirodan broj koji zadovoljava kongruencije (2.18), te neka je $d = (a', m)$. Tada su a'/d i m/d relativno prosti, pa postoji $k \in \mathbb{N}$ takav da je broj $\frac{a'}{d} + \frac{m}{d} \cdot k = q$ prost. Sada broj $a = qd = a' + km$ ima željeno svojstvo.

Dakle, možemo primijeniti Teorem 2.5 za $n = 3$. Zaključujemo da postoje $c_1, c_2, c_3, c_4 \in \mathbb{Q}$, takvi da vrijedi

$$a = a_1c_1^2 + a_2c_2^2, \quad a = -a_3c_3^2 - a_4c_4^2,$$

što je i trebalo dokazati. □

Dokaz Teorema 2.5 za $n \geq 5$ Dovoljno je promatrati forme

$$f(x_1, \ldots, x_n) = a_1 x_1^2 + \cdots a_n x_n^2,$$

gdje su a_i relativno prosti i kvadratno slobodni, te $a_1 > 0$, $a_n < 0$. Pretpostavimo da tvrdnja vrijedi da sve forme s manje od n varijabli. Označimo

$$g(x_1, x_2) = a_1 x_1^2 + a_2 x_2^2, \quad h(x_3, \ldots, x_n) = -a_3 x_3^2 - \cdots - a_n x_n^2.$$

Kao i u slučaju $n = 4$, pomoću Dirichletovog teorema, možemo naći prirodan broj a koji je reprezentiran sa g i sa h u $\mathbb{R}$ i $\mathbb{Q}_p$, s mogućim izuzetkom jednog prostog broja q koji ne dijeli koeficijente a_i. Tada iz svojstava ternarnih kvadratnih formi slijedi da g reprezentira a i u $\mathbb{Q}_q$. Budući da je $n - 2 \geq 3$, forma h reprezentira nulu u $\mathbb{Q}_q$ (Chevalleyov teorem i Henselova lema), pa reprezentira i broj a. Sada na forme $-ax_0^2 + g$ i $-ax_0^2 + h$ možemo primijeniti pretpostavku indukcije, pa zaključujemo da g i h reprezentiraju a u $\mathbb{Q}$. □

Napomena 2.1. Može se pokazati da za $n \geq 5$ svaka kvadratna forma f reprezentira nulu u svakom $\mathbb{Q}_p$ za p prost. Zato je za $n \geq 5$ dovoljan uvjet za rješivost jednadžbe $f(x_1, \ldots, x_n) = 0$ u $\mathbb{Q}$ taj da jednadžba ima rješenja u $\mathbb{R}$.

Poglavlje 3

Rezultati, metode i algoritmi iz diofantskih aproksimacija

3.1 Liouvilleov, Thueov i Rothov teorem

Definicija 3.1. Za kompleksan broj α kažemo da je *algebarski broj* ako postoji polinom $f(x)$ s racionalnim koeficijentima, različit od nulpolinoma, takav da je $f(\alpha) = 0$. Kompleksan broj se zove *transcendentan* ako nije algebarski.

Teorem 3.1. *Neka je α algebarski broj. Tada postoji jedinstveni ireducibilni normirani polinom $g(x)$ s racionalnim koeficijentima takav da je $g(\alpha) = 0$. Nadalje, svaki polinom nad $\mathbb{Q}$ kojeg α poništava djeljiv je sa $g(x)$.*

Dokaz: Neka je $G(x)$ polinom nad $\mathbb{Q}$ najmanjeg stupnja kojeg α poništava. Ako je vodeći koeficijent od $G(x)$ jednak c, definirajmo $g(x) = \frac{1}{c}G(x)$. Tada je $g(\alpha) = 0$ i g je normiran. Pokažimo da je g ireducibilan. U protivnom bi bilo $g(x) = h_1(x)h_2(x)$, pa bi imali $h_1(\alpha) = 0$ ili $h_2(\alpha) = 0$, protivno pretpostavci o minimalnosti stupnja od $G(x)$.

Neka je sada $f(x)$ bilo koji polinom nad $\mathbb{Q}$ sa svojstvom da je $f(\alpha) = 0$. Podijelimo polinom $f(x)$ sa $g(x)$. Dobivamo $f(x) = g(x)q(x) + r(x)$, gdje je $\deg r < \deg g$. No, $r(\alpha) = 0$, pa zbog minimalnosti stupnja od $G(x)$, mora biti $r(x)$ nulpolinom. Dakle, $f(x)$ je djeljiv s $g(x)$.

Konačno, pokažimo jedinstvenost od $g(x)$. Neka je $g_1(x)$ ireducibilan normiran polinom nad $\mathbb{Q}$ takav da je $g_1(\alpha) = 0$. Tada, prema upravo dokazanom, postoji polinom $q(x)$ takav da je $g_1(x) = g(x)q(x)$. No, ireducibilnost od $g_1(x)$ povlači da je $q(x)$ konstanta. U stvari, $q(x) = 1$, budući su $g(x)$ i $g_1(x)$ normirani. □

Definicija 3.2. *Minimalni polinom* algebarskog broja α je polinom $g(x)$ opisan u Teoremu 3.1. *Stupanj* algebarskog broja je stupanj njegovog minimalnog polinoma.

Definicija 3.3. Za algebarski broj α je kažemo da je *algebarski cijeli broj* ako je α korijen nekog normiranog polinoma s cjelobrojnim koeficijentima.

Iz Gaussove leme koja kaže da ako su $f(x) \in \mathbb{Z}[x]$, $g(x), h(x) \in \mathbb{Q}[x]$ normirani polinomi i $f(x) = g(x)h(x)$, onda je $g(x), h(x) \in \mathbb{Z}[x]$, slijedi da minimalni polinom algebarskog cijelog broja ima cjelobrojne koeficijente.

Teorem 3.2 (Liouville)**.** *Neka je α realan algebarski broj stupnja d. Tada postoji konstanta $c(\alpha) > 0$ tako da vrijedi*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$$

za sve racionalne brojeve $\frac{p}{q}$, gdje je $q > 0$ (to ćemo i nadalje pretpostavljati u svim nejednakostima ovakvog tipa) i $\frac{p}{q} \neq \alpha$.

Dokaz: Dokaz ćemo podijeliti u tri dijela, zbog kasnijih komentara o dokazu Rothovog teorema.

(a) Neka je $g(x)$ minimalni polinom od α. Odaberimo prirodan broj m tako da polinom $P(x) = m \cdot g(x)$ ima relativno proste cjelobrojne koeficijente.

(b) Možemo pretpostaviti da je $|\alpha - \frac{p}{q}| \leq 1$ (inače možemo staviti $c(\alpha) = 1$). Razvijemo li $P(x)$ u Taylorov red oko α, dobivamo:

$$\left|P(\frac{p}{q})\right| = \left|\sum_{i=1}^{d} \left(\frac{p}{q} - \alpha\right)^i \frac{1}{i!} P^{(i)}(\alpha)\right| < \frac{1}{c(\alpha)} \cdot \left|\alpha - \frac{p}{q}\right|, \tag{3.1}$$

gdje je $c(\alpha) = \frac{1}{2\sum_{i=1}^{d} \frac{1}{i!}|P^{(i)}(\alpha)|}$.

(c) Budući da je polinom $P(x)$ ireducibilan, to je $P(\frac{p}{q}) \neq 0$. Stoga je broj $q^d|P(\frac{p}{q})|$ prirodan, pa je $|P(\frac{p}{q})| \geq \frac{1}{q^d}$. Usporedimo li nejednakosti dobivene pod (b) i (c), dobivamo tvrdnju teorema.

□

Primjer 3.1. *Dokažimo da je broj $\alpha = \sum_{n=1}^{\infty} 2^{-n!}$ transcendentan.*

Rješenje: Zaista, ako stavimo $q(k) = 2^{k!}$, $p(k) = 2^{k!} \sum_{n=1}^{k} 2^{-n!}$, onda je

$$\begin{aligned}\left|\alpha - \frac{p(k)}{q(k)}\right| &= \sum_{n=k+1}^{\infty} 2^{-n!} < 2^{-(k+1)!} + 2^{-(k+1)!-1} + 2^{-(k+1)!-2} + \cdots \\ &= 2 \cdot 2^{-(k+1)!} = \frac{2}{(q(k))^{k+1}}.\end{aligned}$$

Odavde slijedi da za svaki prirodan broj d i svaki $c > 0$ postoji $k_0 \in \mathbb{N}$ takav da za sve $k \geq k_0$ vrijedi

$$\left|\alpha - \frac{p(k)}{q(k)}\right| < \frac{c}{(q(k))^d}.$$

Po Liouvilleovom teoremu, α ne može biti algebarski broj stupnja d za niti jedan d, pa je stoga α transcendentan. ♢

Neka je α realan algebarski broj stupnja $d \geq 2$. Liouvilleov teorem povlači da nejednadžba

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\mu} \tag{3.2}$$

ima samo konačno mnogo racionalnih rješenja $\frac{p}{q}$ ako je $\mu > d$.

Thue [1909] je dokazao da nejednadžba (3.2) ima samo konačno mnogo rješenja ako je $\mu > \frac{1}{2}d + 1$, Siegel [1921] je dokazao da ista tvrdnja vrijedi ako je $\mu > 2\sqrt{d}$, dok su Dyson [1947] i Geljfond [1948] dokazali tvdnju za $\mu > \sqrt{2d}$. Konačno, Roth [1955] je dokazao da nejednadžba (3.2) ima samo konačno mnogo rješenja ako je $\mu > 2$. Za taj rezultat Klaus Roth je 1958. godine nagrađen Fieldsovom medaljom.

Teorem 3.3 (Roth)**.** *Neka je α realan algebarski broj stupnja $d \geq 2$. Tada za svaki $\delta > 0$, nejednadžba*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}} \tag{3.3}$$

ima samo konačno mnogo rješenja u racionalnim brojevima $\frac{p}{q}$.

Napomena 3.1.

(i) Tvrdnja Teorema 3.3 je istinita i trivijalna za $\alpha \in \mathbb{C} \setminus \mathbb{R}$,

(ii) Ako je α algebarski cijeli broj stupnja d koji zadovoljava jednadžbu $a_d\alpha^d + \cdots + a_0 = 0$ s cjelobrojnim koeficijentima, onda je $\beta = a_d\alpha$ algebarski cijeli broj stupnja d. Pretpostavimo da nejednadžba $|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\delta}}$ ima beskonačno mnogo rješenja. Tada i nejednadžba $|\beta - \frac{a_d p}{q}| < \frac{1}{q^{2+\delta/2}}$ ima beskonačno mnogo rješenja. Stoga je dovoljno tvrdnju Rothovog teorema dokazati za algebarske cijele brojeve.

(iii) Po Dirichletovom teoremu, eksponent 2 u (3.3) je najbolji mogući. Ako je stupanj od α jednak 2, onda je $|\alpha - \frac{p}{q}| > \frac{c(\alpha)}{q^2}$ po Liouvilleovom teoremu, što povlači tvrdnju Rothovog teorema u ovom slučaju.

(iv) Za niti jedan algebarski broj α stupnja ≥ 3 nije poznat odgovor na pitanje vrijedi li $|\alpha - \frac{p}{q}| > \frac{c(\alpha)}{q^2}$ (za takve brojeve se kaže da su *slabo aproksimabilni*; oni imaju ograničene parcijalne kvocijente u razvoju u verižni razlomak).

Ideja dokaza Rothovog teorema je da pokušamo modificirati korake (a), (b) i (c) u dokazu Liouvilleovog teorema.

Jedna potencijalna modifikacija bi bila da u koraku (a) uzmemo polinom $P(x) \in \mathbb{Z}[x]$ takav da je $\deg P = r$ i da je α korijen od P kratnosti i. U koraku (b) pretpostavimo da vrijedi $|\alpha - \frac{p}{q}| < \frac{1}{q^{\mu}}$, pa Taylorov razvoj

$$P(\frac{p}{q}) = \sum_{j=i}^{r} \left(\frac{p}{q} - \alpha\right)^j \frac{1}{j!} P^{(j)}(\alpha)$$

daje $|P(\frac{p}{q})| \leq c \cdot q^{-\mu i}$. Konačno, u koraku (c), iz $P(\frac{p}{q}) \neq 0$ slijedi $|P(\frac{p}{q})| \geq q^{-r}$, pa ova nejednakost vrijedi za sve osim konačno mnogo racionalnih brojeva $\frac{p}{q}$. Dakle, ako (3.2) ima beskonačno mnogo rješenja, onda je $\mu i \leq r$, tj. $\mu \leq \frac{r}{i}$. Zato bi trebalo pokušati broj $\frac{r}{i}$ učiniti što manjim. Međutim, očito je uvijek $\frac{r}{i} \geq d$ i jednakost $\frac{r}{i} = d$ vrijedi ako je $P(x)$ potencija minimalnog polinoma od α. Prema tome, najbolje što na ovaj način možemo dobiti je $\mu \leq d$, tj. ništa bolje od Liouvilleovog teorema.

U svom poboljšanju Liouvilleovog teorema Thue je koristio polinom u dvije varijable oblika $x_2 Q(x_1) - P(x_1)$. Siegel je koristio općenitiji polinom $P(x_1, x_2)$ u dvije varijable, dok je Roth koristio polinom $P(x_1, \ldots, x_m)$ u više varijabli.

Glavna poteškoća u ovakvom pristupu nastupa u koraku (c). Naime, skup rješenja jednadžbe $P(x_1, \cdots, x_m) = 0$ je neka algebarska mnogostrukost u $\mathbb{R}^m$ i jako je teško pokazati da je $P(\frac{p}{q}, \ldots, \frac{p}{q}) \neq 0$. Ta se poteškoća pokušava riješiti korištenjem m-torki $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$ različitih racionalnih aproksimacija i pokušava se dokazati da je $P(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}) \neq 0$. Pokazuje se da nazivnici $q_1 < q_2 < \cdots < q_m$ moraju brzo rasti. Na primjer, u slučaju $m = 2$, trebaju nam dvije dobre aproksimacije $\frac{p_1}{q_1}, \frac{p_2}{q_2}$ od α takve da je q_2 puno veći od q_1. To je razlog zbog čega jedna dobra aproksimacija ne daje nikakvu kontradikciju, te je Rothov teorem, kao i sva ostala poboljšanja Liouvilleovog teorema dobivena ovom metodom, "neefektivan", u smislu da ne daje nikakvu ogradu za veličinu nazivnika u dobrim aproksimacijama.

Feljdman [1971] je koristeći Bakerovu metodu linearnih formi u logaritmima algebarskih brojeva dokazao "efektivno" poboljšanje Liouvilleovog teorema, tj. rezultat tipa

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^{d - c_1(\alpha)}},$$

gdje su $c(\alpha) > 0$ i $c_1(\alpha) > 0$ eksplicitne konstante. No, konstanta $c_1(\alpha)$ dobivena na ovaj način je obično vrlo mala, tako da je eksponent $d - c_1(\alpha)$ veći od eksponenta $\frac{1}{2}d + 1$ iz Thueovog teorema.

Neka je

$$F(x, y) = a_0 x^n + a_1 x^{n-1} y + \cdots + a_n y^n$$

binarna forma s cjelobrojnim koeficijentima, ireducibilna nad $\mathbb{Q}$, stupnja $n \geq 3$. Primijetimo da forma F ne može biti ireducibilna nad $\mathbb{C}$. Naime,

$$F(x,1) = a_0(x-\theta_1)\cdots(x-\theta_n),$$

gdje su $\theta_1, \ldots, \theta_n$ algebarski brojevi stupnja n, pa je

$$F(x,y) = y^n F(\frac{x}{y},1) = a_0(x-\theta_1 y)\cdots(x-\theta_n y).$$

No, ireducibilnost nad $\mathbb{Q}$ povlači da $F(x,1)$ nema višestrukih korijena, tj. da su θ_i-ovi međusobno različiti.

Neka je $m \neq 0$ cijeli broj. Diofantsku jednadžbu oblika $F(x,y) = m$ zovemo *Thueova jednadžba*. Godine 1909. Thue je dokazao da takva jednadžba ima samo konačno mnogo rješenja, koristeći svoj, ranije spomenuti, rezultat iz diofantskih aproksimacija. Dokažimo najprije jednostavan specijalni slučaj tog rezultata.

Teorem 3.4. *Ako jednadžba $F(x,1) = 0$ nema realnih rješenja, tada jednadžba $F(x,y) = m$ ima samo konačno mnogo rješenja. Preciznije, sva rješenja zadovoljavaju nejednakost*

$$|y| \leq \frac{|m|}{\min_{1\leq i\leq n} |Im\,(\theta_i)|},$$

gdje smo sa θ_i označili korijene polinoma $F(x,1)$.

Dokaz: Pretpostavimo da je (x,y) rješenje jednadžbe $f(x,y) = m$ i uzmimo θ_k tako da je $|x-\theta_k y| = \min_{1\leq i\leq n} |x-\theta_i y|$. Tada je jasno da vrijedi $|y| \cdot |\mathrm{Im}\,(\theta_k)| = |\mathrm{Im}\,(\theta_k y)| \leq |x-\theta_k y| \leq |m|$, pa dobivamo tvrdnju teorema. □

Teorem 3.5 (Thue)**.** *Thueova jednadžba ima samo konačno mnogo cjelobrojnih rješenja.*

Dokaz: Neka je $F(x,y) = m$. Uz gore uvedene oznake, možemo pisati

$$a_0(x-\theta_1 y)\cdots(x-\theta_n y) = m. \tag{3.4}$$

Možemo pretpostaviti da je $y \neq 0$, jer za $y = 0$ imamo najviše dva rješenja. Podijelimo (3.4) sa y^n i uzmimo apsolutne vrijednosti, pa dobivamo

$$|a_0| \cdot \left|\theta_1 - \frac{x}{y}\right| \cdots \left|\theta_n - \frac{x}{y}\right| = \left|\frac{m}{y^n}\right|. \tag{3.5}$$

Kao i u dokazu prethodnog teorema, uzmimo θ_k tako da je

$$|x-\theta_k y| = \min_{1\leq i\leq n} |x-\theta_i y|,$$

tj.

$$\left|\theta_k - \frac{x}{y}\right| = \min_{1\le i\le n}\left|\theta_i - \frac{x}{y}\right|.$$

Neka je $\gamma = \frac{1}{2}\min_{i\neq j}|\theta_i - \theta_j| > 0$. Za y dovoljno velik, obje strane od (3.5) se mogu učiniti po volji male. Posebno to onda vrijedi i za najmanji faktor na lijevoj strani, tj. $|\theta_k - \frac{x}{y}|$. Dakle, postoji $y_0 > 0$ tako da za $y \ge y_0$ vrijedi $|\theta_k - \frac{x}{y}| < \gamma$. Za $i \neq k$ imamo:

$$|\theta_i - \frac{x}{y}| \ge |\theta_i - \theta_k| - |\theta_k - \frac{x}{y}| \ge 2\gamma - \gamma = \gamma.$$

Stoga iz (3.5) slijedi

$$\left|\theta_k - \frac{x}{y}\right| \le \left|\frac{m}{a_0 y^n \gamma^{n-1}}\right| = \frac{c}{|y|^d}. \tag{3.6}$$

Budući da je $n \ge 3$, Rothov teorem (u stvari već i Thueov, ali ne i Liouvilleov) povlači da nejednadžba (3.6) ima samo konačno mnogo rješenja, što je i trebalo dokazati. □

Napomena 3.2. Iz teorije linearnih diofantskih jednadžbi i Pellovih jednadžbi znamo da tvrdnja Teorema 3.5 ne vrijedi ako je stupanj $n = 1$ ili $n = 2$. S druge strane, tvrdnja Teorema 3.5 vrijedi ukoliko se pretpostavka da je polinom ireducibilan nad $\mathbb{Q}$ zamijeni s pretpostavkom da polinom $F(x, 1)$ ima barem tri različita (kompleksna) korijena.

Zaista, pretpostavimo da je polinom $F(x, y)$ reducibilan nad $\mathbb{Q}$. Ako F ima barem dva različita ireducibilna faktora F_1 i F_2, onda dobivamo konačno mnogo sustava diofantskih jednadžbi $F_1(x, y) = m_1$, $F_2(x, y) = m_2$. Svaki od tih sustava ima konačno mnogo (kompleksnih) rješenja (po Bezoutovom teoremu broj rješenja nije veći od produkta stupnjeva od F_1 i F_2). Ostaje razmotriti slučaj $F(x, y) = aG(x, y)^k$, gdje je polinom G ireducibilan nad $\mathbb{Q}$. Ako je $\deg G \ge 3$, onda iz Teorema 3.5 slijedi da jednadžba $F(x, y) = 0$ ima konačno mnogo rješenja. Dakle, jedini slučajevi kada jednadžba $F(x, y) = 0$, gdje je F binarna forma, može imati beskonačno mnogo rješenja su jednadžbe oblika

$$F(x, y) = a(bx + cy)^n \quad \text{ili} \quad F(x, y) = a(bx^2 + cxy + dy^2)^{n/2},$$

a to su upravo slučajevi kada $F(x, 1)$ ima manje od tri različita korijena.

Primjer 3.2. *Naći sva cjelobrojna rješenja jednadžbe*

$$x^5 - x^4y - 4x^3y^2 + 2x^2y^3 + 4xy^4 + y^5 = 1.$$

Rješenje: Vrijedi

$$x^5 - x^4y - 4x^3y^2 + 2x^2y^3 + 4xy^4 + y^5 = (x^3 - 3xy^2 - y^3)(x^2 - xy - y^2),$$

pa se rješavanje dane jednadžbe svodi na rješavanje dvaju sustava diofantskih jednadžbi

$$x^3 - 3xy^2 - y^3 = 1, \qquad x^2 - xy - y^2 = 1; \tag{3.7}$$
$$x^3 - 3xy^2 - y^3 = -1, \qquad x^2 - xy - y^2 = -1. \tag{3.8}$$

Jedan od načina za rješavanje sustava polinomijalnih jednadžbi je pomoću tzv. *rezultante* polinoma. Rezultanta polinoma $f(X) = a_0X^l + \cdots + a_l$ i $g(X) = b_0X^m + \cdots + b_m$ nad poljem k, u oznaci $\mathrm{Res}(f, g)$ ili $\mathrm{Res}(f, g, X)$, je $(l + m) \times (l + m)$ determinanta

$$\begin{vmatrix}
a_0 & & & & b_0 & & & \\
a_1 & a_0 & & & b_1 & b_0 & & \\
a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\
\vdots & a_2 & \ddots & a_0 & \vdots & b_2 & \ddots & b_0 \\
a_l & \vdots & \ddots & a_1 & b_m & \vdots & \ddots & b_1 \\
 & a_l & & a_2 & & b_m & & b_2 \\
 & & \ddots & \vdots & & & \ddots & \vdots \\
 & & & a_l & & & & b_m
\end{vmatrix}$$

(na praznim mjestima su nule). Važna svojstva rezultante su:

- $\mathrm{Res}(f, g) = 0$ ako i samo ako f i g imaju zajednički faktor u $k[X]$;
- postoje polinomi A i B iz $k[X]$ takvi da vrijedi $Af + Bg = \mathrm{Res}(f, g)$.

Ako su $f, g \in k[x, y]$, onda ovo posljednje svojstvo povlači da za svako rješenje sustava $f(x, y) = 0, g(x, y) = 0$ vrijedi $\mathrm{Res}(f, g, x) = 0$ i $\mathrm{Res}(f, g, y) = 0$. U slučaju sustava (3.7), dobivamo jednadžbu

$$\mathrm{Res}(x^3 - 3xy^2 - y^3 - 1, x^2 - xy - y^2 - 1, x) = \begin{vmatrix}
1 & 0 & 1 & 0 & 0 \\
0 & 1 & -y & 1 & 0 \\
-3y^2 & 0 & -y^2 - 1 & -y & 1 \\
-y^3 - 1 & -3y^2 & 0 & -y^2 - 1 & -y \\
0 & -y^3 - 1 & 0 & 0 & -y^2 - 1
\end{vmatrix} = -y^6 + y^3 + 3y^2 - 3y = 0,$$

čija su jedina cjelobrojna rješenja $y = 0$ i $y = 1$. Za sustav (3.8), dobivamo jednadžbu

$$\mathrm{Res}(x^3 - 3xy^2 - y^3 + 1, x^2 - xy - y^2 + 1, x) = -y^6 - y^3 + 3y^2 - 3y + 2 = 0,$$

čije je jedino cjelobrojno rješenje $y = 1$. Sada se lako provjeri da su sva rješenja polazne jednadžbe $(x, y) = (1, 0), (2, 1)$ i $(0, 1)$. ♢

3.2 Hipergeometrijska metoda

Neka je α algebarski broj stupnja $d \geq 2$, te $\kappa > 2$. Tada Rothov teorem povlači da postoji konstanta $c = c(\alpha, \kappa) > 0$ takva da je

$$|\alpha - \frac{p}{q}| > \frac{c}{q^\kappa} \tag{3.9}$$

za sve racionalne brojeve $\frac{p}{q}$, $q > 0$. Međutim, dokaz Rothovog teorema ne daje metodu za eksplicitno određivanje konstante c. U ovom poglavlju ćemo dokazati nejednakost (3.9) s eksplicitnom vrijednošću od c i $\kappa < d$, za jednu klasu algebarskih brojeva. Tako ćemo dobiti "efektivno" poboljšanje Liouvilleovog teorema.

Za $n \in \mathbb{N}$ neka je

$$\mu_n = \prod_{p|n} p^{1/(p-1)}.$$

Tada je $1 \leq \mu_n \leq n$.

Teorem 3.6 (Baker [1964])**.** *Neka su m, n prirodni brojevi takvi da vrijedi $n \geq 3$ i $1 \leq m < n$. Neka su a, b prirodni brojevi za koje je $\frac{7}{8}a \leq b < a$ i pretpostavimo da je $a \equiv b \pmod{n}$. Pretpostavimo, nadalje, da je*

$$\lambda = 4b(a-b)^{-2}\mu_n^{-1} > 1. \tag{3.10}$$

Tada $\alpha = \left(\frac{a}{b}\right)^{m/n}$ zadovoljava (3.9) za sve $p \in \mathbb{Z}$, $q \in \mathbb{N}$, gdje su κ i c dani sa

$$\lambda^{\kappa-1} = 2\mu_n(a+b), \tag{3.11}$$
$$c^{-1} = 2^{\kappa+2}(a+b). \tag{3.12}$$

Napomena 3.3. Uvjet $a \equiv b \pmod{n}$ se može uvijek zadovoljiti množeći, ako je nužno, a i b sa n. To, međutim, povećava vrijednosti od κ i c^{-1}, definirane s (3.11) i (3.12).

Rezultat Teorema 3.6 je zanimljiv (u svijetlu Liouvilleovog teorema) samo ako je $\kappa \leq n$, tj. ako je $\lambda^{n-1} \geq 2\mu_n(a+b)$.

Korolar 3.1. *Za sve racionalne brojeve $\frac{p}{q}$, $q > 0$, vrijedi*

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1.36 \cdot 10^{-6}}{q^{2.954}}.$$

Dokaz: Stavimo u Teorem 3.6 $n = 3$, $m = 1$, $a = 128$, $b = 125$, tako da je $(\frac{a}{b})^{m/n} = \frac{4}{5}\sqrt[3]{2}$. Tada je $\mu_3 = \sqrt{3}$ i $\lambda = \frac{500}{9\sqrt{3}} > 1$. Dobivamo: $\kappa \approx 2.95377$, $c \approx 0.0001275$, pa Teorem 3.6 povlači da za sve $p \in \mathbb{Z}$, $q \in \mathbb{N}$ vrijedi

$$\left|\frac{4}{5}\sqrt[3]{2} - \frac{4p}{5q}\right| > \frac{0.000127}{(5q)^{2.954}},$$

odnosno

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1.36 \cdot 10^{-6}}{q^{2.954}}\,.$$

□

Sa $F\left(\begin{matrix}\alpha\,,\,\beta\\ \gamma\end{matrix}\Big|x\right)$ označavat ćemo hipergeometrijsku funkciju definiranu sa

$$F\left(\begin{matrix}\alpha\,,\,\beta\\ \gamma\end{matrix}\Big|x\right) = \sum_{k\geq 0}\frac{\alpha^{\overline{k}}\beta^{\overline{k}}}{\gamma^{\overline{k}}}\cdot\frac{x^k}{k!} = \sum_{k\geq 0}\left(\prod_{j=0}^{k-1}\frac{(\alpha+j)(\beta+j)}{(\gamma+j)(1+j)}\right)x^k.$$

Ona zadovoljava diferencijalnu jednadžbu

$$x(x-1)F'' + ((1+\alpha+\beta)x-\gamma)F' + \alpha\beta F = 0.$$

Ako su β i γ negativni brojevi i $\beta > \gamma$, podrazumijevamo da su koeficijenti uz x^k za $k \geq 1-\gamma$ jednaki 0.

Lema 3.1. *Neka su m, n prirodni brojevi takvi da je $1 \leq m < n$ i neka je $\nu = \frac{m}{n}$. Za $r \in \mathbb{N}$ stavimo*

$$A_r(x) = F\left(\begin{matrix}-\nu-r\,,\,-r\\ -2r\end{matrix}\Big|x\right), \quad B_r(x) = F\left(\begin{matrix}\nu-r\,,\,-r\\ -2r\end{matrix}\Big|x\right),$$

$$E_r(x) = \frac{F\left(\begin{matrix}-\nu+r+1\,,\,r+1\\ 2r+2\end{matrix}\Big|x\right)}{F\left(\begin{matrix}-\nu+r+1\,,\,r+1\\ 2r+2\end{matrix}\Big|1\right)}.$$

Tada za svaki x, takav da je $0 < x < 1$, vrijedi

$$A_r(x) - (1-x)^\nu B_r(x) = x^{2r+1}A_r(1)E_r(x). \tag{3.13}$$

Dokaz: Neka je

$$f_1^{(r)}(x) = x^{2r+1}F\left(\begin{matrix}-\nu+r+1\,,\,r+1\\ 2r+2\end{matrix}\Big|x\right), \;\; f_2^{(r)}(x) = (1-x)^\nu B_r(x). \tag{3.14}$$

Tada funkcije $f_1^{(r)}$ i $f_2^{(r)}$ zadovoljavaju diferencijalnu jednadžbu za $A_r(x)$. Provjerimo to za funkciju $f_1^{(r)}$, koju ćemo kraće označiti sa f_1. Imamo:

$$\begin{aligned} f_1' &= (2r+1)x^{2r}F + x^{2r+1}F', \\ f_1'' &= 2r(2r+1)x^{2r-1}F + 2(2r+1)x^{2r}F' + x^{2r+1}F'', \end{aligned}$$

pa je

$$\begin{aligned} x(x-1)f_1'' + ((1-\nu-2r)x+2r)f_1' + r(\nu+r)f_1 = \\ x(x-1)x^{2r+1}F'' + x^{2r+1}((1-\nu+r+1+r+1)x-2r-2)F' \\ + x^{2r+1}(r+1)(1-\nu+r)F = 0. \end{aligned}$$

Funkcije $f_1^{(r)}$ i $f_2^{(r)}$ su linearno nezavisne budući da je

$$f_1^{(r)}(0) = 0, \quad f_2^{(r)}(0) = 1. \tag{3.15}$$

Prema tome, postoje realni brojevi u_1, u_2 takvi da je

$$A_r(x) = u_1 f_1^{(r)}(x) + u_2 f_2^{(r)}(x). \tag{3.16}$$

Budući da je $A_r(0) = 1$, iz (3.15) dobivamo da je $u_2 = 1$, a iz (3.14) i (3.16) dobivamo

$$A_r(1) = u_1 f_1^{(r)}(1) = u_1 F\left(\begin{matrix}-\nu + r + 1\,,\ r + 1 \\ 2r + 2\end{matrix}\Big|1\right).$$

Uvrstimo li sada vrijednosti dobivene za u_1 i u_2 u (3.16), dobivamo (3.13). □

Lema 3.2. *Neka vrijede pretpostavke Leme 3.1. Tada za svaki x, takav da je $0 < x < 1$, vrijedi*

$$A_r(x)B_{r+1}(x) - A_{r+1}(x)B_r(x) = x^{2r+1}A_r(1)E_r(0), \tag{3.17}$$

$$A_r(x) = A_r(1)F\left(\begin{matrix}-\nu - r\,,\ -r \\ 1 - \nu\end{matrix}\Big|1 - x\right), \tag{3.18}$$

gdje je

$$A_r(1) = \frac{(r!)^2}{(2r)!}\prod_{j=1}^{r}\left(1 - \frac{\nu}{j}\right), \tag{3.19}$$

$$E_r(0) = \frac{(r!)^2}{(2r+1)!}\nu\prod_{j=1}^{r}\left(1 + \frac{\nu}{j}\right). \tag{3.20}$$

Dokaz: Iz Leme 3.1, za r i $r + 1$, imamo:

$$A_r(x)B_{r+1}(x) - A_{r+1}(x)B_r(x) = \\ x^{2r+1}(A_r(1)B_{r+1}(x)E_r(x) - x^2 A_{r+1}(x)B_r(x)E_{r+1}(x)).$$

Lijeva strana ove jednakosti predstavlja polinom u x stupnja najviše $2r + 1$, dok na desnoj strani imamo red potencija u x čiji je početni član jednak $x^{2r+1}A_r(1)E_r(0)$. Time je dokazano (3.17).

Po definiciji su $A_r(x)$ i $B_r(x)$ polinomi. Polinom $F\left(\begin{matrix}-\nu - r\,,\ -r \\ 1 - \nu\end{matrix}\Big|1 - x\right)$ također zadovoljava diferencijalnu jednadžbu za $A_r(x)$, pa je stoga linearno zavisan sa $A_r(x)$ i $(1-x)^\nu B_r(x)$. Međutim, ako on ne bi bio linearno zavisan sa $A_r(x)$, onda bi $(1 - x)^\nu$ mogli prikazati kao kvocijent dva polinoma, tj. racionalnu funkciju. Dobivena kontradikcija dokazuje relaciju (3.18).

U dokazu relacija (3.19) i (3.20) koristit ćemo tzv. Gaussovu formulu:

$$F\left(\begin{matrix}\alpha\,,\,\beta\\ \gamma\end{matrix}\Big|1\right)=\frac{\Gamma(\gamma)\Gamma(\gamma-\alpha-\beta)}{\Gamma(\gamma-\alpha)\Gamma(\gamma-\beta)}\,, \tag{3.21}$$

koja vrijedi uz pretpostavku da je $\operatorname{Re}\gamma>\operatorname{Re}\alpha+\operatorname{Re}\beta$ ili da je β nepozitivan cijeli broj. Stavimo $x=0$ u (3.18) i primijenimo (3.21). Dobivamo:

$$\begin{aligned}A_r(1)&=\frac{\Gamma(r+1)\Gamma(r+1-\nu)}{\Gamma(1-\nu)\Gamma(2r+1)}=\frac{r!(r-\nu)(r-\nu-1)\cdots(1-\nu)\Gamma(1-\nu)}{\Gamma(1-\nu)(2r)!}\\&=\frac{(r!)^2}{(2r)!}\prod_{j=1}^{r}(1-\frac{\nu}{j}).\end{aligned}$$

Slično, iz definicije od $E_r(x)$, dobivamo:

$$\begin{aligned}E_r(0)&=\frac{1}{F\left(\begin{matrix}-\nu+r+1\,,\,r+1\\ 2r+2\end{matrix}\Big|1\right)}=\frac{\Gamma(r+1-\nu)\Gamma(r+1)}{\Gamma(2r+2)\Gamma(\nu)}\\&=\frac{(r+\nu)(r+\nu-1)\cdots\nu\Gamma(\nu)r!}{(2r+1)!\Gamma(\nu)}=\frac{(r!)^2}{(2r+1)!}\nu\prod_{j=1}^{r}(1+\frac{\nu}{j}).\end{aligned}$$

□

Lema 3.3. *Neka vrijede pretpostavke Leme 3.1, te neka su a,b prirodni brojevi takvi da vrijedi $\frac{7}{8}a\le b<a$ i $a\equiv b \pmod n$. Za $r\in\mathbb{N}$ stavimo*

$$\begin{aligned}\sigma_r&=\prod_{p|n}p^{\lfloor r/p-1\rfloor},\\ p_r&=\binom{2r}{r}\sigma_r a^r B_r\left(1-\frac{b}{a}\right),\\ q_r&=\binom{2r}{r}\sigma_r a^r A_r\left(1-\frac{b}{a}\right).\end{aligned}$$

Tada su p_r,q_r prirodni brojevi i

$$q_r<2(2\mu_n(a+b))^r. \tag{3.22}$$

Dokaz: Po definiciji je

$$\begin{aligned}A_r(x)&=\sum_{k=0}^{r}\frac{r(r-1)\cdots(r-k+1)(r+\nu)(r+\nu-1)\cdots(r+\nu-k+1)}{(2r)(2r-1)\cdots(2r-k+1)k!}(-x)^k\\&=\sum_{k=0}^{r}l_r^{(k)}n^{-k}\frac{(r)!}{(2r)!k!}\binom{2r-k}{r}(-x)^k,\end{aligned}$$

gdje je $l_r^{(k)} = \prod_{j=r-k+1}^{r} (jn+m)$.

Ako je p prost broj koji ne dijeli n, onda je za svaki prirodan broj i, točno $\left\lfloor \frac{k}{p^i} \right\rfloor$ od brojeva $1, 2, \ldots, k$, te barem $\left\lfloor \frac{k}{p^i} \right\rfloor$ od k faktora u $l_r^{(k)}$, djeljivo s p^i. Prema tome, najveća potencija od p koja dijeli $k!$, a to je $\sum_{i=1}^{\infty} \left\lfloor \frac{k}{p^i} \right\rfloor$, nije veća od najveće potencije od p koja dijeli $l_r^{(k)}$.

Ako sada prost broj p dijeli n, onda je najveća potencija od p koja dijeli $r!$ manja li jednaka

$$\sum_{i=1}^{\infty} \left\lfloor \frac{r}{p^i} \right\rfloor \leq \left\lfloor \frac{r}{p-1} \right\rfloor .$$

Zaključujemo da su svi koeficijenti od $\binom{2r}{r}\sigma_r A_r(nx)$ cijeli brojevi, a isti zaključak vrijedi i za $\binom{2r}{r}\sigma_r B_r(nx)$. Sada uvjet da n dijeli $a-b$ povlači da su p_r i q_r cijeli brojevi.

Iz Leme 3.2 slijedi

$$q_r = \sigma_r n^{-r} \frac{1}{r!} \sum_{k=0}^{r} \Big(\prod_{j=k+1}^{r} (jn-m) \Big) l_r^{(k)} \binom{r}{k} a^{r-k} b^k .$$

Odavde je očito $q_r > 0$, a slično se vidi i da je $p_r > 0$.

Konačno, koristeći ocjene

$$\begin{aligned} l_r^{(k)} \prod_{j=k+1}^{r} (jn-m) &\leq n^r \prod_{j=r-k+1}^{r} (j+1) \prod_{j=k+1}^{r} j = n^r (r+1)^{\underline{k}} \cdot \frac{r!}{k!} = r! n^r \binom{r+1}{k} \\ &\leq r! n^r 2^{r+1} \end{aligned}$$

i $\sigma_r \leq \mu_n^r$, dobivamo

$$q_r < \mu_n^r \sum_{k=0}^{r} \binom{r}{r} 2^{r+1} a^{r-k} b^k = 2(2\mu_n(a+b))^r .$$

□

Lema 3.4. *Neka vrijede pretpostavke Leme 3.3. Tada za svaki $r \in \mathbb{N}$ vrijedi*

$$0 < \left(\frac{a}{b}\right)^{\nu} - \frac{p_r}{q_r} < \frac{3(a+b)}{4bq_r\lambda^r} , \tag{3.23}$$

gdje je λ definiran s (3.10), te

$$p_r q_{r+1} \neq p_{r+1} q_r .$$

Dokaz: Uvedimo oznaku $u = \frac{a-b}{b}$. Iz Leme 3.1, za $x = u$, dobivamo

$$\left(\frac{a}{b}\right)^{\nu} - \frac{p_r}{q_r} = \left(\frac{a}{b}\right)^{\nu} u^{2r+1} t_r, \tag{3.24}$$

gdje je

$$t_r = \frac{A_r(1)E_r(u)}{A_r(u)}\,. \tag{3.25}$$

Budući da $E_r(u)$ predstavlja red s pozitivnim članovima, ovo očito povlači lijevu nejednakost u (3.23).

Da bi dokazali desnu nejednakost u (3.23), najprije ćemo naći jednu gornju ogradu za $E_r(u)$. Neka je $s = \lfloor \frac{r}{2} \rfloor$,

$$w_r^{(k)} = \binom{r+k}{k}^2 \binom{2r+k+1}{k}^{-1}, \quad k = 0, 1, 2, \dots\,,$$

$$U_r = \sum_{k=0}^{s} w_r^{(k)} u^k, \quad V_r = \sum_{k=s+1}^{\infty} w_r^{(k)} u^k.$$

Tada je $F\left(\begin{matrix}-\nu+r+1\,,\, r+1 \\ 2r+2\end{matrix}\Big| u\right) \le U_r + V_r$, jer je

$$\frac{(-\nu+r+1)^{\overline{k}}(r+1)^{\overline{k}}}{(2r+2)^{\overline{k}}k!} \le \frac{(r+k)^{\underline{k}}(r+k)^{\underline{k}}}{k!(2r+k+1)^{\underline{k}}} = \binom{r+k}{k}^2 \binom{2r+k+1}{k}^{-1}.$$

Za svaki k je očito $w_r^{(k)} \le \binom{r+k}{k} \le 2^{r+k}$, pa zbog $u = \frac{a-b}{b} \le \frac{1}{8}$, dobivamo

$$V_r \le \sum_{k=s+1}^{\infty} 2^{r+k} u^k \le \sum_{k=s+1}^{\infty} 2^{r-2k} \le 2 \sum_{k=1}^{\infty} 2^{-2k} = \frac{2}{3}.$$

Sada ćemo iskoristiti nejednakost

$$(r+1+j)^2 < r(2r+2+j),$$

koja je ekvivalentna s $r^2 > rj + (j+1)^2$, pa vrijedi za $0 \le j \le s$ i $r \ge 5$. Imamo:

$$w_r^{(k)} = \frac{1}{k!} \prod_{j=0}^{k-1} \frac{(r+1+j)^2}{2r+2+j} \le \frac{r^k}{k!}$$

za sve $k \le s$ i $r \ge 5$. Prema tome,

$$U_r \le \sum_{k=0}^{s} \frac{r^k}{k!} u^k < e^{ur} < (1-u)^{-r} = \left(\frac{a}{b}\right)^r$$

ako je $r \ge 5$. Lako se provjeri (koristeći da je $1 < \frac{a}{b} \le \frac{8}{7}$) da nejednakost $U_r < (\frac{a}{b})^r$ vrijedi i za $r = 1, 2, 3, 4$.

Kombinirajući ocjene za U_r i V_r, dobivamo:

$$E_r(u) = E_r(0)F\left(\begin{matrix}-\nu+r+1\,,\ r+1\\ 2r+2\end{matrix}\Big|u\right) < E_r(0)\left(\frac{2}{3}+\left(\frac{a}{b}\right)^r\right)$$
$$< \frac{5}{3}E_r(0)\left(\frac{a}{b}\right)^r. \tag{3.26}$$

Sada iz Leme 3.2, koristeći nejednakost

$$2^{2r} = \sum_{k=0}^{2r}\binom{2r}{k} < (2r+1)\binom{2r}{r},$$

dobivamo

$$E_r(0) < 2^{-2r}\nu\prod_{j=1}^{r}\left(1+\frac{\nu}{j}\right), \tag{3.27}$$

pa iz (3.26) i (3.27) dobivamo željenu gornju ogradu za $E_r(u)$.

Iz Lema 3.2 i 3.3 imamo:

$$\frac{A_r(1)}{A_r(u)} = \frac{\sigma_r a^r}{q_r}\prod_{j=1}^{r}\left(1-\frac{\nu}{j}\right) \le \frac{(\mu_n a)^r}{q_r}\prod_{j=1}^{r}\left(1-\frac{\nu}{j}\right).$$

Kombinirajući ovu nejednakost sa (3.24), (3.25) i (3.26), dobivamo

$$t_r < \frac{5\nu}{3q_r}\left(\frac{\mu_n a^2}{4b}\right)^r\prod_{j=1}^{r}\left(1-\frac{\nu^2}{j^2}\right) \le \frac{5\nu(1-\nu^2)}{3q_r}\left(\frac{\mu_n a^2}{4b}\right)^r. \tag{3.28}$$

Uočimo da za $0<\nu<1$ funkcija $f(\nu)=\nu(1-\nu^2)$ poprima maksimum za $\nu=\frac{1}{\sqrt{3}}$ i taj maksimum je $<\frac{9}{20}$. Budući da je $\lambda^{-1}=\mu_n(au)^2(4b)^{-1}$, iz (3.28) i (3.24) slijedi desna strana od (3.23).

Konačno, $p_rq_{r+1}\neq p_{r+1}q_r$ slijedi iz Leme 3.2 za $x=u$, imajući u vidu da je $A_r(1)\neq 0$, $E_r(0)\neq 0$. □

Dokaz Teorema 3.6: Leme 3.1 i 3.2 povlače da postoji niz parova prirodnih brojeva p_r, q_r takvih da vrijedi (3.22), (3.23) i (3.24).

Neka su $p\in\mathbb{Z}$, $q\in\mathbb{N}$ i pretpostavimo da je $q\ge\frac{1}{2}\lambda\mu_n$. Tada postoji $r\in\mathbb{N}$ takav da je

$$\lambda^r \le 2\mu_n^{-1}q < \lambda^{r+1}. \tag{3.29}$$

Odaberimo $\rho=r$ ili $\rho=r+1$ tako da bude $pq_\rho\neq qp_\rho$. Iz (3.11), (3.12), (3.22) i lijeve strane od (3.29) slijedi

$$q_\rho < 2\lambda^{(\kappa-1)(r+1)} \le 2(2\lambda\mu_n^{-1}q)^{\kappa-1} = (2c)^{-1}\mu_n^{2-\kappa}q^{\kappa-1}. \tag{3.30}$$

Iz (3.10), (3.23) i desne strane od (3.29) slijedi

$$\left|\alpha-\frac{p_\rho}{q_\rho}\right| < \frac{3(a-b)\lambda\mu_n}{8bqq_\rho} = \frac{3}{2(a-b)qq_\rho}.$$

Ako sada iskoristimo da je $a-b \geq n \geq 3$ i $\kappa > 2$, iz (3.30) dobivamo

$$\left|\alpha - \frac{p}{q}\right| \geq \left|\frac{p_\rho}{q_\rho} - \frac{p}{q}\right| - \left|\alpha - \frac{p_\rho}{q_\rho}\right| > \frac{1}{qq_\rho} - \frac{1}{2qq_\rho} > \frac{1}{2}(2c\mu_n^{\kappa-2})q^{-\kappa} > cq^{-\kappa}\,.$$

Prema tome, dokazali smo da vrijedi (3.9) ako je $q \geq \frac{1}{2}\lambda\mu_n$.

Neka su sada $p, q \in \mathbb{Z}$ i pretpostavimo da je $0 < q < \frac{1}{2}\lambda\mu_n$. Koristimo razvoj u Taylorov red funkcije $(1+x)^\nu$:

$$\alpha = \left(1 + \frac{a-b}{b}\right)^\nu = 1 + \nu\frac{a-b}{b} + S,$$

gdje je

$$S = \sum_{j=2}^{\infty}\binom{\nu}{j}\left(\frac{a-b}{b}\right)^j = \sum_{j=2}^{\infty}\frac{\prod_{i=0}^{j-1}(i-\nu)}{j!}\left(1-\frac{a}{b}\right)^j.$$

Nađimo gornju ogradu za $|S|$. Očito je za $j \geq 2$

$$\left|\frac{1}{j!}\prod_{i=2}^{j-1}(i-\nu)\right| \leq \frac{1}{j!}(j-1)! \leq \frac{1}{2},$$

te $\nu(1-\nu) \leq \frac{1}{4}$. Odavde, koristeći $\frac{7}{8}a \leq b$, dobivamo

$$|S| \leq \frac{1}{8}\sum_{j=2}^{\infty}\left(\frac{a}{b}-1\right)^j = \frac{1}{8}\frac{(a-b)^2}{b(2b-a)} \leq \frac{1}{6}\frac{(a-b)^2}{ab}\,.$$

Iz pretpostavke $q < 2b(a-b)^{-2}$, zaključujemo da je

$$|S| < \frac{1}{3aq}\,. \tag{3.31}$$

Primijetimo nadalje da je

$$1 + \frac{m(a-b)}{nb} \neq \frac{p}{q}\,. \tag{3.32}$$

Inače bi nb dijelilo $mq(a-b)$, a to je nemoguće jer je $m < n$ i $q(a-b) < b$. Budući da n dijeli $a-b$, (3.31) i (3.32) povlače

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{bq} - |S| > \frac{1}{bq} - \frac{1}{3aq} = \frac{3a-b}{3abq} > \frac{2}{3bq} > \frac{1}{q^\kappa 2^{\kappa+2}(a+b)} = \frac{c}{q^\kappa}\,,$$

pa smo dokazali da (3.9) vrijedi i u slučaju da je $q < \frac{1}{2}\lambda\mu_n$. □

Korolar 3.2. *Sva rješenja Thueove jednadžbe*

$$x^3 - 2y^3 = M$$

zadovoljavaju nejednakost $\max\{|x|,|y|\} < 10^{127}\cdot|M|^{22}$.

Dokaz: Iz dokaza Teorema 3.5 (preciznije, iz relacije (3.6)), imamo

$$\left|\sqrt[3]{2}-\frac{x}{y}\right| \leq \left|\frac{M}{1.18y^3}\right|.$$

Usporedimo li ovo s Korolarom 3.1, dobivamo da je

$$\frac{1.36\cdot 10^{-6}}{|y|^{2.954}} < \frac{|M|}{1.18|y|^3},$$

odakle je $|y| < (6.3\cdot 10^5\cdot |M|)^{21.8} < 10^{127}\cdot |M|^{22}$. □

Napomena 3.4. Easton [1986] je poboljšao rezultat iz Korolara 3.1 i dobio nejednakost

$$\left|\sqrt[3]{2}-\frac{p}{q}\right| > \frac{2.2\cdot 10^{-8}}{q^{2.795}}.$$

Najbolji poznati rezultat ovog tipa je Bennettov [1997]:

$$\left|\sqrt[3]{2}-\frac{p}{q}\right| > \frac{0.25}{q^{2.45}}.$$

Slični rezultati su dobiveni i za neke druge algebarske brojeve. Npr.

$$\left|\sqrt[5]{7}-\frac{p}{q}\right| > \frac{0.25}{q^{4.43}}, \qquad \left|\sqrt[17]{50}-\frac{p}{q}\right| > \frac{0.25}{q^{6.96}}.$$

Ove nejednakosti su dobivene korištenjem nekih funkcija, definiranih pomoću krivuljnih integrala, koje poopćuju hipergeometrijske funkcije.

3.3 Simultane diofantske aproksimacije

Vidjeli smo već da se mnogi važni problemi vezani uz diofantske jednadžbe mogu preformulirati u odgovarajuće probleme iz diofantskih aproksimacija. No, osim "običnih" aproksimacija, mogu se pojaviti i tzv. simultane diofantske aproksimacije, tj. problemi istovremene aproksimacije više realnih brojeva. Tipičan primjer je sustav Pellovih (ili pellovskih) jednadžbi. Npr. iz

$$x^2-2y^2=1, \quad z^2-3y^2=1$$

slijedi da je $\sqrt{2}\approx\frac{x}{y}$, $\sqrt{3}\approx\frac{z}{y}$ (preciznije $\left|\sqrt{2}-\frac{x}{y}\right| < \frac{1}{2y^2}$, $\left|\sqrt{3}-\frac{z}{y}\right| < \frac{1}{2y^2}$), pa vidimo da bi iracionalni brojevi $\sqrt{2}$ i $\sqrt{3}$ trebali imati jako dobre racionalne aproksimacije s istim nazivnikom. Postavlje se pitanje mogu li takve aproksimacije postojati, te posebno koji je "kritični eksponent" koji razdvaja aproksimacije kojih ima beskonačno mnogo, od onih kojih može postojati samo konačno mnogo.

Navest ćemo analogone glavnih rezultata iz "običnih" aproksimacija, tj. Dirichletovog i Rothovog teorema.

Teorem 3.7 (Dirichlet (1842))**.** *Neka su α_{ij} $(i = 1, \dots, n;\ j = 1, \dots, m)$ realni brojevi, te $Q > 1$ prirodan broj. Tada postoje cijeli brojevi $q_1, \dots, q_m$, $p_1, \dots, p_n$ takvi da je*

$$\begin{aligned} 1 \le \max\{|q_1|, \dots, |q_m|\} &< Q^{n/m}, \\ |\alpha_{i1}q_1 + \cdots + \alpha_{im}q_m - p_i| &\le \frac{1}{Q}, \quad i = 1, \dots, n. \end{aligned} \tag{3.33}$$

Dokaz: Promotrimo točke

$$(\{\alpha_{11}x_1 + \cdots + \alpha_{1m}x_m\}, \dots, \{\alpha_{n1}x_1 + \cdots + \alpha_{nm}x_m\}),$$

gdje su x_j, $j = 1 \dots, m$, cijeli brojevi koji zadovoljavaju uvjet $0 \le x_j < Q^{n/m}$. Postoji barem Q^n takvih točaka i svaka od njih leži u zatvorenoj jediničnoj kocki $I^n = \{(t_1, \dots, t_n) : 0 \le t_k \le 1,\ k = 1, \dots, n\}$. Također je i $(1, 1, \dots, 1) \in I^n$, pa zajedno s ovom točkom promatramo barem $Q^n + 1$ točaka iz I^n.

Podijelimo I^n na Q^n u parovima disjunktnih potkocaka čiji su bridovi duljine $\frac{1}{Q}$. (Dakle, potkocke sadrže neke od svojih strana ili bridova, a neke ne.) Po Dirichletovom principu, dvije od promatranih točaka nalaze se u istoj potkocki. Recimo da su to točke

$$(\alpha_{11}x_1 + \cdots + \alpha_{1m}x_m - y_1, \dots, \alpha_{n1}x_1 + \cdots + \alpha_{nm}x_m - y_n),$$

$$(\alpha_{11}x'_1 + \cdots + \alpha_{1m}x'_m - y'_1, \dots, \alpha_{n1}x'_1 + \cdots + \alpha_{nm}x'_m - y'_n).$$

Ovdje je $(x_1, \dots, x_m) \ne (x'_1, \dots, x'_m)$. Stavimo $q_j = x_j - x'_j$ za $j = 1, \dots, m$, te $p_i = y_i - y'_i$ za $i = 1, \dots, n$. Tada je (3.33) očito zadovoljeno. □

Korolar 3.3. *Neka je barem jedan od brojeva $\alpha_1, \alpha_2, \dots, \alpha_n$ iracionalan. Tada postoji beskonačno mnogo n-torki racionalnih brojeva $\frac{p_1}{q}, \dots, \frac{p_n}{q}$ sa svojstvom*

$$|\alpha_i - \frac{p_i}{q}| < \frac{1}{q^{1+1/n}}, \quad i = 1, \dots, n. \tag{3.34}$$

Dokaz: Primijenit ćemo Teorem 3.7 za $m = 1$. Zaključujemo da postoje (relativno prosti) cijeli brojevi $q, p_1, \dots, p_n$ takvi da je

$$1 \le q < Q^n, \quad \text{i} \quad |\alpha_i q - p_i| \le \frac{1}{Q},\ i = 1, \dots, n. \tag{3.35}$$

Očito je da nejednakosti (3.35) povlače nejednakosti (3.34).

Neka je, recimo, α_1 iracionalan. Tada je $|\alpha_1 q - p_1| \ne 0$. Zato, za fiksne $q, p_1, \dots, p_n$, nejednakosti (3.35) mogu vrijediti samo za $Q \le \frac{1}{|\alpha_1 q - p_1|}$. Prema tome, kad $Q \to \infty$, dobivamo beskonačno mnogo različitih rješenja. □

Korolar 3.4. *Neka su* $1, \alpha_1, \cdots, \alpha_m$ *realni brojevi linearno nezavisni nad* $\mathbb{Q}$. *Tada postoji beskonačno mnogo* $(m+1)$*-torki relativno prostih brojeva* $(q_1, \ldots, q_m, p)$ *sa svojstvom*

$$q = \max\{|q_1|, \ldots, |q_m|\} > 0 \quad i \quad |\alpha_1 q_1 + \cdots + \alpha_m q_m - p| < \frac{1}{q^m}. \tag{3.36}$$

Dokaz: Iz Teorema 3.7 za $n = 1$ slijedi da postoje cijeli brojevi $q_1, \cdots, q_m, p$ takvi da je

$$1 \leq \max\{|q_1|, \ldots, |q_m|\} < Q^{1/m} \quad \text{i} \quad |\alpha_1 q_1 + \cdots + \alpha_m q_m - p| \leq \frac{1}{Q}. \tag{3.37}$$

Očito je da (3.37) povlači (3.36). Zbog linearne nezavisnosti, vrijedi $|\alpha_1 q_1 + \cdots + \alpha_m q_m - p| \neq 0$. Zbog toga, za fiksne $q_1, \ldots, q_m, p$, nejednakost (3.37) vrijedi samo za $Q \leq \frac{1}{|\alpha_1 q_1 + \cdots + \alpha_m q_m - p|}$. Prema tome, kad $Q \to \infty$, dobivamo beskonačno mnogo različitih rješenja. □

Analogon Rothovog teorema dobivamo kao posljedicu poznatog *Schmidtovog teorema o potprostorima.*

Teorem 3.8 (Schmidt (1972))**.** *Neka su* $L_1, \ldots, L_n$ *linearno nezavisne linearne forme u* n *varijabli s algebarskim koeficijentima, te neka je* $\delta > 0$. *Tada sve cjelobrojne točke* $x = (x_1, \ldots, x_n)$ *koje zadovoljavaju nejednadžbu*

$$|L_1(x) \cdot \ldots \cdot L_n(x)| < \frac{1}{\|x\|^\delta}$$

leže u konačno mnogo pravih potprostora od $\mathbb{Q}^n$.

Korolar 3.5. *Neka su* $\alpha_1, \ldots, \alpha_n$ *algebarski brojevi takvi da su* $1, \alpha_1, \ldots, \alpha_n$ *linearno nezavisni nad* $\mathbb{Q}$, *te neka je* $\delta > 0$. *Tada postoji samo konačno mnogo* n*-torki* $(\frac{p_1}{q}, \ldots, \frac{p_n}{q})$ *racionalnih brojeva takvih da je*

$$\left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+\frac{1}{n}+\delta}}, \quad i = 1, 2, \ldots, n. \tag{3.38}$$

Dokaz: Pomnožimo li sve nejednakosti u (3.38), te rezultat još pomnožimo s q^{n+1}, dobivamo

$$q|\alpha_1 q - p_1| \cdots |\alpha_n q - p_n| < \frac{1}{q^\delta}.$$

Stavimo $x = (p_1, \ldots, p_n, q) \in \mathbb{Z}^{n+1}$. Promotrimo linearne forme

$$L_i(x_1, \ldots, x_{n+1}) = \alpha_i x_{n+1} - x_i, \quad L_{n+1}(x_1, \ldots, x_{n+1}) = x_{n+1}.$$

Za dovoljno veliki q, imamo

$$|L_1(x) \cdots L_{n+1}(x)| < \frac{1}{q^\delta} < \frac{1}{\|x\|^{\delta/2}}.$$

Primjenom Teorema 3.8 za dimenziju $n+1$, dobivamo da rješenja ove nejednadžbe leže u konačno mnogo pravih racionalnih potprostora. Elementi takvog potprostora zadovoljavaju jednadžbu oblika

$$c_1x_1 + \cdots + c_{n+1}x_{n+1} = 0, \quad c_i \in \mathbb{Q}.$$

Za rješenja od (3.38) koja leže u tom potprostoru vrijedi

$$(c_1\alpha_1 + \cdots c_n\alpha_n + c_{n+1})q = c_1(\alpha_1 q - p_1) + \cdots + c_n(\alpha_n q - p_n).$$

Stavimo $\gamma = |c_1\alpha_1 + \cdots + c_n\alpha_n + c_{n+1}|$. Tada je $\gamma > 0$ zbog uvjeta linearne nezavisnosti od $1, \alpha_1, \ldots, \alpha_n$. Za dani potprostor, broj γ je fiksan. Nadalje,

$$\gamma \cdot q \leq |c_1||\alpha_1 q - p_1| + \cdots + |c_n||\alpha_n q - p_n| \leq |c_1| + \cdots + |c_n|.$$

Stoga je q omeđen. Dakle, u svakom od konačno potprostora imamo samo konačno mnogo q-ova koji zadovoljavaju (3.38). □

Slično kao kod Rothovog teorema, i ovaj njegov analogon je "neefektivan", tj. ne daje eksplicitnu gornju ogradu za veličinu q-ova koji zadovoljavaju (3.38). Postoje efektivni rezultati ovog tipa za neke konkretne vrijednosti α_i-ova. Metode kojima su dobiveni ti rezultati vrlo su slične onima iz prethodnog poglavlja. Spomenimo rezultat Rickerta iz 1993. godine:

$$\max\{|\sqrt{2} - \frac{p_1}{q}|, |\sqrt{3} - \frac{p_2}{q}|\} > \frac{10^{-7}}{q^{1.913}},$$

za sve $p_1, p_2, q \in \mathbb{N}$. Kao posljedica dobiva se da sva rješenja sustava pellovskih jednadžbi

$$x^2 - 2y^2 = u, \quad z^2 - 3y^2 = v$$

zadovoljavaju nejednakost $\max\{|x|, |y|, |z|\} \leq (10^7 \cdot \max\{|u|, |v|\})^{12}$.

3.4 Linearne forme u logaritmima

Želimo li riješiti sustav pellovskih jednadžbi

$$x^2 - ay^2 = c, \quad z^2 - by^2 = d,$$

možemo riješiti svaku jednadžbu zasebno i dobivena rješenja (za y) izjednačiti. Znamo da će rješenja biti oblika

$$x + y\sqrt{a} = (x^* + y^*\sqrt{a})(u + v\sqrt{a})^m,$$

odnosno

$$z + y\sqrt{b} = (z' + y'\sqrt{b})(s + t\sqrt{b})^n,$$

gdje su $u + v\sqrt{a}$ i $s + t\sqrt{b}$ fundamentalna rješenja pripadnih Pellovih jednadžbi, a $x^* + y^*\sqrt{a}$ i $z' + y'\sqrt{b}$ prolaze konačnim skupom fundamentalnih rješenja promatranih pellovskih jednadžbi. Odavde je

$$y = \frac{1}{2\sqrt{a}}\Big[(x^* + y^*\sqrt{a})(u + v\sqrt{a})^m - (x^* - y^*\sqrt{a})(u - v\sqrt{a})^m\Big],$$

odnosno

$$y = \frac{1}{2\sqrt{b}}\Big[(z' + y'\sqrt{b})(s + t\sqrt{b})^n - (z' - y'\sqrt{b})(s - t\sqrt{b})^n\Big].$$

Ugrubo imamo da je $\gamma\cdot\alpha^m \approx \delta\cdot\beta^n$, gdje su $\alpha, \beta, \gamma, \delta$ kvadratne iracionalnosti. Logaritmiranjem dobivamo

$$m\ln\alpha - n\ln\beta + \ln\frac{\gamma}{\delta} \approx 0.$$

Od kraja 60-tih godina 20. stoljeća (Alan Baker) do danas, pojavilo se više rezultata koji govore o tome da linearna forma u logaritmima algebarskih brojeva ne može biti jako blizu nuli. Takvi rezultati daju (eksplicitnu) gornju ogradu za m i n u našem problemu traženja rješenja sustava pellovskih jednadžbi, a primjenjivi su i na mnoge druge diofantske probleme.

Razvoj teorije linearnih formi u logaritmima motiviran je sedmim Hilbertovim problemom koji je tražio da se dokaže da ako je α algebarski broj $\neq 0, 1$, te β algebarski i iracionalan, onda je α^β transcendentan broj. Tu su tvrdnju dokazali neovisno Gelfond i Schneider 1934. godine. Baker je 1967. godine poopćio taj rezultat i dokazao da ako su $\alpha_1, \dots \alpha_n$ algebarski brojevi $\neq 0, 1$ i $\beta_1, \dots, \beta_n$ algebarski brojevi takvi da su $1, \beta_1, \dots, \beta_n$ linearno nezavisni nad $\mathbb{Q}$, onda je broj $\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$ transcendentan.

Dakle, ako su $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ kao gore, a α_{n+1} proizvoljan algebarski broj, onda je $\beta_1\ln\alpha_1 + \cdots + \beta_n\ln\alpha_n \neq \alpha_{n+1}$. Štoviše, Baker je pokazao da broj

$$|\beta_1\ln\alpha_1 + \cdots + \beta_n\ln\alpha_n - \alpha_{n+1}|$$

ne može biti jako mali.

Za primjene na diofantske jednadžbe, od interesa je malo drugačija situacija u kojoj su β_i-ovi cijeli brojevi. Dakle, promatramo izraze oblika

$$\Lambda = b_1\ln\alpha_1 + \cdots + b_n\ln\alpha_n,$$

gdje su $b_i \in \mathbb{Z}$, $i = 1, \dots, n$. Pokazuje se da ako je $\Lambda \neq 0$, onda se $|\Lambda|$ može ocijeniti odozdo u terminima veličine apsolutne vrijednosti od b_i-ova, te stupnja i visina α_i-ova. Mi ćemo dokazati jedan jednostavniji rezultat takvog tipa (Stewart), koji međutim nije dovoljno jak za primjene na diofantske jednadžbe (može se povući analogija s Liouvilleovim teoremom), a potom ćemo navesti i rezultat (Baker-Wüstholz) koji ćemo kasnije primjenjivati.

Prije toga recimo nešto o visinama algebarskih brojeva. Neka je α algebarski broj, neka je $g(x)$ njegov minimalni polinom, te neka je, kao i prije, $P(x)$ višekratnik od $g(x)$ s relativno prostim cjelobrojnim koeficijentima (zvat ćemo ga cjelobrojni minimalni polinom od α):

$$P(x) = a_d x^d + \cdots a_1 x + a_0 = a_d \prod_{i=1}^{d} (x - \alpha^{(i)}).$$

Visina (naivna visina) od α je $H(\alpha) = \max\{|a_d|, \ldots, |a_1|, |a_0|\}$.

Postoje i druge definicije visine algebarskog broja. Npr.

$$M(\alpha) = |a_d| \prod_{i=1}^{d} \max\{|\alpha^{(i)}|, 1\},$$

koja se naziva *Mahlerova mjera* broja α, ili *logaritamska Weilova visina* $h(\alpha) = \frac{1}{d} \ln M(\alpha)$. Vrijedi sljedeća nejednakost između naivne visine i Mahlerove mjere: $M(\alpha) \leq \sqrt{d+1} H(\alpha)$.

Propozicija 3.1. *Neka je $\alpha \neq 0$ algebarski broj. Tada vrijedi*

$$\left(\frac{H(\alpha)}{|a_0|} + 1 \right)^{-1} < |\alpha| < \frac{H(\alpha)}{|a_d|} + 1.$$

Dokaz: Možemo pretpostaviti da je $|\alpha| \geq 1$. Iz $P(\alpha) = 0$, imamo

$$a_d \alpha = -a_{d-1} - a_{d-2}\alpha^{-1} - \cdots - a_0 \alpha^{-d+1},$$

pa je

$$\begin{aligned} |a_d| \cdot |\alpha| &\leq (|a_{d-1}| + |a_{d-2}||\alpha^{-1}| + \cdots + |a_0||\alpha^{-d+1}|) \\ &\leq H(\alpha)(1 + |\alpha|^{-1} + \cdots + |\alpha|^{-d+1}) < \frac{H(\alpha)}{1 - |\alpha|^{-1}}, \end{aligned}$$

odakle je $|\alpha| - 1 < \frac{H(\alpha)}{|a_d|}$.

Time je dokazana desna nejednakost iz propozicije. Lijeva nejednakost slijedi primjenom desne na algebarski broj α^{-1}, čiji je cjelobrojni minimalni polinom jednak $x^d P(\frac{1}{x})$. □

Propozicija 3.2. *Neka je $d = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n)] : \mathbb{Q}]$ stupanj algebarskog proširenja polja $\mathbb{Q}$ generiranog algebarskim brojevima $\alpha_1, \ldots, \alpha_n$. Neka je $B = \max\{|b_1|, \ldots, |b_n|, 2\}$, te $A = \max\{H(\alpha_1), \ldots, H(\alpha_n)\}$. Ako je $\Lambda \neq 0$, onda je $|\Lambda| > \frac{1}{(3A)^{dnB}}$.*

Dokaz: Neka je a_j vodeći koeficijent cjelobrojnog minimalnog polinoma od α_j ako je $b_j \geq 0$, odnosno od α_j^{-1} ako je $b_j < 0$. Stavimo

$$\begin{aligned} w &= a_1^{|b_1|} \cdots a_n^{|b_n|} (\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1) \\ &= a_1^{|b_1|} \cdots a_n^{|b_n|} (\alpha_1^{\varepsilon_1 |b_1|} \cdots \alpha_n^{\varepsilon_n |b_n|} - 1). \end{aligned}$$

Uočimo da je w algebarski cijeli broj stupnja najviše d (jer je $a_i^{|b_i|}\alpha_i^{\varepsilon_i|b_i|}$ algebarski cijeli broj).

Konjugati od w imaju oblik

$$\sigma(w) = a_1^{|b_1|}\cdots a_n^{|b_n|}(\sigma(\alpha_1^{\varepsilon_1})^{|b_1|}\cdots\sigma(\alpha_n^{\varepsilon_n})^{|b_n|} - 1),$$

gdje je σ ulaganje od $\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$ koje fiksira $\mathbb{Q}$. Po Propoziciji 3.1 imamo $|a_i\sigma(\alpha_i^{\varepsilon_i})| < 2A$, pa je

$$|\sigma(w)| < 2\cdot(2A)^{nB}. \tag{3.39}$$

Ako je $w = 0$, onda je $e^{\Lambda} = 1$, pa je Λ višekratnik od $2\pi i$ (različit od 0), pa tvrdnja propozicije vrijedi.

Ako je $w \neq 0$, onda je apsolutna vrijednost produkta svih konjugata od w prirodan broj. Zato iz (3.39) dobivamo

$$|w| \geq \frac{1}{\prod_{\sigma\neq\mathrm{id}}|\sigma(w)|} \geq \left(2\cdot(2A)^{nB}\right)^{-d+1}. \tag{3.40}$$

Za sve kompleksne brojeve z vrijedi nejednakost

$$|e^{|z|} - 1| \leq |z|\cdot e^{|z|}. \tag{3.41}$$

Možemo pretpostaviti da je $|\Lambda| < \frac{1}{2}$. Tada je $e^{|\Lambda|} < 2$, pa iz (3.41) dobivamo

$$|\alpha_1^{b_1}\cdots\alpha_n^{b_n} - 1| = |e^{\Lambda} - 1| \leq |\Lambda|\cdot e^{|\Lambda|} \leq 2|\Lambda|.$$

Odavde i iz (3.40) slijedi

$$\begin{aligned}
|\Lambda| &\geq \frac{|\alpha_1^{b_1}\cdots\alpha_n^{b_n} - 1|}{2} = \frac{|w|}{2a_1^{|b_1|}\cdots a_n^{|b_n|}} \\
&\geq \frac{1}{2\cdot(2\cdot(2A)^{nB})^{d-1}}\cdot\frac{1}{(2A)^{nB}} = \frac{1}{2^d\cdot(2A)^{dnB}} \\
&> \frac{1}{(3A)^{dnB}}.
\end{aligned}$$

□

Već smo napomenuli da nejednakost iz Propozicije 3.2 nije dovoljno dobra za većinu primjena. Možemo se pitati koliko jaka nejednakost bi uopće mogla vrijediti. Uzmimo zbog jednostavnosti da su α_i-ovi racionalni brojevi. Neka je $S = \{b_1\ln\alpha_1 + \cdots + b_n\ln\alpha_n \,:\, |b_j| \leq B,\ H(\alpha_j) \leq A_j,\ j = 1,\ldots,n\}$. Kardinalni broj od S je $\leq (2B+1)^n(2A+1)^{2n}$ (minimalni polinomi od α_i-ova imaju samo dva koeficijenta). Elementi skupa S su sadržani u segmentu $[-nB\ln A, nB\ln A]$. Ako bi elementi od S bili "uniformno distribuirani" unutar ovog segmenta, onda bismo očekivali da najmanji element u S ima apsolutnu vrijednost približno

$$\frac{2nB\ln A}{(2B+1)^n(2A+1)^{2n}}.$$

Ovakva razmatranja su motivirala Lang-Waldschmidtovu slutnju, koja glasi da (uz oznake $B_j = |b_j|$, $B = \max_{1\le j\le n} B_j$, $A_j = \max\{H(\alpha_j), 1\}$) za svaki $\varepsilon > 0$, postoji $C(\varepsilon) > 0$ tako da ako je $\Lambda \neq 0$, onda je

$$|\Lambda| > \frac{C(\varepsilon)^n B}{(B_1 \cdots B_n A_1^2 \cdots A_n^2)^{1+\varepsilon}}.$$

Jedan od najboljih (i najspretnijih za primjenu) poznatih općih rezultata ovog tipa je sljedeći teorem Bakera i Wüstholza iz 1993:

Teorem 3.9 (Baker-Wüstholz)**.** *Neka je* $\Lambda = b_1 \ln \alpha_1 + \cdots + b_n \ln \alpha_n$ *linearna forma u logaritmima algebarskih brojeva* $\alpha_1, \ldots, \alpha_n$ *s cjelobrojnim koeficijentima* $b_1, \ldots, b_n$*. Ako je* $\Lambda \neq 0$*, onda je*

$$\ln |\Lambda| \geq -18(n+1)!n^{n+1}(32d)^{n+2} \ln(2nd) h'(\alpha_1) \cdots h'(\alpha_n) \ln B,$$

gdje je $d = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$*,* $B = \max\{|b_1|, \ldots, |b_n|\}$*,* $h'(\alpha) = \max\{h(\alpha), \frac{1}{d}|\ln \alpha|, \frac{1}{d}\}$*, a* $h(\alpha)$ *je logaritamska Weilova visina.*

Usporedimo ovaj teorem s Propozicijom 3.2 i Lang-Waldschmidtovom slutnjom. Ugrubo, Teorem 3.9 kaže da je $\ln |\Lambda| \geq -C(n,d) \ln A_1 \cdots \ln A_n \ln B$. Usporedimo li to s Propozicijom 3.2 koja daje $\ln |\Lambda| > -C_1(n,d) \ln A \cdot B$, vidimo da je faktor B zamijenjen sa $\ln B$. Ako pak Teorem 3.9 usporedimo s Lang-Waldschmidtovom slutnjom, vidimo da bi se možda moglo očekivati da je moguće produkt $\ln A_1 \cdots \ln A_n$ zamijeniti sa sumom $\ln A_1 + \cdots + \ln A_n$.

Rezultat Bakera i Wüstholza je malo poboljšao Matveev 2000. godine. Postoje i poboljšanja za slučajeve (koji su najvažniji za primjene) $n = 2$ (Laurent, Mignotte, Nesterenko [1995]) i $n = 3$ (Mignotte [2006]). Ta poboljšanja su vrlo relevantna kod rješavanja parametarskih familija diofantskih jednadžbi, jer obično daju zaključak da za velike vrijednosti parametara imamo samo "trivijalna" rješenja, te ostavljaju relativno mali broj pojedinačnih jednadžbi koje treba posebno ispitati. Kad je u pitanju samo jedna konkretna jednadžba, onda je Baker-Wüstholzov teorem (pa čak i originalni Bakerov rezultat iz 1967.), u kombinaciji s metodama redukcije koje ćemo obraditi u sljedećim poglavljima, najčešće sasvim dovoljan.

3.5 Baker-Davenportova redukcija

Već smo napomenuli da se mnogi problemi iz diofantskih jednadžbi mogu transformirati u nejednadžbe za linearne forme u logaritmima algebarskih brojeva. Te nejednadžbe obično imaju oblik

$$|n_1 \ln \alpha_1 + \cdots + n_k \ln \alpha_k| < c_1 e^{-c_2 N},$$

gdje su $n_1, \ldots, n_k \in \mathbb{Z}$, $N = \max\{|n_1|, \ldots, |n_k|\}$, te c_1, c_2 pozitivne konstante. Tada se mogu primijeniti rezultati iz prethodnog poglavlja (npr. Baker-Wüstholzov teorem). Tako se dobije nejednadžba oblika

$$c_3 \ln N > c_2 N - \ln c_1,$$

odakle slijedi da je $N \leq N_0$, gdje je N_0 eksplicitna konstanta (obično dosta velika, npr. 10^{20} ili 10^{100}). Budući da je N_0 najčešće prevelik (osim kada je $k = 2$) da bi se ispitali svi mogući preostali slučajevi, postavlja se pitanje može li se ta ograda smanjiti. Odgovor je potvrdan. Naime, poznata su dva algoritma koji (ako su ispunjeni određeni tehnički uvjeti) ogradu $N \leq N_0$ zamjenjuju sa $N \leq N_1$, gdje je $N_1 \approx \ln N_0$.

U ovom i sljedećem poglavlju prikazat ćemo te dvije metode. Prva je tzv. *Baker-Davenportova redukcija*. Nju su uveli Baker i Davenport u članku iz 1969. godine u kojem su riješili problem koji se pojavio u diskusiji tijekom konferencije u Oberwolfachu u ožujku 1968. Problem je povezan s tzv. *Diofantovim m-torkama*, tj. skupovima prirodnih brojeva sa svojstvom da je produkt svaka dva njihova različita člana uvećan za 1 jednak kvadratu nekog prirodnog broja. Najpoznatija Diofantova četvorka je skup $\{1, 3, 8, 120\}$ koji je pronašao Fermat (zaista, $1 \cdot 3 + 1 = 2^2$, $1 \cdot 8 + 1 = 3^2$, $1 \cdot 120 + 1 = 11^2$, $3 \cdot 8 + 1 = 5^2$, $3 \cdot 120 + 1 = 19^2$, $8 \cdot 120 + 1 = 31^2$). Na spomenutoj konferenciji, van Lint je prikazao svoje rezultate vezane uz pitanje može li se Fermatov skup proširiti do petorke s istim svojstvom. Ili još preciznije: ako je d prirodan broj takav da je $\{1, 3, 8, d\}$ Diofantova četvorka, mora li d biti jednak 120?

Primjenom Bakerove teorije linearnih formi u logaritmima, te novouvedene metode redukcije, Baker i Davenport su u potpunosti riješili taj problem. Njihov rezultat je kasnije generaliziran u više smjerova. Danas je poznato da ne postoji Diofantova šestorka, te da Diofantovih petorki ima najviše konačno mnogo (Dujella [2004]).

Prikazat ćemo sada kako se Baker-Wüstholzov teorem (ili bilo koji rezultat sličnog tipa) može primijeniti na problem proširenja Fermatovog skupa.

Neka je d prirodan broj takav da je

$$1 \cdot d + x^2, \quad 3 \cdot d + 1 = y^2, \quad 8 \cdot d + 1 = z^2.$$

Tada je

$$y^2 - 3x^2 = -2, \tag{3.42}$$
$$z^2 - 8x^2 = -7, \tag{3.43}$$

pa smo dobili sustav pellovskih jednadžbi. Očito su fundamentalna rješenja pripadnih Pellovih jednadžbi $2 + \sqrt{3}$, odnosno $3 + \sqrt{8}$. Sada se lako dobije da su sva rješenja jednadžbe (3.42) dana sa

$$y + x\sqrt{3} = \pm(1 \pm \sqrt{3})(2 + \sqrt{3})^n, \tag{3.44}$$

a sva rješenja jednadžbe (3.43) sa

$$z + x\sqrt{8} = \pm(1 \pm \sqrt{8})(3 + \sqrt{8})^m. \tag{3.45}$$

Možemo pretpostaviti da je x pozitivan. Imajući u vidu da je $(1 - \sqrt{3})(2 + \sqrt{3}) = -(1+\sqrt{3})$, u (3.44) možemo izostaviti predznake $-$ (klasa je dvoznačna), pa dobivamo sljedeću eksponencijalnu jednadžbu:

$$\begin{aligned} &\frac{(1+\sqrt{3})(2+\sqrt{3})^n - (1-\sqrt{3})(2-\sqrt{3})^n}{2\sqrt{3}} \\ = \quad &\frac{(2\sqrt{2}\pm 1)(3+2\sqrt{2})^m + (2\sqrt{2}\mp 1)(3-2\sqrt{2})^m}{4\sqrt{2}}, \end{aligned} \tag{3.46}$$

tj. jednadžbu oblika $v_n = w_m^{+,-}$, gdje su v_n, $w_m^{+,-}$ (binarni rekurzivni) nizovi. Imamo $v_0 = w_0^{+,-} = 1$, odakle je $d = 0$ (trivijalno rješenje), te $v_2 = w_2^- = 11$, odakle je $d = 11^2 - 1 = 120$. Želimo dokazati da drugih rješenja nema.

Lako se vidi da je $w_n^{+,-} > v_n$, odakle slijedi da je $m < n$.

Lema 3.5. *Neka su $m, n > 2$ prirodni brojevi koji zadovoljavaju (3.46). Tada vrijedi*

$$0 < |\Lambda| < 7.3 \cdot (2+\sqrt{3})^{-2n}, \tag{3.47}$$

gdje je

$$\Lambda = n\ln(2+\sqrt{3}) - m\ln(3+2\sqrt{2}) + \ln\frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)}.$$

Dokaz: Očito je

$$v_n > \frac{(1+\sqrt{3})(2+\sqrt{3})^n}{2\sqrt{3}}, \quad w_m^{+,-} < \frac{2\sqrt{2}+1)(3+2\sqrt{2})^m}{2\sqrt{2}},$$

pa iz $v_n = w_m^{+,-}$ slijedi

$$(3-2\sqrt{2})^m < \frac{(2\sqrt{2}+1)\sqrt{3}}{(\sqrt{3}+1)\sqrt{2}}(2-\sqrt{3})^n < 1.7163(2-\sqrt{3})^n.$$

Sada iz (3.46), dijeljenjem s $\frac{2\sqrt{2}\pm 1}{2\sqrt{2}} \cdot (3+2\sqrt{2})^m$, dobivamo

$$\begin{aligned} &\left|\frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)} \cdot \frac{(2+\sqrt{3})^n}{(3+2\sqrt{2})^m} - 1\right| \\ &\le \frac{2\sqrt{2}+1}{2\sqrt{2}-1} \cdot (3-2\sqrt{2})^{2m} + \frac{2\sqrt{2}(\sqrt{3}-1)}{\sqrt{3}(2\sqrt{2}-1)}(2-\sqrt{3})^n(3-2\sqrt{2})^m \\ &< 7.29(2-\sqrt{3})^{2n}. \end{aligned}$$

Iskoristit ćemo sljedeću jednostavnu činjenicu:

Ako je $a \in \langle 0,1\rangle$ i $0 < |X| < a$, onda je

$$|\ln(X+1)| < \frac{-\ln(1-a)}{a} \cdot |X|. \tag{3.48}$$

Zaista,

$$|\ln(X+1)| = \left|\sum_{i=1}^{\infty} \frac{(-1)^{i-1}X^i}{i}\right| \leq |X| \cdot \sum_{i=1}^{\infty} \frac{a^{i-1}}{i} = |X| \cdot \frac{-\ln(1-a)}{a}.$$

Primjenom nejednakosti (3.48) na $X = \frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)} \cdot \frac{(2+\sqrt{3})^n}{(3+2\sqrt{2})^m} - 1$ i $a = 0.0027$ ($\approx 7.29 \cdot (2-\sqrt{3})^6$), dobivamo traženu nejednakost

$$|\Lambda| < 7.3 \cdot (2-\sqrt{3})^{2n}.$$

Još treba dokazati da je $|\Lambda| > 0$. Ako bi bilo $\Lambda = 0$, onda bi (kvadriranjem) dobili da je

$$16(2+\sqrt{3})^{2n+1} = 3(9 \pm 4\sqrt{2})(3+2\sqrt{2})^{2m},$$

što je kontradikcija (jer je jednakost oblika $a+b\sqrt{3} = c+d\sqrt{2}$, $a,b,c,d \in \mathbb{Q}$, moguća samo ako je $b = d = 0$). □

Sada imamo sve spremno za primjenu Baker-Wüstholzovog teorema na formu Λ iz Leme 3.5. Imamo: $\alpha_1 = 2+\sqrt{3}$, $\alpha_2 = 3+2\sqrt{2}$, $\alpha_3 = \frac{2(4\pm\sqrt{2})(3+\sqrt{3})}{21}$, $b_1 = n$, $b_2 = -m$, $b_3 = 1$, $d = 4$ (jer je $\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3) = \mathbb{Q}(\sqrt{2},\sqrt{3})$). Minimalni polinomi su

$$\begin{aligned} P_{\alpha_1}(x) &= x^2 - 4x + 1, \\ P_{\alpha_2}(x) &= x^2 - 6x + 1, \\ P_{\alpha_3}(x) &= 441x^4 - 2016x^3 + 2880x^2 - 1536x + 256, \end{aligned}$$

pa su visine $h(\alpha_1) = \frac{1}{2}\ln(2+\sqrt{3}) \approx 0.6585$, $h(\alpha_2) = \frac{1}{2}\ln(3+2\sqrt{2}) \approx 0.8814$, $h(\alpha_3) = \frac{1}{4}\ln\left(441 \cdot \frac{2(4+\sqrt{2})(3+\sqrt{3})}{21} \cdot \frac{2(4-\sqrt{2})(3+\sqrt{3})}{21}\right) \approx 1.7836$. Dakle, Baker-Wüstholzov teorem nam daje

$$\ln(|\Lambda|) \geq -18\cdot 4!\cdot 3^4\cdot(32\cdot 4)^5\cdot \ln 24\cdot 0.6585\cdot 0.8814\cdot 1.7836 \ln n \geq -3.96\cdot 10^{15}\ln n.$$

Usporedimo li ovo s (3.47), dobivamo nejednadžbu

$$3.96 \cdot 10^{15} \ln n > 2.63n - 1.99,$$

koja povlači da je $n < 6 \cdot 10^{16}$.

Sljedeća lema predstavlja jednu od varijanti Baker-Davenportove redukcije.

Lema 3.6. *Neka su κ i μ realni brojevi, te neka je N prirodan broj. Neka je $\frac{p}{q}$ konvergenta u razvoju verižnog razlomka od κ takva da je $q > 6N$, te neka je $\varepsilon = \|\mu q\| - N \cdot \|\kappa q\|$, gdje $\| \ \|$ označava udaljenost od najbližeg cijelog broja.*

Ako je $\varepsilon > 0$, onda nejednadžba

$$0 < n\kappa - m + \mu < A \cdot B^{-n},$$

($A > 0$, $B > 1$ realni brojevi) nema rješenja u prirodnim brojevima m i n takvima da vrijedi

$$\frac{\ln(\frac{Aq}{\varepsilon})}{\ln B} \leq n \leq N.$$

Dokaz: Pretpostavimo da je $1 \leq n \leq N$. Imamo:

$$n(\kappa q - p) + np - mq + \mu q < qAB^{-n}.$$

Odavde je

$$qAB^{-n} > |\mu q - (mq - np)| - n\|\kappa q\| \geq \|\mu q\| - N\|\kappa q\| = \varepsilon,$$

što povlači da je

$$n < \frac{\ln(\frac{Aq}{\varepsilon})}{\ln B}.$$

□

Napomena 3.5. Uvjet $q > 6N$ u lemi je donekle proizvoljan. Naime, s jedne strane želimo biti što sigurniji da će vrijediti uvjet $\varepsilon > 0$, a s druge strane želimo da q bude što manji (da bi nova granica bila što manja). Iz svojstava konvergenti verižnih razlomaka, znamo da vrijedi $\|\kappa q\| < \frac{1}{q}$, dok o $\|\mu q\|$ općenito znamo samo da je $\leq \frac{1}{2}$. Zato je razumno uzeti da je barem $q > 2N$, a $q > 6N$ je eksperimentalno potvrđen kao solidan izbor.

Napomena 3.6. Ako uvjet $\varepsilon > 0$ nije zadovoljen, onda možemo pokušati uzeti sljedeću konvergentu i provjeriti hoće li za nju uvjet biti zadovoljen. Čak i ako je $\varepsilon < 0$, moguće je dobiti neku informaciju o n. Naime, ako označimo $r = \lfloor \mu q + \frac{1}{2} \rfloor$, onda je

$$\begin{aligned} |np - mq + r| &< qAB^{-n} + |\mu q - r| + n|\kappa q - p| \leq qAB^{-n} + \|\mu q\| + N\|\kappa q\| \\ &< qAB^{-n} + \frac{1}{2} + \frac{1}{6}. \end{aligned}$$

Ako je $qAB^{-n} > \frac{1}{3}$, onda je $n < \frac{\ln(3Aq)}{\ln B}$. Ako je $qAB^{-n} \leq \frac{1}{3}$, onda je $np - mq + r = 0$, što znači da je $np \equiv -r \pmod{q}$. Ova kongruencija ima jedinstveno rješenje $n \equiv n_0 \pmod{q}$, pa iz $n \leq N < q$, slijedi da je $n = n_0$.

Primjer 3.3. Primijenimo redukciju iz Leme 3.6 na formu Λ iz Leme 3.5 uz $N = 6 \cdot 10^{16}$. Ovdje je $\kappa = \frac{\ln(2+\sqrt{3})}{\ln(3+2\sqrt{2})}$, $\mu_{1,2} = \frac{\ln\left(\frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)}\right)}{\ln(3+2\sqrt{2})}$, $A = \frac{7.3}{\ln(3+2\sqrt{2})}$, $B = (2+\sqrt{3})^2$. Razvoj od κ u verižni razlomak je

$$[0; 1, 2, 1, 20, 1, 5, 3, 8, 5, 1, 2, 1, 1, 1, 1, 4, 3, 3, 3, 1, 6, 3, 1, 2, 22,\\ 1, 2, 8, 2, 1, 2, 6, 3, 20, 2, 10, 3, \ldots],$$

pa je prva konvergenta od κ koja zadovoljava uvjet $q > 6N$ jednaka

$$\frac{p}{q} = \frac{742265900639684191}{9935223607325971 20}.$$

Vidjet ćemo da će za μ_1 trebati uzeti sljedeću konvergentu, pa promotrimo najprije što se dobije za μ_2. Imamo $\|\mu_2 q\| \approx 0.24492$, $\|\kappa q\| \cdot N \approx 0.01878$, pa je $\varepsilon \approx 0.22614 > 0$. Primjenom Leme 3.6, dobivamo da je $n \leq 16$. Sada možemo ponoviti redukciju s $N = 16$. Odgovarajuća konvergenta je sada $\frac{p'}{q'} = \frac{387}{518}$ i redukcija daje $n \leq 3$.

Kao što smo već rekli, primjenom Leme 3.6 za μ_1 i gore navedene p, q, dobivamo negativan ε ($\|\mu_1 q\| \approx 0.007626$, $\|\kappa q\| \cdot N \approx 0.01878$). Stoga uzimamo sljedeću konvergentu

$$\frac{P}{Q} = \frac{2297570640187354392}{3075296607888933649}.$$

Dobivamo $\|\mu_1 Q\| \approx 0.2989$, $\|\kappa Q\| \cdot N \approx 0.002254$, pa je pripadni $\varepsilon \approx 0.29665 > 0$, te možemo primijeniti redukciju, koja nam daje $n \leq 17$. Ponovimo li redukciju za $N = 17$, ponovo dobivamo da je odgovarajuća konvergenta $\frac{p'}{q'} = \frac{387}{518}$ i redukcija nam daje $n \leq 4$.

Lako se provjerava da jednadžbe $v_n = w_m^{+,-}$ nemaju rješenja za $n = 3, 4$. Tako smo dovršili dokaz tvrdnje da ako je $\{1, 3, 8, d\}$ Diofantova četvorka, onda mora biti $d = 120$.

3.6 LLL-redukcija

Neka su $b_1, \ldots, b_n$ linearno nezavisni vektori u $\mathbb{R}^n$. *Rešetka* L razapeta ovim vektorima je skup svih njihovih cjelobrojnih linearnih kombinacija:

$$L = \left\{ \sum_{i=1}^{n} n_i \cdot b_i \ : \ n_i \in \mathbb{Z} \right\}.$$

Npr. u $\mathbb{R}^2$, ako je $b_1 = (1, 0)$, $b_2 = (0, 1)$, onda je L rešetka svih točaka u ravnini s cjelobrojnim koordinatama. Kaže se da je $B = \{b_1, \ldots, b_n\}$ *baza rešetke* L. Jedna rešetka može imati više različitih baza, pa se pitamo možemo li izabati bazu koja bi imala neko dodatno dobro svojstvo. Jasno je

da B predstavlja bazu vektorskog prostora $\mathbb{R}^n$. Znamo da Gram-Schmidtovim postupkom možemo dobiti ortogonalnu bazu za isti vektorski prostor ($b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*$, $i = 1, \ldots, n$, gdje je $\mu_{ij} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$). No, ta nova baza ne mora razapinjati istu rešetku kao polazna baza B, jer koeficijenti μ_{ij} ne moraju biti cijeli brojevi. Općenito, rešetka ni ne mora imati ortogonalnu bazu. A. K. Lenstra, H. W. Lenstra i L. Lovász uveli su *pojam LLL-reducirane baze*, koja ima svojstva:

1) $|\mu_{i,j}| \leq \frac{1}{2}$, $1 \leq j < i \leq n$;

2) $\|b_i^*\|^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)\|b_{i-1}^*\|^2$.

Prvi uvjet se može interpretirati tako da se kaže da je LLL-reducirana baza "skoro ortogonalna", dok drugi uvjet govori da niz normi vektora $\|b_i^*\|$ "skoro raste". Dodatno važno svojstvo LLL-reducirane baze je da je prvi vektor u toj bazi vrlo kratak, tj. ima malu normu. Može se dokazati da uvijek vrijedi da je $\|b_1\| \leq 2^{(n-1)/2}\|x\|$, za sve ne-nul vektore $x \in L$, no, u praksi se vrlo često događa da je $\|b_1\|$ upravo najkraći ne-nul vektor iz L. To ćemo precizirati u sljedećoj lemi. U njoj se pojavljuje broj $\Delta(L) = |\det(b_1, \ldots, b_n)|$ koji zovemo *determinanta rešetke*. Može se pokazati da $\Delta(L)$ ne ovisi o izboru baze (zato što prelazak iz baze u bazu odgovara množenju zdesna matricom iz $GL_n(\mathbb{Z})$.)

Lema 3.7. *Neka je $\{b_1, \ldots, b_n\}$ LLL-reducirana baza, te $\{b_1^*, \ldots, b_n^*\}$ pripadna Gram-Schmidtova baza. Tada vrijedi:*

1) $\|b_j\|^2 \leq 2^{i-1}\|b_i^*\|^2$, $1 \leq j \leq i \leq n$;

2) $\Delta(L) \leq \prod_{i=1}^n \|b_i\| \leq 2^{\frac{n(n-1)}{4}}\Delta(L)$;

3) $\|b_1\| \leq 2^{\frac{n-1}{4}} (\Delta(L))^{\frac{1}{n}}$;

4) za svaki $x \in L$, $x \neq 0$, vrijedi $\|b_1\|^2 \leq c_1\|x\|^2$, gdje je

$$c_1 = \max\left\{ \frac{\|b_1\|^2}{\|b_i^*\|^2} \,:\, 1 \leq i \leq n \right\} \leq 2^{n-1}.$$

5) Za vektor $y \notin L$ definiramo $\sigma = B^{-1}y$, gdje je B matrica čiji su stupci $b_1, \ldots, b_n$. Neka je i_0 najveći indeks takav da $\sigma_{i_0} \notin \mathbb{Z}$, te $\{\sigma_{i_0}\}$ udaljenost od σ_{i_0} do najbližeg cijelog broja. Tada za svaki $x \in L$ vrijedi

$$\|x - y\|^2 \geq c_1^{-1}\{\sigma_{i_0}\}\|b_1\|^2.$$

Dokaz: Dokazat ćemo samo tvrdnju 4). Dokazi ostalih tvrdnji mogu se naći u [Smart: The Algorithmic Resolution of Diophantine Equations].

Neka je

$$x = \sum_{i=1}^{n} r_i b_i = \sum_{i=1}^{n} r_i' b_i^*, \quad r_i \in \mathbb{Z},\ r_i' \in \mathbb{R}.$$

Neka je i_0 najveći indeks za kojega je $r_{i_0} \neq 0$. Tada je (po definiciji Gram-Schmidtove baze) $r'_{i_0} = r_{i_0}$, pa imamo

$$\|x\|^2 = \sum_{i=1}^{n} {r_i'}^2 \|b_i^*\|^2 \geq {r'_{i_0}}^2 \|b_{i_0}^*\|^2 \geq \|b_{i_0}^*\|^2 \geq c_1^{-1}\|b_1\|^2.$$

□

U svom članku iz 1982. godine, Lenstra, Lenstra i Lovász prikazali su polinomijalni algoritam za konstrukciju LLL-reducirane baze iz proizvoljne baze rešetke (po njima nazvan *LLL-algoritam*). Algoritam je ubrzo našao brojne primjene, npr. u faktorizaciji polinoma s racionalnim koeficijentima, kriptoanalizi RSA kriptosustava s malim javnim ili tajnim eksponentom, problemu ruksaka, te diofantskim aproksimacijama i diofantskim jednadžbama.

Prikazat ćemo de Wegerovu varijantu LLL-algoritma iz 1989. godine, koja koristi samo cjelobrojnu aritmetiku. Za $i = 1, \ldots, n$, uvedimo oznaku

$$D_i = \det(\langle b_j, b_l \rangle_{1 \leq j,l \leq i}) = \prod_{j=1}^{i} \langle b_j^*, b_j^* \rangle.$$

Tada je $c_i = D_{i-1} b_i^* \in \mathbb{Z}^n$, $\lambda_{ij} = D_j \mu_{ij} \in \mathbb{Z}$.

Algoritam INIT: (nalazi Gram-Schmidtovu bazu)

$D_0 = 1$
for $i = 1$ to n do
    $c_i = b_i$
    for $j = 1$ to $i - 1$ do
        $\lambda_{ij} = \langle b_j, c_j \rangle$
        $c_i = (D_j c_i - \lambda_{ij} c_j)/D_{j-1}$
    $D_i = \langle c_i, c_i \rangle / D_{i-1}$

Algoritam MI-LAMBDA: (postiže da $|\mu_{kl}| \leq \frac{1}{2}$)

if $(2|\lambda_{kl}| > D_l)$ then
    $r = [\lambda_{kl}/D_l]$
    $b_k = b_k - r b_l$
    for $j = 1$ to $l - 1$ do
        $\lambda_{kj} = \lambda_{kj} - r\lambda_{lj}$
    $\lambda_{kl} = \lambda_{kl} - r D_l$

Algoritam ZAMIJENI: (zamjenjuje b_k i b_{k-1}, te pripadne podatke)

zamijeni vektore b_{k-1} i b_k
for $j = 1$ to $k-2$ do
    zamijeni $\lambda_{k-1,j}$ i $\lambda_{k,j}$
for $i = k+1$ to n do
    $t = \lambda_{i,k-1}$
    $\lambda_{i,k-1} = (\lambda_{i,k-1}\lambda_{k,k-1} + \lambda_{i,k}D_{k-2})/D_{k-1}$
    $\lambda_{i,k} = (tD_k - \lambda_{i,k}\lambda_{k,k-1})/D_{k-1}$
$D_{k-1} = (D_{k-2}D_k + \lambda_{k,k-1}^2)/D_{k-1}$

LLL-algoritam (de Wegerova varijanta):

primijeni algoritam INIT na matricu B
$k = 2$
while $(k \leq n)$ do
    primijeni algoritam MI-LAMBDA za $l = k-1$
    if $(4D_{k-2}D_k < (3D_{k-1}^2 - 4\lambda_{k,k-1}^2)$ then
        primijeni algoritam ZAMIJENI
        if $k > 2$ then $k = k-1$
    else
        for $l = k-1$ to 1 do
            primijeni algoritam MI-LAMBDA
        $k = k+1$

Pokazat ćemo sada kako se LLL-algoritam može primijeniti na diofantske probleme koji se mogu transformirati u nejednakosti za linearne forme (u logaritmima).

Promotrimo nejednadžbu oblika

$$|\alpha_0 + x_1\alpha_1 + \cdots x_n\alpha_n| < c_2 e^{-c_3 X},$$

gdje su α_i dani realni ili kompleksni brojevi, c_2 i c_3 pozitivne realne konstante, te $X = \max\{|x_1|, \ldots, |x_n|\}$. Rješenja tražimo u cijelim brojevima $x_1, \ldots, x_n$. Pretpostavimo da je poznato da je $X \leq X_0$, gdje je X_0 neka (velika) konstanta. Slično kao kod Baker-Davenportove redukcije, želimo dobiti novu gornju ogradu oblika $X \leq c \ln X_0$. Razmotrit ćemo slučaj kada su svi α_i realni.

Odaberimo konstantu $C \approx X_0^n$. Linearnoj formi $\alpha_0 + \sum_{i=1}^n x_i\alpha_i$ pridružimo rešetku L generiranu stupcima matrice

$$A = \begin{bmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & 0 & 0 \\ 0 & \cdots & 1 & 0 \\ [C\alpha_1] & \cdots & [C\alpha_{n-1}] & [C\alpha_n] \end{bmatrix}.$$

Ovdje $[\alpha]$ označava najbliži cijeli broj realnom broju α. Konstantu C smo izabrali da bude približno jednaka X_0^n, jer tada po Lemi 3.7.3) možemo očekivati da će najmanji vektor LLL-reducirane baze imati normu približno X_0. Koristeći LLL-algoritam možemo naći donju ogradu c_4 za veličinu

$$l(L,y) = \begin{cases} \min\{\|x-y\| \,:\, x \in L\}, & y \notin L \\ \min\{\|x\| \,:\, x \in L,\ x \neq 0\}, & y \in L, \end{cases}$$

gdje je $y = [0,\ldots,0,-[C\alpha_0]]^\tau$.

Lema 3.8. *Neka je* $S = (n-1)X_0^2$ *i* $T = \frac{1+nX_0}{2}$. *Ako je* $c_4^2 \geq T^2 + S$, *onda vrijedi*

$$X \leq \frac{1}{c_3}\left(\ln(Cc_2) - \ln(\sqrt{c_4^2 - S} - T)\right),$$

ili je $x_1 = \cdots = x_{n-1}$, $x_n = -\frac{[C\alpha_0]}{[C\alpha_n]}$.

Dokaz: Neka je $\varphi = [C\alpha_0] + \sum_{i=1}^n x_i[C\alpha_i]$. Tada je

$$|\varphi - C(\alpha_0 + \sum_{i=1}^n x_i\alpha_i)| \leq \frac{1}{2} + \sum_{i=1}^n \frac{X_0}{2} = T.$$

Stoga je $|\varphi| \leq T + C \cdot c_2 e^{-c_3 X}$. Neka je $x = [x_1,\ldots,x_n]^\tau$, te $z = Ax$. Tada je $z - y = [x_1,\ldots,x_{n-1},\varphi]^\tau$. Budući da je $z \in L$, imamo da je ili $z = y$ (pa je $x_1 = \cdots = x_{n-1} = 0$ i $x_n = -\frac{[C\alpha_0]}{[C\alpha_n]}$) ili

$$c_4^2 \leq l(L,y)^2 \leq \sum_{i=1}^{n-1} x_i^2 + \varphi^2 \leq S + \left(T + Cc_2e^{-c_3X}\right)^2.$$

Po pretpostavci je $c_4^2 \geq S$, pa dobivamo

$$e^{-c_3X} \geq \frac{1}{Cc_2}(\sqrt{c_4^2 - S} - T). \tag{3.49}$$

Koristeći pretpostavku da je $c_4^2 \geq T^2 + S$, iz (3.49) logaritmiranjem dobivamo

$$X \leq \frac{1}{c_3}\left(\ln(Cc_2) - \ln(\sqrt{c_4^2 - S} - T)\right).$$

□

Napomena 3.7. Ako su α_i kompleksni brojevi, onda se umjesto gornje matrice A promatra matrica

$$\begin{bmatrix} 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & 0 & 0 & 0 \\ 0 & \cdots & 1 & 0 & 0 \\ [C\mathrm{Re}(\alpha_1)] & \cdots & \cdots & [C\mathrm{Re}(\alpha_{n-1})] & [C\mathrm{Re}(\alpha_n)] \\ [C\mathrm{Im}(\alpha_1)] & \cdots & \cdots & [C\mathrm{Im}(\alpha_{n-1})] & [C\mathrm{Im}(\alpha_n)] \end{bmatrix}.$$

Primjer 3.4. *Nađimo kubni polinom s cjelobrojnim koeficijentima (malim po apsolutnoj vrijednosti) kojem je jedan korijen blizu* $\pi = 3.14159\ldots$*, a jedan blizu* $e = 2.71828\ldots$.

Rješenje: Problem možemo shvatiti kao nalaženje koeficijenata $x_1, \ldots, x_4$ takvih da linearne forme $|x_1\pi^3 + x_2\pi^2 + x_3\pi + x_4|$ i $|x_1e^3 + x_2e^2 + x_3e + x_4|$ budu (istovremeno) male, a da pritom $|x_i|$ ne budu preveliki (recimo reda veličine 10^2). Zato promotrimo rešetku generiranu stupcima matrice

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 3101 & 987 & 314 & 100 \\ 2009 & 739 & 272 & 100 \end{pmatrix}$$

(elementi u trećem retku su $[100 \cdot \pi^{4-i}]$, a u četvrtom $[100 \cdot e^{4-i}]$). Želimo dobiti LLL-reduciranu bazu za ovu rešetku. Točnije, ovdje nas zanima matrica "prijelaza" U takva da stupci matrice AU čine LLL-reduciranu bazu. Nju možemo dobiti korištenjem naredbe `qflll`$(A, 1)$ u programskom paketu PARI (drugi argument 1 znači da se koristi cjelobrojna varijanta LLL-algoritma). Naredbe za nalaženje LLL-reducirane baze postoje i u drugim programskim paketima (npr. `lattice` u Maplu ili `LatticeReduce` u Mathematici). Dobivamo:

$$\begin{pmatrix} -3 & 0 & -8 & 1 \\ 2 & 1 & -1 & -9 \\ 66 & -6 & 214 & 27 \\ -134 & 9 & -414 & -27 \end{pmatrix}.$$

Sada prvi stupac od U daje koeficijente željenog polinoma:

$$f(x) = 3x^3 - 2x^2 - 66x + 134.$$

Njegovi korijeni su približno 3.147875, 2.725321 i -5.20653. ♢

Primjer 3.5. *Nađimo sva rješenja nejednadžbe*

$$|x_1 \ln 2 + x_2 \ln 3 + x_3 \ln 5| \leq 2e^{-X}, \tag{3.50}$$

gdje je $X = \max\{|x_1|, |x_2|, |x_3|\} \leq X_0 = 10^{30}$.

Rješenje: Nejednadžba je oblika $|\Lambda| \leq c_2e^{-c_3X}$, gdje je $c_2 = 2$, $c_3 = 1$. Kao što smo već ranije opisali, linearnoj formi Λ pridružujemo rešetku generiranu stupcima matrice

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ [C \ln 2] & [C \ln 3] & [C \ln 5] \end{pmatrix}.$$

Savjet je bio uzeti C reda veličine X_0^3. Pokazuje se da obično treba uzeti C nešto veći, da bi uvjeti Leme 3.8 bili zadovoljeni. Stoga uzmimo $C = 10^{100}$. Veličine S i T iz Leme 3.8 su $S = 2 \cdot 10^{30}$, $T = \frac{1}{2}(1 + 3 \cdot 10^{30})$. Za prvi vektor LLL-reducirane baze dobivamo

$$\begin{pmatrix} -151524626390368016373546862561679 9 \\ -502897304507254890263203391695738 \\ 116593725586775716630432905636640 3 \end{pmatrix}.$$

Imamo: $\|b_1\|^2 \approx 3.9083 \cdot 10^{66}$ i dobivamo $c_1 = 1$. Iz Leme 3.7 je

$$l(L,0)^2 \geq c_1^{-1}\|b_1\|^2 = c_4^2 \approx 3.9083 \cdot 10^{66}.$$

Vidimo da je zadovoljen uvjet $c_4^2 \geq T^2 + S$ iz Leme 3.8. Uvrštavanjem svih poznatih vrijednosti u Lemu 3.8, dobivamo novu ogradu:

$$X \leq 154.$$

Ovo je znatno manja ograda od polazne $X \leq 10^{30}$. No, i nju možemo još reducirati. Dakle, uzmimo da je $X_0 = 154$, te neka je $C = 10^9$. Promotrimo rešetku generiranu stupcima matrice

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 693147181 & 10988612289 & 1609437912 \end{pmatrix}.$$

Dobivamo da se pripadna LLL-reducirana baza sastoji od stupaca matrice

$$\begin{pmatrix} 573 & 747 & 713 \\ -237 & 938 & -611 \\ -300 & -55 & 1794 \end{pmatrix}.$$

Nadalje je $c_1 = 1$, $c_4 = 474498$, $S = 47432$, $T = 231.5$, pa se može primijeniti Lema 3.8 koja nam daje novu gornju ogradu

$$X \leq 15.$$

Postupak se može dalje nastaviti. No, ograda je već dovoljno mala da se sve preostale mogućnosti mogu i direktno ispitati. Dobiva se da su sva rješenja:

$$\begin{aligned}(x_1, x_2, x_3) = {} & (-6,-5,6), (-4,4,1), (-3,-4,4), (-3,-1,2), (-2,0,1), \\ & (-1,-1,1), (-1,0,0,), (-1,1,0), (-1,2,-1), (0,-3,2), \\ & (0,-1,1), (0,0,0), (0,1,-1), (0,3,-2), (1,-2,1), (1,-1,0), \\ & (1,0,0), (1,1,-1), (2,0,-1), (3,1,-2), (3,4,-4), (4,-4,1), \\ & (6,5,-6).\end{aligned}$$

Napomenimo da su ova 23 rješenja ujedno i sva rješenja nejednadžbe (3.50), jer iz Baker-Wüstholzovog teorema slijedi da (3.50) nema rješenja u kojima je $X > 10^{15}$. ♢

Poglavlje 4

Cjelobrojne točke na eliptičkim krivuljama i Thueova jednadžba

4.1 Elementarni rezultati o Mordellovoj jednadžbi $\mathbf{y^2 = x^3 + k}$

Godine 1923. Mordell je dokazao da diofantske jednadžbe oblika

$$y^2 = ax^3 + bx^2 + cx + d,$$

gdje kubni polinom na desnoj strani jednadžbe nema višestrukih korijena, imaju samo konačno mnogo cjelobrojnih rješenja. Krivulje zadane takvim jednadžbama se nazivaju *eliptičke krivulje*. Mordellov dokaz koristi svođenje ovakve jednadžbe na konačno mnogo Thueovih jednadžbi, o čemu će biti više riječi kasnije.

Problem nalaženja svih cjelobrojnih rješenja ovakvih jednadžbi, (tj. svih cjelobrojnih točaka na eliptičkim krivuljama) nije jednostavan. No, poznato je dosta rezultata, posebno za jednadžbe oblika $y^2 = x^3 + k$, koji su dobiveni sasvim elementarnim metodama - razmatranjem konguencija modulo 4 i 8, te svojstava kvadratnih ostataka.

Propozicija 4.1. *Neka je $k = (4b-1)^3 - 4a^2$, gdje je a cijeli broj koji nema prostih faktora oblika $4l + 3$. Tada jednadžba $y^2 = x^3 + k$ nema cjelobrojnih rješenja.*

Dokaz: Imamo $k \equiv -1 \pmod 4$, pa je $y^2 \equiv x^3 - 1 \pmod 4$. Budući da je $y^2 \equiv 0$ ili $1 \pmod 4$, x ne može biti paran niti kongruentan -1 modulo 4. Stoga je $x \equiv 1 \pmod 4$. Zapišimo jednadžbu $y^2 = x^3 + (4b-1)^3 - 4a^2$ u obliku

$$y^2 + 4a^2 = x^3 + (4b-1)^3 = (x + 4b - 1)(x^2 - x(4b-1) + (4b-1)^2).$$

Zadnji faktor $x^2 - x(4b-1) + (4b-1)^2$ je kongruentan 3 modulo 4. Stoga on mora imati barem jedan prosti faktor p koji je također kongruentan 3 modulo 4. No, taj prosti faktor p može dijeliti zbroj dva kvadrata $y^2 + 4a^2$ jedino ako su i y i a djeljivi s p (jer je s jedne strane Legendeov simbol $(\frac{-1}{p}) = (-1)^{(p-1)/2} = -1$, a s druge strane bi bilo $(\frac{-1}{p}) = (\frac{-4a^2}{p}) = (\frac{y^2}{p}) = 1$), a to je u suprotnosti s pretpostavkom da a nema prostih faktora oblika $4l+3$. □

Navedimo nekoliko cijelih brojeva k koji zadovoljavaju uvjete Propozicije 4.1: $k = -5,\ 11,\ 23,\ -73$.

Sljedeći rezultat se dokazuje sasvim analogno kao Propozicija 4.1.

Propozicija 4.2. *Neka je $k = (4b+2)^3 - (2a+1)^2$, te neka su svi prosti faktori od $2a+1$ oblika $4l+1$. Tada jednadžba $y^2 = x^3 + k$ nema cjelobrojnih rješenja.*

Propozicija 4.3. *Neka je $k = 2b^2 - a^3$, gdje je $a \equiv 2, 4 \pmod 8$, $b \equiv 1 \pmod 2$ i svi prosti faktori od b su oblika $8l \pm 1$. Tada jednadžba $y^2 = x^3 + k$ nema cjelobrojnih rješenja.*

Dokaz: Imamo $y^2 \equiv x^3 + 2 \pmod 4$, pa je $x \not\equiv 0 \pmod 2$ i $x \not\equiv 1 \pmod 4$. Stoga je $x \equiv 3 \pmod 4$, tj. $x \equiv 3$ ili $7 \pmod 8$. Nadalje,

$$y^2 - 2b^2 = x^3 - a^3 = (x-a)(x^2 + ax + a^2).$$

Ako je $x \equiv 3 \pmod 8$, onda je $x^2 + ax + a^2 \equiv 1 + 3a + a^2 \equiv \pm 3 \pmod 8$, pa $x^2 + ax + a^2$ ima barem jedan prosti faktor p oblika $8l \pm 3$. Po pretpostavci, p ne dijeli b, pa dobivamo

$$\left(\frac{2}{p}\right) = \left(\frac{2b^2}{p}\right) = \left(\frac{y^2}{p}\right) = 1.$$

Dobili smo kontradikciju jer je $(\frac{2}{p}) = 1$ akko $p \equiv \pm 1 \pmod 8$.

Ako je $x \equiv 7 \pmod 8$, onda je $x - a \equiv 7 - a \equiv \pm 3 \pmod 8$, pa $x - a$ mora imati barem jedan prosti faktor oblika $8l \pm 3$, iz čega dobivamo kontradikciju na sasvim isti način kao i u prethodnom slučaju. □

Nekoliko vrijednosti od k koje zadovoljavaju uvjete Propozicije 4.3 su $k = -6,\ 34,\ 58,\ -62,\ 66,\ 90$.

Sasvim analogno prethodnoj propoziciji dokazuje se sljedeći rezultat.

Propozicija 4.4. *Neka je $k = -2b^2 - a^3$, gdje je $a \equiv 4 \pmod 8$, $b \equiv 1 \pmod 2$ i svi prosti faktori od b su oblika $8l+1$ ili $8l+3$. Tada jednadžba $y^2 = x^3 + k$ nema cjelobrojnih rješenja.*

Primjer 4.1. *Pokažimo da jednadžba $y^2 = x^3 + 45$ nema cjelobrojnih rješenja.*

Dokaz: Zbog $y^2 \equiv x^3+5 \pmod 8$, imamo da je $x \equiv 3$ ili $7 \pmod 8$. Ako bi bilo $x \equiv 0 \pmod 3$, onda bi iz $x = 3X$, $y = 3Y$, dobili $Y^2 = 3X^3 + 5 \equiv 2 \pmod 3$, što je kontradikcija, jer 2 nije kvadratni ostatak modulo 3. Stoga x nije djeljiv s 3.

Pretpostavimo da je $x \equiv 3 \pmod 8$. Zapišimo jednadžbu u obliku

$$y^2 - 2 \cdot 6^2 = x^3 - 27 = (x-3)(x^2+3x+9).$$

Imamo da je $x^2 + 3x + 9 \equiv 3 \pmod 8$, pa taj broj mora imati neki prosti faktor p oblika $8l \pm 3$. No, budući da smo provjerili da je $p \neq 3$, p ne može biti faktor od $y^2 - 2 \cdot 6^2$.

Pretpostavimo da je $x \equiv 7 \pmod 8$. Sada ćemo polaznu jednadžbu zapisati u obliku

$$y^2 - 2 \cdot 3^2 = x^3 + 27 = (x+3)(x^2-3x+9).$$

Imamo da je $x^2 - 3x + 9 \equiv 5 \pmod 8$, pa taj broj mora imati neki prosti faktor p oblika $8l \pm 3$. No, p ne može biti faktor od $y^2 - 2 \cdot 3^2$, pa smo ponovo dobili kontradikciju. ♢

4.2 Primjena faktorizacije u kvadratnim poljima

Jednadžbu $y^2 = x^3 + k$ možemo zapisati u obliku $x^3 = y^2 - k$, te je faktorizirati u polju $\mathbb{Q}(\sqrt{k})$:

$$x^3 = (y + \sqrt{k})(y - \sqrt{k}). \tag{4.1}$$

Da bi mogli ovu faktorizaciju iskoristiti za rješavanje polazne jednadžbe, potrebne su nam neke informacije o cijelim brojevima u kvadratnom polju $\mathbb{K} = \mathbb{Q}(\sqrt{k})$. Pretpostavit ćemo da je k kvadratno slobodan. Ponajprije, podsjetimo se da je prsten cijelih brojeva $O_{\mathbb{K}}$ u $\mathbb{K}$ jednak $\{u + v\sqrt{k} : u, v \in \mathbb{Z}\}$ ako je $k \equiv 2$ ili $3 \pmod 4$, odnosno $\{u + v\frac{1+\sqrt{k}}{2} : u, v \in \mathbb{Z}\}$ ako je $k \equiv 1 \pmod 4$. Sljedeći važan podatak je struktura skupa jedinica (invertibilnih elemenata) u $O_{\mathbb{K}}$. Kod proučavanja Pellovih jednadžbi pokazali smo da ako je $k \geq 2$, onda ima beskonačno mnogo jedinica u $\mathbb{K}$, i one imaju oblik $\pm\varepsilon_k^n$, $n \in \mathbb{Z}$, gdje je ε_k fundamentalna jedinica. Ako je k negativan, onda $\mathbb{K}$ ima jednice ± 1, i to su jedine jedinice, osim u slučajevima $k = -1$ i $k = -3$. Jedinice u $\mathbb{Q}(\sqrt{-1})$ su ± 1, $\pm i$, a u $\mathbb{Q}(\sqrt{-3})$ su ± 1, $\frac{\pm 1 \pm \sqrt{-3}}{2}$.

U relaciji 4.1 imamo da je produkt dva broja jednak kubu. Kad bi se radilo o produktu (običnih) cijelih brojeva i ako bi faktori bili relativno prosti, onda bismo mogli zaključiti da su oba faktora kubovi. U tom zaključku se koristi jednistvenost rastava cijelih brojeva na proste faktore. Nažalost, to svojstvo ne vrijedi za cijele brojeve u svim kvadratnim poljima. Preciznije, jedina kvadratna polja s takvim svojstvom za $k < 0$ su ona za

$k = -1, -2, -3, -7, -11, -13, -19, -43, -67, -163$, dok je slutnja da takvih polja za $k > 0$ ima beskonačno mnogo.

Na primjer, u $\mathbb{Q}(\sqrt{-5})$ imamo:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5}) \qquad (4.2)$$

i može se pokazati da su svi faktori $3, 7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{5}, 4 + \sqrt{5}, 4 - \sqrt{5}$ *nerastavljivi*, tj. da su djeljivi samo s jedinicama i sebi pridruženim brojevima (brojevi su pridruženi ako im je kvocijent jedinica).

Ipak, jedinstvenost faktorizacije je moguće dobiti ukoliko se umjesto brojeva promatraju ideali. Neka je D integralna domena. *Ideal* I u D je potprsten od D koji je zatvoren s obzirom na množenje elementima iz D, tj. $r \in D$, $a \in I \Rightarrow ra \in I$. Važan primjer ideala su *glavni ideali*, koji su oblika $< a > = \{ra : r \in D\}$. Općenitije, skup $< a_1, \ldots, a_n >= \{\sum_{i=1}^{n} r_i a_i : r_i \in D\}$ je ideal u D. Ukoliko su svi ideali u D glavni, onda kažemo da je D *domena glavnih ideala* (PID). Na primjer, može se pokazati da ideal $< 7, 4 + \sqrt{5} >$ nije glavni ideal u $O_{\mathbb{Q}(\sqrt{-5})}$, pa $O_{\mathbb{Q}(\sqrt{-5})}$ nije PID. Usporedimo li ovaj primjer s (4.2), naslućujemo da su pitanja jednoznačne faktorizacije i postojanja ideala koji nisu glavni usko povezana. I zaista, vrijedi: $O_{\mathbb{K}}$ ima svojstvo jednoznačne faktorizacije na nerastavljive elemente (kaže se da je UFD - Unique Factorization Domain) ako i samo ako je $O_{\mathbb{K}}$ domena glavnih ideala.

Produkt ideala I i J se definira sa

$$IJ = \{x \in D : x = i_1 j_1 + \cdots + i_r j_r,\ r \in \mathbb{N},\ i_1, \ldots, i_r \in I,\ j_1, \ldots, j_r \in J\}.$$

Posebno, $< a >< b >=< ab >$, $< a_1, a_2 >< b_1, b_2 >=< a_1 b_1, a_1 b_2, a_2 b_1, a_2 b_2 >$. Ideal $< 1 >= D$ je neutralni element na ovu operaciju množenja. Neka su A i B ideali. Reći ćemo da A dijeli B, i pisati $A|B$, ako postoji ideal C tako da je $B = AC$. Vrijedi: $A|B \Leftrightarrow B \subseteq A$.

Pravi ideal P (tj. ideal koji je različit od $< 0 >$ i $< 1 >$) se naziva *prost ideal* ako

$$a, b \in D, ab \in P \Rightarrow a \in P \text{ ili } b \in P.$$

Svaki ideal u $O_{\mathbb{K}}$ može se na jedinstven način prikazati kao produkt prostih ideala.

Vratimo se sada na naš primjer (4.2) nejednoznačne faktorizacije broja 21 u $O_{\mathbb{Q}(\sqrt{-5})}$, te rastavimo glavni ideal $< 21 >$ na produkt prostih ideala: $< 21 >= \mathfrak{p}\mathfrak{p}'\mathfrak{q}\mathfrak{q}'$, gdje je

$$\mathfrak{p} =< 3, 1 + \sqrt{-5} >, \quad \mathfrak{p}' =< 3, 1 - \sqrt{-5} >,$$
$$\mathfrak{q} =< 7, 4 + \sqrt{-5} >, \quad \mathfrak{q}' =< 7, 4 - \sqrt{-5} > .$$

Sada one tri različite faktorizacije iz (4.2) dobijemo tako da na različite

načine grupiramo dva po dva od ova četiri prosta ideala. Zaista,

$$\begin{aligned} \mathfrak{p}\mathfrak{p}' &= <3>, \quad \mathfrak{q}\mathfrak{q}' = <7>; \\ \mathfrak{p}\mathfrak{q} &= <4+\sqrt{-5}>, \quad \mathfrak{p}'\mathfrak{q}' = <4-\sqrt{-5}>; \\ \mathfrak{p}\mathfrak{q}' &= <1-2\sqrt{-5}>, \quad \mathfrak{p}'\mathfrak{q} = <1+2\sqrt{-5}> . \end{aligned}$$

Dokažimo samo prvu jednakost:

$$\begin{aligned} \mathfrak{p}\mathfrak{p}' &= <9, 3(1-\sqrt{-5}), 3(1+\sqrt{-5}), 6> = <3><3, 1-\sqrt{-5}, 1+\sqrt{-5}, 2> \\ &= <3><1> = <3> \end{aligned}$$

(ako ideal sadrži 3 i 2, onda mora sadržavati i $3-2=1$).

Na skupu svih ideala u $O_{\mathbb{K}}$ definiramo relaciju ekvivalencije: $A \sim B$ ako postoje $\alpha, \beta \in O_{\mathbb{K}} \setminus \{0\}$ takvi da je $<\alpha> A = <\beta> B$. Uz množenje klasa definirano pomoću predstavnika ($[A][B] = [AB]$), dobivamo grupu koja se naziva *grupa klasa ideala*. Broj klasa ekvivalencije (red grupe klasa ideala) je konačan broj i označava se s $h(\mathbb{K})$, te zove broj klasa od $\mathbb{K}$ (engl. class number). Očito je da su svi glavni ideali međusobno ekvivalentni, pa ako je $O_{\mathbb{K}}$ PID, onda je $h(\mathbb{K}) = 1$. Vrijedi i obrat. Stoga je $O_{\mathbb{K}}$ UFD ako i samo ako je $h(\mathbb{K}) = 1$, pa možemo reći da $h(\mathbb{K})$ mjeri koliko $O_{\mathbb{K}}$ odstupa od svojstva jedinstvene faktorizacije na nerastavljive elemente.

Teorem 4.1. *Neka je $k < -1$ kvadratno slobodan cijeli broj, $k \equiv 2, 3 \pmod 4$ i $h(\mathbb{Q}(\sqrt{k})) \not\equiv 0 \pmod 3$.*

a) Ako je k oblika $k = 1-3a^2$, onda su sva cjelobrojna rješenja jednadžbe $y^2 = x^3 + k$ dana sa

$$x = 4a^2 - 1, \quad y = \pm(3a - 8a^3).$$

b) Ako je k oblika $k = -1-3a^2$, onda su sva cjelobrojna rješenja jednadžbe $y^2 = x^3 + k$ dana sa

$$x = 4a^2 + 1, \quad y = \pm(3a + 8a^3).$$

c) Ako je $k \neq \pm 1 - 3a^2$, onda jednadžba $y^2 = x^3 + k$ nema cjelobrojnih rješenja.

Dokaz: Pretpostavimo da jednadžba $y^2 = x^3 + k$ ima cjelobrojnih rješanja. Iz $y^2 \equiv 0, 1 \pmod 4$ i $k \equiv 2, 3 \pmod 4$ slijedi $x^3 \equiv 1, 2, 3 \pmod 4$, pa zaključujemo da x mora biti neparan. Nadalje, $(x, k) = 1$. Zaista, pretpostavimo da prost broj p dijeli i x i k. Tada p^2 dijeli $y^2 - x^3 = k$, što je kontradikcija s pretpostavkom da je k kvadratno slobodan. Dakle, $(x, 2k) = 1$, pa postoje $l, m \in \mathbb{Z}$ takvi da vrijedi

$$lx + 2mk = 1. \tag{4.3}$$

Promotrimo sada imaginarno kvadratno polje $\mathbb{K} = \mathbb{Q}(\sqrt{k})$. Budući da je $k \equiv 2, 3 \pmod 4$, prsten cijelih u $\mathbb{K}$ je $O_{\mathbb{K}} = \{u + v\sqrt{k} : u, v \in \mathbb{Z}\}$. Iz $x^3 = (y + \sqrt{k})(y - \sqrt{k})$, dobivamo jednadžbu u idealima

$$< x >^3 = < y + \sqrt{k} >< y - \sqrt{k} > . \tag{4.4}$$

Pokažimo da su glavni ideali $< y + \sqrt{k} >$ i $< y - \sqrt{k} >$ relativno prosti. Pretpostavimo suprotno, tj. da postoji prosti ideal P takav da $P| < y+\sqrt{k} >$ i $P| < y-\sqrt{k} >$. Tada su $y+\sqrt{k}, y-\sqrt{k} \in P$, pa je $2\sqrt{k} = (y+\sqrt{k})-(y-\sqrt{k}) \in P$ i $2k = \sqrt{k}(2\sqrt{k}) \in P$. Nadalje, $P|< x >^3$ pa, jer je P prost, imamo da $P| < x >$. Sada iz $x, 2k \in P$ i (4.3) slijedi da je $1 \in P$, što je u kontradikciji s pretpostavkom da je P prost.

Zbog jednoznačnosti rastava na produkt prostih ideala, iz (4.4) slijedi da je $< y + \sqrt{k} >= A^3$ za neki ideal A iz $O_{\mathbb{K}}$. Zbog pretpostavke da $3 \nmid h$, ideal A je glavni. Zaista, budući da je h red grupe klasa ideala, to je A^h glavni ideal. Iz $(h, 3) = 1$ slijedi da postoje $r, s \in \mathbb{Z}$ takvi da je $3r + hs = 1$. Ideali A^3 i A^h su glavni, pa je i

$$A = A^{3t+hs} = (A^3)^r (A^h)^s$$

glavni ideal.

Prema tome, $A = < a + b\sqrt{k} >$, gdje su $a, b \in \mathbb{Z}$. Stoga je

$$< y + \sqrt{k} >= < a + b\sqrt{k} >^3 = < (a + b\sqrt{k})^3 > .$$

Dva glavna ideala $< \alpha >$ i $< \beta >$ su jednaka ako i samo ako je α/β jedinica. Zbog naših pretpostavki na k, jedinice u $O_{\mathbb{K}}$ su $\varepsilon = \pm 1$. Dakle, imamo

$$y + \sqrt{k} = \varepsilon(a + b\sqrt{k})^3,$$

a također i $y - \sqrt{k} = \varepsilon(a - b\sqrt{k})^3$. Sada je $x^3 = y^2 - k = \varepsilon^2(a^2 - kb^2)^3 = (a^2 - kb^2)^3$, pa je $x = a^2 - kb^2$. Nadalje, $2\sqrt{k} = \varepsilon \left((a + b\sqrt{k})^3 - (a - b\sqrt{k})^3 \right) = \varepsilon \cdot 2\sqrt{k}(3a^2 b + kb^3)$, pa je $\varepsilon b(3a^2 + kb^2) = 1$. Odavde je očito $b = \pm 1$. Drugim riječima, $b = \pm\varepsilon$.

Ako je $b = \varepsilon$, onda imamo

$$x = a^2 - k, \quad y = \varepsilon(a^3 + 3ka), \quad 1 = 3a^2 + k,$$

pa je

$$k = 1 - 3a^2, \quad x = 4a^2 - 1, \quad y = \pm(3a - 8a^3).$$

Ako je $b = -\varepsilon$, onda imamo $1 = -3a^2 - k$, pa je

$$k = -1 - 3a^2, \quad x = 4a^2 + 1, \quad y = \pm(3a + 8a^3).$$

□

Napomena 4.1. Npr. $k = -2$ zadovoljava uvjete Teorema 4.1.a), jer je $h(\mathbb{Q}(\sqrt{-2})) = 1$. Stoga su sva rješenja jednadžbe $y^2 = x^3 - 2$ dana sa $(x, y) = (3, \pm 5)$. Uvjete Teorema 4.1.b) zadovoljava npr. $k = -13$, jer je $h(\mathbb{Q}(\sqrt{-13})) = 2$. Uvjete Teorema 4.1.c) zadovoljava npr. $k = -5$, jer je $h(\mathbb{Q}(\sqrt{-5})) = 2$. Primijetimo da je slučaj $k = -5$ bio već pokriven i s Propozicijom 4.1. Broj klasa se može izračunati u PARI-ju pomoću naredbe `quadclassunit`, ili koristeći vezu s brojem reduciranih kvadratnih formi s diskriminantom $4k$.

U slučaju kada je $k > 0$, postupamo na sličan način. Bitna razlika je što u tom slučaju imamo beskonačno mnogo jedinica. Preciznije $\varepsilon = \pm\eta^l$, gdje je $\eta = T + U\sqrt{k}$ fundamentalna jedinica u $O_{\mathbb{K}}$ i $l \in \mathbb{Z}$. Budući da je $-1 = (-1)^3$ i $\eta^{3m} = (\eta^m)^3$, zapravo treba promotriti samo tri slučaja:

$$\begin{aligned} y + \sqrt{k} &= (a + b\sqrt{k})^3, \\ y + \sqrt{k} &= \eta(a + b\sqrt{k})^3, \\ y + \sqrt{k} &= \eta^2(a + b\sqrt{k})^3, \end{aligned}$$

Prvi slučaj se rješava na sasvim analogan način kao u Teoremu 4.1, dok se drugi i treći slučaj mogu eliminirati ako se pretpostave neki dodatni uvjeti na k, T, U. Kao primjer navodimo (bez dokaza) sljedeći rezultat.

Teorem 4.2. *Neka je k kvadratno slobodan prirodan broj, $k \equiv 2, 3 \pmod 4$ i $h(\mathbb{Q}(\sqrt{k})) \not\equiv 0 \pmod 3$. Neka je $T + U\sqrt{k}$ fundamentalno rješenje Pellove jednadžbe $T^2 - kU^2 = 1$. Ako je $k \equiv 7 \pmod 9$ i $U \equiv \pm 3 \pmod 9$, onda jednadžba $y^2 = x^3 + k$ nema cjelobrojnih rješenja.*

Napomena 4.2. Npr. $k = 7$ zadovoljava uvjete Teorema 4.2 jer je $7 \equiv 3 \pmod 4$, $7 \equiv 7 \pmod 9$, $h(\mathbb{Q}(\sqrt{7})) = 1$, a fundamentalno rješenje Pellove jednadžbe $T^2 - 7U^2 = 1$ je $8 + 3\sqrt{7}$, pa je $U = 3 \equiv 3 \pmod 9$. Dakle, jednadžba $y^2 = x^3 + 7$ nema cjelobrojnih rješenja.

Dat ćemo i jedan primjer koji pokazuje kako se može postupiti u slučaju kada je $h(\mathbb{Q}(\sqrt{k}))$ djeljiv s 3.

Primjer 4.2. *Jednadžba $y^2 = x^3 - 31$ nema cjelobrojnih rješenja.*

Rješenje: Pokažimo najprije da x mora biti paran. Ako je $x \equiv 1 \pmod 4$, onda dobivamo $y^2 \equiv 2 \pmod 4$, što je nemoguće. Ako je $x \equiv 3 \pmod 4$, onda iz

$$y^2 + 4 = x^3 - 27 = (x - 3)(x^2 + 3x + 9)$$

i $x^2 + 3x + 9 \equiv 3 \pmod 4$ dobivamo kontradikciju.

Faktorizacija broja 2 na produkt prostih ideala u $O_{\mathbb{Q}(\sqrt{-31})}$ je

$$<2> = <2, \frac{3 + \sqrt{-31}}{2}> <2, \frac{3 - \sqrt{-31}}{2}> .$$

Nije teško provjeriti da $<2, \frac{3+\sqrt{-31}}{2}>$ nije glavni ideal.

Iz $y^2 - 31 = x^3$ dobivamo sljedeću faktorizaciju ideala:

$$<\frac{y+\sqrt{-31}}{2}><\frac{y-\sqrt{-31}}{2}>=<2, \frac{3+\sqrt{-31}}{2}><2, \frac{3-\sqrt{-31}}{2}> <\frac{x}{2}>^3.$$

Ideali $<\frac{y+\sqrt{-31}}{2}>$ i $<\frac{y-\sqrt{-31}}{2}>$ su relativno prosti. Stoga zaključujemo da postoji ideal A u $O_{\mathbb{Q}(\sqrt{-31})}$ takav da je

$$<\frac{y+\sqrt{-31}}{2}>=<2, \frac{3+\sqrt{-31}}{2}> A^3.$$

Iz $h(\mathbb{Q}(\sqrt{-31})) = 3$ slijedi da je A^3 glavni ideal, pa dobivamo da je i $<2, \frac{3+\sqrt{-31}}{2}>$, što je kontradikcija. □

4.3 Transformacija eliptičkih krivulja u Thueove jednadžbe

Promotrimo općenitu jednadžbu oblika

$$y^2 = x^3 + ax^2 + bx + c,$$

gdje su koeficijenti a, b, c cijeli brojevi, a kubni polinom na desnoj strani nema višestrukih korijena. Prikazat ćemo Mordellov argument kojim je pokazao da takva jednadžba ima samo konačno mnogo cjelobrojih rješenja. Istovremeno, bit će to i važan korak u jednoj od općih metoda za nalaženje svih cjelobrojnih točaka na eliptičkoj krivulji.

Ideja je faktorizirati polinom

$$f(x) = x^3 + ax^2 + bx + c = (x - \vartheta_1)(x - \vartheta_2)(x - \vartheta_3). \tag{4.5}$$

Tako dobivamo polja $\mathbb{Q}(\vartheta_i)$ u kojima promatramo jednadžbu (4.5). Mguća su tri slučaja:

1) sva tri korijena od f su racionalni (pa onda i cijeli);

2) jedan korijen od f je racionalan, a ostala dva su kvadratne iracionalnosti;

3) f je ireducibilan nad $\mathbb{Q}$, korijeni su mu algebarski cijeli brojevi 3. stupnja.

Podsjetimo se da u $\mathbb{Z}$ vrijedi: ako je $XY = Z^l$ i $(X, Y) = 1$, onda postoje $U, V \in \mathbb{Z}$ tako da je $X = \pm U^l$, $Y = \pm V^l$. Poopćenje tog rezultata na cijele brojeve u polju algebarskih brojeva $\mathbb{K}$ dano je sa:

Lema 4.1. *Sva rješenja jednadžbe* $XY = cZ^l$, *gdje* $(X, Y)|\delta$ *za dani ideal* δ, *imaju oblik*

$$X = \lambda\varepsilon_1 U^l, \quad Y = \mu\varepsilon_2 V^l, \quad Z = \nu\varepsilon_3 UV,$$

gdje su U, V *proizvoljni cijeli brojevi iz* $\mathbb{K}$, $\varepsilon_1, \varepsilon_2, \varepsilon_3$ *su jedinice,* λ, μ, ν *su elementi iz* $\mathbb{K}$. *Posljednjih šest brojeva* $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \lambda, \mu, \nu)$ *poprimaju samo konačno mnogo vrijednosti i zadovoljavaju* $\lambda\mu\varepsilon_1\varepsilon_2 = c\nu^l\varepsilon_3^l$.

Dokaz: Zbog jedinstvene faktorizacije na proste ideale, dana jednadžba povlači sljedeće jednadžbe u idealima:

$$< X >= \delta_1 c_1 a^l, \quad < Y >= \delta_2 c_2 b^l,$$

gdje su δ_1, δ_2 elementi konačnog skupa ideala i u njihovoj faktorizaciji na proste ideale svi prosti ideali dijele δ, a $< c >= c_1 c_2$ je neka faktorizacija ideala $< c >$. Postoji konačno mnogo klasa ideala. Neka je $[a']$ inverz od $[a]$. Tada je aa' glavni ideal, recimo $aa' =< U >$. Iz $a'^l < X >= \delta_1 c_1 < U >^l$, slijedi da je $\delta_1 c_1 / a'^l =< \lambda >$ za neki $\lambda \in \mathbb{K}$. Stoga je $< X >=< \lambda > < U >^l$, što povlači $X = \varepsilon\lambda U^l$, gdje je ε jedinica. Zbog toga što je grupa jedinica konačno generirana, vrijedi da je $\varepsilon = \varepsilon_1 \cdot \varepsilon_0^l$, gdje ε_1 poprima samo konačno mnogo vrijednosti (produkt generatora s potencijama manjim od l). Zbog konačnosti broja klasa i λ poprima samo konačno mnogo vrijednosti. □

Vratimo se na jednadžbu (4.5). Promatramo je u polju $\mathbb{K} = \mathbb{Q}(\vartheta_i)$. Dat ćemo detalje za treći slučaj, kad je kubni polinom $f(x)$ ireducibilan. Transformacija eliptičke krivulje u Thueove jednadžbe u preostala dva slučaja provodi se na sličan način. Iz Leme 4.1 slijedi relacija

$$x - \vartheta_i = m(r + s\vartheta_i + t\vartheta_i^2)^2, \tag{4.6}$$

gdje su $r, s, t \in \mathbb{Z}$, a m poprima konačno mnogo vrijednosti iz $\mathbb{Q}(\vartheta_i)$. Zaista, ϑ_i je algebarski cijeli broj 3. stupnja, pa se svaki element iz $\mathbb{K}$ može napisati u obliku $\alpha + \beta\vartheta_i + \gamma\vartheta_i^2$, $\alpha, \beta, \gamma \in \mathbb{Q}$. No, $\{1, \vartheta_i, \vartheta_i^2\}$ ne mora biti baza za $O_{\mathbb{K}}$ (podsjetimo se polja $\mathbb{Q}(\sqrt{d})$, $d \equiv 1 \pmod 4$). Međutim, može se pokazati da ako je $\frac{1}{d}(r + s\vartheta_i + t\vartheta_i^2) \in O_{\mathbb{K}}$ i $(d, r, s, t) = 1$, onda d^2 dijeli diskriminantu $\Delta[1, \vartheta_i, \vartheta_i^2] = (\vartheta_1 - \vartheta_2)^2(\vartheta_1 - \vartheta_3)^2(\vartheta_2 - \vartheta_3)^2$. Stoga imamo konačno mnogo mogućnosti za d, koje možemo "prebaciti" u m.

I broj m (svaki od konačno mnogo njih) možemo zapisati u obliku $m = r_0 + s_0\vartheta_i + t_0\vartheta_i^2$, gdje su $r_0, s_0, t_0 \in \mathbb{Q}$. Uvrstimo to u (4.6), izmožimo, te ϑ_i^3 i ϑ_i^4 prikažemo pomoću $1, \vartheta_i, \vartheta_i^2$. Usporedimo li koeficijente uz 1, ϑ_i i ϑ_i^2 na obje strane jednadžbe, dobivamo tri jednadžbe oblika

$$f_1(r, s, t) = 0, \quad f_2(r, s, t) = 1, \quad f_3(r, s, t) = x,$$

gdje su f_1, f_2, f_3 ternarne kvadratne forme s racionalnim koeficijentima. U Poglavlju 2 smo vidjeli da se rješivost jednadžbe $f_1(r, s, t) = 0$ može efikasno

ustanoviti. Također smo pokazali da su (uz pretpostavku da netrivijalno rješenje postoji) sva rješenja dana s

$$gr = q_1(u,v), \quad gs = q_2(u,v), \quad qt = q_3(u,v),$$

gdje su q_1, q_2, q_3 binarne kvadratne forme s cjelobrojnim koeficijentima, a g poprima konačno mnogo cjelobrojnih vrijednosti. Uvrstimo li to u jednadžbu $f_2(r,s,t) = 1$, dobivamo konačno mnogo jednadžbi oblika

$$h(u,v) = g^2, \tag{4.7}$$

gdje je h homogeni polinom 4. stupnja s cjelobrojnim koeficijentima. Može se provjeriti da h nije kvadrat polinoma 2. stupnja. Stoga po Thueovom teoremu zaključujemo da jednadžba (4.7) ima konačno mnogo rješenja, pa zato i polazna eliptička krivulja ima samo konačno mnogo cjelobrojnih točaka (koje dobijemo iz $f_3(r,s,t) = x$).

Primjer 4.3. *Želimo naći sve trokutaste brojeve koji su jednaki produktu tri uzastopna prirodna broja (problem je postavio Mohanty [1988], a riješio de Weger [1989]). Podsjetimo da se trokutasti brojevi definirani sa* $T_n = \frac{n(n+1)}{2}$. *Pokazuje se da postoji točno 6 rješenja:*

$$T_3 = 1\cdot 2\cdot 3, \quad T_{15} = 4\cdot 5\cdot 6, \quad T_{20} = 5\cdot 6\cdot 7, \quad T_{44} = 9\cdot 10\cdot 11,$$
$$T_{608} = 56\cdot 57\cdot 58, \quad T_{22736} = 636\cdot 637\cdot 638.$$

Rješenje: Na ovom primjeru ćemo ilustrirati gore opisanu metodu transformacije eliptičkih krivulja u Thueove jednadžbe. Neke od dobivenih jednadžbi 4. stupnja će biti vrlo jednostavne, dok ćemo rješavanje nekih odgoditi dok ne objasnimo metodu za rješavanje općih Thueovih jednadžbi.

Zadani uvjet se može zapisati u obliku $\frac{n(n+1)}{2} = m(m+1)(m+2)$. Pomnožimo obje strane jednadžbe s 8, te uvedimo supstituciju $x = 2m+2$, $y = 2n+1$. Tako dobivamo jednadžbu eliptičke krivulje

$$y^2 = x^3 - 4x + 1 \tag{4.8}$$

(tražimo cjelobrojne točke na (4.8) u kojima je $x \geq 4$ paran i $y \geq 3$ neparan). Pokazat ćemo da eliptička krivulja (4.8) ima točno 22 cjelobrojne točke:

$$(x,y) = (-2,\pm 1),(-1,\pm 2),(0,\pm 1),(2,\pm 1),(3,\pm 4),(4,\pm 7),(10,\pm 31),$$
$$(12,\pm 41),(20,\pm 89),(114,\pm 1217),(1274,\pm 45473),$$

od kojih zadnjih 6 parova zadovoljava naše uvjete.

Tvrdnja se lako provjeri za $x \leq 0$ (jer je tada očito $x \geq -2$), pa nadalje pretpostavljamo da je $x \geq 1$.

Promotrimo polje $\mathbb{K} = \mathbb{Q}(\vartheta)$, gdje je $\vartheta^3 - 4\vartheta + 1 = 0$. Uzmimo $\vartheta = \vartheta_1 \approx 0.2541$, $\vartheta_2 \approx -2.1149$, $\vartheta_3 \approx 1.8608$. Koristeći npr. PARI, mogu se dobiti

sljedeće informacije o polju $\mathbb{K}$: $O_{\mathbb{K}} = \mathbb{Z}[\vartheta]$, $h(\mathbb{K}) = 1$, fundamentalne jedinice su ϑ i $2 - \vartheta$ (općenito je broj fundamentalni jedinica (generiraju grupu jedinica, uz korijene od 1) jednak $s + t - 1$, gdje je s broj realnih korijena, a t broj parova konjugirano kompleksnih korijena minimalnog polinoma od ϑ; dakle, za stupanj 3 je $s + t - 1 = 1$ ili 2).

Jednadžbu (4.8) zapišimo u obliku

$$y^2 = (x - \vartheta)(x^2 + \vartheta x + (\vartheta^2 - 4)). \tag{4.9}$$

Lako se vidi da su faktori $x - \vartheta$ i $x^2 + \vartheta x + (\vartheta^2 - 4)$ relativno prosti. Odavde slijedi da se $x - \vartheta$ može zapisati u obliku

$$x - \vartheta = \pm\vartheta^i(2 - \vartheta)^j U^2, \quad U \in \mathbb{Z}[\vartheta], \ \ i, j \in \{0, 1\}.$$

Ista relacija vrijedi za svaki od konjugata ϑ_i. Za ϑ_1 vidimo (zbog $x \geq 1$ i $U \in \mathbb{R}$) da u (4.9) treba uzeti predznak $+$, a za ϑ_2 vidimo da mora biti $i = 0$. Stoga je ostalo promotriti dva slučaja: $j = 0$ i $j = 1$.

$\boxed{j = 0}$

Tražimo rješenje u obliku

$$x - \vartheta = (r + s\vartheta + t\vartheta^2)^2. \tag{4.10}$$

Izjednačavanjem koeficijenata uz potencije od ϑ u (4.10) dobivamo

$$s^2 + 4t^2 + 2rt = 0, \quad t^2 - 2rs - 8st = 1, \quad r^2 - 2st = x.$$

Vidimo da je s paran, t neparan, pa je i r paran. Stavimo $r = 2r_1$, $s = 2s_1$. Dobivamo: $4s_1^2 + 4t^2 + 4r_1t = 4s_1^2 + (2t + r_1)^2 - r_1^2 = 0$. Dakle, dobili smo Pitagorinu jednadžbu

$$(2s_1)^2 + (2t + r_1)^2 = r_1^2.$$

Zaključujemo da postoje $u, v \in \mathbb{Z}$ takvi da je

$$s_1 = uv, \quad 2t + r_1 = u^2 - v^2, \quad r_1 = \pm(u^2 + v^2).$$

Za predznak $+$ dobivamo $t = -v^2$, a za predznak $-$ dobivamo $t = u^2$. Uvrstimo li ove vrijednosti u drugu jednadžbu, dobivamo

$$v(v^3 + 8uv^2 - 8u^2v) = 1,$$

odnosno

$$u(u^3 + 8u^2v - 8uv^2) = 1.$$

Budući da su dobiveni homogeni polinomi reducibilni, ove jednadžbe je vrlo lako riješiti. Dobije se da je $(u, v) = (0, 1), (1, 1), (0, -1), (-1, -1)$ u prvom slučaju, a $(u, v) = (1, 0), (1, 1), (-1, 0), (-1, -1)$ u drugom. Odavde je

$(r,s,t) = (2,0,-1),(4,2,-1),(-2,0,1),(-4,2,1)$, pa je $x = 4, 20, 12$. Tako dobivamo cjelobrojne točke na eliptičkoj krivulji (4.8): $(4,\pm 7)$, $(20,\pm 89)$ i $(12,\pm 41)$.

$\boxed{j=1}$

Tražimo rješenje u obliku

$$x - \vartheta = (2-\vartheta)(r + s\vartheta + t\vartheta^2)^2. \tag{4.11}$$

Dobivamo jednadžbe

$$2s^2 + 9t^2 - 2rs + 4rt - 8st = 0, \quad r^2 + 4s^2 + 18t^2 - 4rs + 8rt - 18st = 1,$$
$$2r^2 + s^2 + 4t^2 + 2rt - 4st = x.$$

Iz prve jednadžbe imamo

$$0 = 2s^2 + 9t^2 - 2rs + 4rt - 8st = 2(s-2t)^2 + t^2 - 2r(s-2t).$$

Uz supstituciju $z = s - 2t$, dobivamo $t^2 + 2z^2 = 2rz$, tj. $t^2 = 2z(r-z)$.

Ako je z neparan, onda postoje $u, v \in \mathbb{Z}$ tako da je $z = u^2$, $r - z = 2v^2$, pa dobivamo

$$r = u^2 + 2v^2, \quad s = u^2 + 4uv, \quad t = 2uv,$$

što nam daje Thueovu jednadžbu

$$u^4 - 4u^3v - 12u^2v^2 + 4v^4 = 1. \tag{4.12}$$

Ako je z paran, onda postoje $u, v \in \mathbb{Z}$ tako da je $z = 2u^2$, $r - z = v^2$, pa dobivamo

$$r = 2u^2 + v^2, \quad s = 2u^2 + 4uv, \quad t = 4uv,$$

što nam daje Thueovu jednadžbu

$$4u^4 - 8u^3v - 12u^2v^2 + v^4 = 1. \tag{4.13}$$

Jednadžbe (4.12) i (4.13) su "prave" Thueove jednadžbe, tj. pripadni homogeni polinom je ireducibilan. Iz onog što smo do sada rekli o Thueovim jednadžbama, znamo da te jednadžbe imaju konačno mnogo rješenja, no još nismo dali algoritam za nalaženje svih rješenja. To ćemo napraviti u sljedećem poglavlju.

4.4 Algoritam za rješavanje Thueove jednadžbe

U Poglavlju 3.1 smo promatrali Thueovu jednadžbu oblika $F(x,y) = m$, gdje je $F(x,y) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n$ ireducibilan polinom nad $\mathbb{Q}$ stupnja $n \geq 3$. U prethodnom poglavlju smo vidjeli da se i nalaženja cjelobrojnih točaka na eliptičkim krivuljama može svesti na rješavanje Thueovih jednadžbi. Stoga je od velikog interesa postojanje algoritma za sistematsko rješavanje Thueovih jednadžbi. Mi ćemo prikazati jedan takav algoritam - de Wegerov algoritam iz 1989. godine.

Podijelit ćemo skup mogućih rješenja u četiri klase:

- jako mala rješenja: $|y| \leq Y_1$ - provjera "grubom silom";

- mala rješenja: $Y_1 < |y| \leq Y_2$ - odgovaraju konvergentama verižnog razlomka od ϑ_i;

- velika rješenja: $Y_2 < |y| \leq Y_3$ - eliminirat ćemo ih LLL-redukcijom;

- jako velika rješenja: $|y| > Y_3$ - dokazat ćemo da ne postoje pomoću linearnih formi u logaritmima.

Neka je $g(x) = F(x,1) = f_0(x-\vartheta_1)\cdots(x-\vartheta_n)$. Tada dobivamo jednadžbu $F(x,y) = f_0(x-\vartheta_1 y)\cdots(x-\vartheta_n y) = m$, koju ćemo promatrati u polju algebarskih brojeva $\mathbb{K} = \mathbb{Q}(\vartheta_i)$ (sva su ta polja $\mathbb{Q}$-izomorfna). Neka su $\vartheta_1, \ldots, \vartheta_s$ realni, a $\vartheta_{s+1} = \overline{\vartheta_{s+t+1}}, \ldots, \vartheta_{s+t} = \overline{\vartheta_{s+2t}}$ konjugirano kompleksni korijeni od $g(x)$. Vidjeli smo u 3.4, da je slučaj $s = 0$ vrlo jednostavan. Stoga ćemo u daljnjem pretpostaviti da je $s \geq 1$.

Uvedimo oznaku: $\beta_i = x - \vartheta_i y$, za $i = 1, \ldots, n$. Pretpostavimo da je $|f_0| = |m| = 1$. Tada iz $\beta_1\beta_2\cdots\beta_n = \pm 1$, zaključujemo da je β_i jedinica (invertibilni element) u prstenu $O_{\mathbb{K}}$. Po Dirichletovom teoremu o jedinicama znamo da je

$$b_i = \pm\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r},$$

gdje je $\varepsilon_1, \ldots, \varepsilon_r$ sustav fundamentalnih jedinica, te $r = s + t - 1$. U općem slučaju ćemo imati

$$b_i = \pm\mu_i\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r},$$

gdje μ_i pripada konačnom skupu M neasociranih elemenata iz $O_{\mathbb{K}}$ čija norma zadovoljava uvjet $f_0 \cdot N(\mu_i) = m$.

Neka je $|\beta_{i_0}| = \min\{|\beta_i| : 1 \leq i \leq n\}$. Tada je $i_0 \in \{1, \ldots, s\}$ i vrijedi

$$|\beta_{i_0}| \leq c_1|y|^{-(n-1)}, \tag{4.14}$$
$$|\beta_i| \geq c_2|y|, \quad i \neq i_0, \tag{4.15}$$

gdje je

$$c_1 = \frac{2^{n-1}|m|}{\min\{|g'(\vartheta_i)| : 1 \leq i \leq s\}},$$
$$c_2 = \frac{1}{2}\min\{|\vartheta_i - \vartheta_j| : 1 \leq i < j \leq n\}$$

(vidi dokaz Teoreme 3.5).

Lema 4.2. *Ako je* $|y| > Y_1 = (4c_1)^{\frac{1}{n-2}}$, *onda je* $\frac{x}{y}$ *konvergenta u razvoju u verižni razlomak broja* ϑ_{i_0}.

Dokaz: Imamo:

$$\left|\frac{x}{y}\right| = |\beta_{i_0}| \cdot |y|^{-1} \leq c_1 \cdot |y|^{-n} \leq \frac{1}{4} Y_1^{n-2} \cdot |y|^{-n} < \frac{1}{4y^2},$$

pa tvrdnja slijedi iz Legendreovog teorema o verižnim razlomcima. □

Promotrimo sada vezu između tri različita elementa $\beta_i = x - \vartheta_i y$, $\beta_j = x - \vartheta_j y$, $\beta_k = x - \vartheta_k y$. Eliminirajući x i y iz ove tri jednadžbe, dobivamo *Siegelov identitet*

$$\beta_i(\vartheta_j - \vartheta_k) + \beta_j(\vartheta_k - \vartheta_i) + \beta_k(\vartheta_i - \vartheta_j) = 0.$$

Za β_i ćemo uzeti β_{i_0}, dok ćemo ϑ_j i ϑ_k uzeti da budu realni (ako je $s \geq 3$), odnosno da je $\vartheta_k = \overline{\vartheta_j}$ (ako je $s = 1$). Detalje ćemo dati samo za prvi, realni, slučaj. Seigelov identitet možemo pisati i u obliku

$$\frac{\vartheta_{i_0} - \vartheta_j}{\vartheta_{i_0} - \vartheta_k} \cdot \frac{\beta_k}{\beta_j} - 1 = -\frac{\vartheta_k - \vartheta_j}{\vartheta_k - \vartheta_{i_0}} \cdot \frac{\beta_{i_0}}{\beta_j}. \tag{4.16}$$

Identitet (4.16) će nam dati vezu s linearnim formama u logaritmima. Definirajmo:

$$\Lambda = \ln\left(\frac{\vartheta_{i_0} - \vartheta_j}{\vartheta_{i_0} - \vartheta_k} \cdot \frac{\beta_k}{\beta_j}\right).$$

Nije teško vidjeti da je izraz pod logaritmom pozitivan.

Lema 4.3. *Neka je*

$$c_3 = \max\left\{\left|\frac{\vartheta_{i_1} - \vartheta_{i_2}}{\vartheta_{i_1} - \vartheta_{i_3}}\right| : i_1 \neq i_2 \neq i_3 \neq i_1\right\},$$
$$Y_2 = \max\left\{Y_1, \left(\frac{2c_1c_3}{c_2}\right)^{\frac{1}{n}}\right\}.$$

Ako je $|y| > Y_2$, *onda vrijedi*

$$|\Lambda| < \frac{1.39c_1c_3}{c_2}|y|^{-n}.$$

Dokaz: Lijeva strana od (4.16) je jednaka $e^\Lambda - 1$. Iz definicije od c_3, te nejednakosti (4.14) i (4.15), imamo

$$e^\Lambda - 1 < c_3 \cdot \frac{c_1|y|^{-(n-1)}}{c_2|y|} = \frac{c_1c_3}{c_2}|y|^{-n} < \frac{1}{2}.$$

Stoga je

$$|\Lambda| \leq 2\ln 2 \cdot |e^\Lambda - 1| \leq \frac{1.39c_1c_3}{c_2}|y|^{-n}.$$

□

Sjetimo se da je $\beta_i = \mu_i(\varepsilon_1^{(i)})^{a_1}\cdots(\varepsilon_r^{(i)})^{a_r}$. Stoga (4.16) postaje

$$\frac{\vartheta_{i_0}-\vartheta_j}{\vartheta_{i_0}-\vartheta_k}\cdot\frac{\mu_k}{\mu_j}\cdot\prod_{i=1}^{r}(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}})^{a_i}-1=-\frac{\vartheta_k-\vartheta_j}{\vartheta_k-\vartheta_{i_0}}\cdot\frac{\mu_{i_0}}{\mu_j}\cdot\prod_{i=1}^{r}(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}})^{a_i}.$$

U realnom slučaju naša linearna forma Λ je

$$\ln\left|\frac{\vartheta_{i_0}-\vartheta_j}{\vartheta_{i_0}-\vartheta_k}\cdot\frac{\mu_k}{\mu_j}\right|+\sum_{i=1}^{r}a_i\cdot\ln\left|\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right|.$$

Neka je $A=\max\{|a_i|\,:\,i=1,\ldots,r\}$. Želimo dobiti gornju ogradu za A. Uspijemo li naći relativno malu ogradu za A, onda ćemo moći ispitati sve mogućnosti za $\mu\cdot\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}$, provjeriti koja od njih ima oblik $x-\vartheta y$, te konačno provjeriti je li $F(x,y)=m$.

Najprije ćemo prikazati kako se dobije gornja ograda za A u ovisnosti o y. Za $I=\{i_1,\ldots,i_r\}\subset\{1,\ldots,s+t\}$, definiramo matricu $U_I=(\ln|\varepsilon_l^{(i_l)}|)_{1\le i,l\le r}$. Primijetimo da iz $\beta=\mu\cdot\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}$, slijedi

$$U_I\begin{bmatrix}a_1\\ \vdots\\ a_r\end{bmatrix}=\begin{bmatrix}\ln\left|\frac{\beta^{(i_1)}}{\mu^{(i_1)}}\right|\\ \vdots\\ \ln\left|\frac{\beta^{(i_r)}}{\mu^{(i_r)}}\right|\end{bmatrix}.$$

Analizirajući ovu relaciju, može se dobiti sljedeća nejednakost

$$A<c_5\ln(c_4|y|). \tag{4.17}$$

Konstante c_4 i c_5 su definirane na sljedeći način:

$$\begin{aligned}U_I^{-1}&=[u_{il}],\\ N(U_I^{-1})&=\max\{\sum_{i=1}^{r}|u_{il}|\,:\,i=1,\ldots,r\},\\ \mu_-&=\min\{|\mu_i|\,:\,\mu\in M,\ i=1,\ldots,n\},\\ \mu_+&=\max\{|\mu_i|\,:\,\mu\in M,\ i=1,\ldots,n\},\\ c_4&=\frac{\frac{1}{2}+\max\{|\vartheta_{i_1}-\vartheta_{i_2}|\,:\,1\le i_1<i_2\le n\}}{\mu_-},\\ c_5&=\min\{(n-1)\cdot\min_I N(U_I^{-1}),\max_I N(U_I^{-1})\}.\end{aligned}$$

Tada se može pokazati da (4.17) vrijedi čim je $|y|>\max\{Y_1,2|m|^{\frac{1}{n}},\frac{\mu_+}{c_2}\}$.

Kombinirajući Lemu 4.3 i (4.17), dobivamo nejednakost

$$|\Lambda|<c_6\cdot e^{-\frac{n}{c_3}A}, \tag{4.18}$$

gdje je $c_6 = \frac{1.39c_1c_3c_4^n}{c_2}$. S druge strane, iz Baker-Wüstholzovog teorema primjenjenog na formu Λ, dobivamo nejednakost oblika

$$|\Lambda| > e^{-c_7(\ln A + c_8)}. \tag{4.19}$$

Usporedbom nejednakosti (4.18) i (4.19), dobivamo (vrlo veliku) gornju ogradu za A. Potom tu veliku ogradu smanjujemo primjenom LLL-redukcije na nejednakost (4.18).

Primjer 4.4. *Da bi dovršili Primjer 4.3 i našli sve trokutaste brojeve koji su jednaki produktu tri uzastopna prirodna broja, trebamo još provjeriti da su sva rješenja Thueove jednadžbe*

$$x^4 - 4x^3y - 12x^2y^2 + 4y^4 = 1$$

dana sa $(x, y) = (1, 0)$, $(-1, 0)$, *a sva rješenja Thueove jednadžbe*

$$x^4 - 12x^3y - 8xy^3 + 4y^4 = 1$$

sa $(x, y) = (\pm 1, 0)$, $(1, -1)$, $(-1, 1)$, $(1, 3)$, $(-1, -3)$, $(3, -1)$, $(-3, 1)$.

Rješenje: Promatraju se polja algebarski brojeva $\mathbb{Q}(\varphi)$, gdje je $\varphi^4 - 4\varphi^3 - 12\varphi^2 + 4 = 0$, te $\mathbb{Q}(\vartheta)$, gdje je $\vartheta^4 - 12\vartheta^2 - 8\vartheta + 4 = 0$. No, uočimo da je $\mathbb{Q}(\varphi) = \mathbb{Q}(\vartheta)$, jer je $\varphi = \frac{2}{\vartheta}$. Koristeći programski paket PARI/GP nalazimo da je sustav fundamentalnih jedinica u $\mathbb{Q}(\vartheta)$:

$$\varepsilon_1 = 1 + \vartheta, \quad \varepsilon_2 = 3 + \vartheta, \quad \varepsilon_3 = \frac{1}{2}\vartheta^2.$$

Primjenom de Wegerovog algoritma, dobivamo najprije za se za veličine Y_1 i Y_3 može uzeti $Y_1 = 1$, $Y_2 = 3$. Potom dobivamo nejednakost koja odgovara nejednakosti (4.18):

$$|\Lambda| < k_2 \cdot e^{-k_3 A}, \tag{4.20}$$

gdje je

$$k_2 = 6.39 \cdot 10^4, \quad k_3 = 3.303.$$

S druge strane se i Baker-Wüstholzovog teorema dobiva nejednakost

$$|\Lambda| > e^{-k_4 \ln A}, \tag{4.21}$$

gdje je $k_4 = 5.87 \cdot 10^{21}$. Usporedbom (4.20) i (4.21), dobivamo da je $A < 1.44 \cdot 10^{23}$. Primjenom nekoliko koraka LLL-redukcije, ova je velika gornja ograda za A može reducirati do $A \leq 6$.

Ostaje provjeriti koji od $13^3 = 2197$ brojeva

$$\pm\varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}, \quad |a_i| \leq 6,$$

imaju oblik $x - y\vartheta$ ili $x - y\varphi$, $x, y \in \mathbb{Z}$. Posebno treba ispitati i slučaj $|y| \leq 3$, jer su gornje ocjene dobivene uz pretpostavku da je $|y| > Y_2$. Dobije se da su rješenja promatranih Thueovih jednadžbi upravo ona gore navedena. $\diamondsuit$

4.5 Racionalne točke na eliptičkim krivuljama

Dosad smo promatrali cjelobrojne točke na eliptičkim krivuljama, tj. promatrali smo eliptičke krivulje nad prstenom $\mathbb{Z}$. Sada ćemo nešto reći o eliptičkim krivuljama nad poljem $\mathbb{Q}$. Budući da je $\mathbb{Q}$ polje, na skupu racionalnih točaka na eliptičkoj krivulji moguće je uvesti operaciju zbrajanja točaka, uz koju taj skup postaje Abelova grupa. Promotrimo najprije eliptičke krivulje, tj. skup točaka koje zadovoljavaju jednadžbu oblika $y^2 = x^3 + ax + b$, nad poljem $\mathbb{R}$. Tu krivulju možemo nacrtati u ravnini i ona ima jedan od dva karakteristična oblika (u ovisnosti o tome ima li polinom $f(x) = x^3 + ax + b$ jednu ili tri realne nultočke). Zbrajanje točaka se može definirati "geometrijski": pravac kroz točke P i Q siječe eliptičku krivulju u još jednoj točki R; točka $P + Q$ se definira kao osnosimetrična točka točki R s obzirom na os x (kod $P + P$ povlačimo tangentu kroz točku P, te dalje postupamo na isti način). Neutralni element je "točka u beskonačnosti" (kroz nju prolazi svaki "vertikalni pravac").

Točka u beskonačnosti se pojavljuje prirodno ukoliko eliptičku krivulju prikažemo u projektivnoj ravnini. *Projektivnu ravninu* $\mathbb{P}^2(\mathbb{R})$ dobijemo tako da na skupu $\mathbb{R}^3 \setminus \{(0,0,0)\}$ uvedemo relaciju ekvivalencije $(X, Y, Z) \sim (kX, kY, kZ)$, $k \in \mathbb{R}$, $k \neq 0$. Ako u (afinoj) jednadžbi eliptičke krivulje uvedemo supstituciju $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, dobivamo projektivnu jednadžbu

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Ako je $Z \neq 0$, onda klasa ekvivalencije od (X, Y, Z) ima reprezentant $(x, y, 1)$, pa tu klasu možemo identificirati s (x, y). Međutim, postoji i jedna klasa ekvivalencije koja sadrži točke za koje je $Z = 0$. Ona ima reprezentant $(0, 1, 0)$ i tu klasu identificiramo s točkom u beskonačnosti $\mathcal{O}$.

Naravno da se geometrijska definicija zbrajanja točaka iz $E(\mathbb{R})$ može opisati i eksplicitnim formulama za koordinate zbroja točaka. Tako dobivene formule onda mogu poslužiti za definiciju zbrajanja točaka na eliptičkoj krivulji nad proizvoljnim poljem $\mathbb{K}$ (uz malu modifikaciju ako je karakteristika polja 2 ili 3). Navedimo sada te formule.

Neka je $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Tada je

1) $-\mathcal{O} = \mathcal{O}$;
2) $-P = (x_1, -y_1)$;
3) $\mathcal{O} + P = P$;
4) ako je $Q = -P$, onda je $P + Q = \mathcal{O}$;
5) ako je $Q \neq -P$, onda je $P + Q = (x_3, y_3)$, gdje je

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = -y_1 + \lambda(x_1 - x_3),$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1, \\ \frac{3x_1^2 + a}{2y_1}, & \text{ako je } x_2 = x_1. \end{cases}$$

Broj λ je koeficijent smjera pravca kroz P i Q, odnosno tangente u točki P u slučaju $P = Q$.

Pokazuje se da je $(E(\mathbb{K}), +)$ Abelova grupa. Sva svojstva Abelove grupe su evidentna, osim asocijativnosti čiji je dokaz nešto kompliciraniji (asocijativnost se može dokazati sredstvima projektivne geometrije, kompleksne analize ili direktnim računom).

Najvažija činjenica o eliptičkim krivuljama nad $\mathbb{Q}$ jest Mordell-Weilov teorem.

Teorem 4.3 (Mordell-Weil)**.** *$E(\mathbb{Q})$ je konačno generirana Abelova grupa.*

Mordell-Weilov teorem nam, drugim riječima, kaže da postoji konačan skup racionalnih točaka $P_1, \ldots, P_k$ na E iz kojih se sve ostale racionalne točke na E mogu dobiti povlačeći sekante i tangente. Dva osnovna koraka u dokazu Teorema 4.3 su

- dokaz da je indeks $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ konačan;
- svojstva visine h, definirane sa $h(P) = \ln H(x)$, gdje je $P = (x, y)$ i $H(\frac{m}{n}) = \max\{|m|, |n|\}$.

Kako je svaka konačno generirana Abelova grupa izomorfna produktu cikličkih grupa, dobivamo sljedeću neposrednu posljedicu Mordell-Weilova teorema.

Korolar 4.1.

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

Podgrupa $E(\mathbb{Q})_{\text{tors}}$ od $E(\mathbb{Q})$ koja se sastoji od svih točaka konačnog reda naziva se *torzijska grupa* od E, a nenegativni cijeli broj r se naziva *rang* od E i označava se s $\text{rank}(E)$. Korolar nam kaže da postoji r racionalnih točaka $P_1, \ldots, P_r$ na krivulji E sa svojstvom da se svaka racionalna točka P na E može prikazati u obliku

$$P = T + [m_1]P_1 + \cdots + [m_r]P_r,$$

gdje je T neka točka konačnog reda, a $m_1, \ldots, m_r$ cijeli brojevi. Ovdje $[m_1]P_1$ označava sumu $P_1 + \cdots + P_1$ od m_1 pribrojnika.

Postavlja se pitanje koje sve vrijednosti mogu poprimiti $E(\mathbb{Q})_{\text{tors}}$ i $\text{rank}(E)$. Nadalje, pitanje je kako ih izračunati za konkretnu krivulju E. Pokazuje se da je puno lakše dati odgovore na ova pitanja za torzijsku grupu, nego za rang.

Mazur je 1978. godine dokazao da postoji točno 15 mogućih torzijskih grupa (do na izomorfizam). To su grupe:

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z}, &\quad \text{za } n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, &\quad \text{za } n = 2, 4, 6, 8. \end{aligned}$$

Točke reda 2 su upravo točke s y-koordinatom jednakom 0. Možemo imati 0, 1 ili 3 takve točke, što ovisi o broju racionalnih nultočaka polinoma $x^3 + ax + b$. Te točke, zajedno s točkom $\mathcal{O}$, čine podgrupu od $E(\mathbb{Q})_{\text{tors}}$ koja je ili trivijalna ili izomorfna $\mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ostale točke konačnog reda možemo naći pomoću sljedećeg teorema.

Teorem 4.4 (Lutz-Nagell)**.** *Neka je eliptička krivulja E zadana jednadžbom*

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}.$$

Ako je $P = (x, y) \in E(\mathbb{Q})_{tors}$, onda su x, y cijeli brojevi, te vrijedi da je ili $y = 0$ ili y^2 dijeli diskriminantu D.

Teorem 4.4 nećemo dokazivati, no recimo kako drugi dio teorema slijedi iz prvog. Ako je P točka konačnog reda, onda i $[2]P$ također ima konačni red, pa je po prvom dijelu teorema $x([2]P) \in \mathbb{Z}$. No, iz eksplicitnih formula za $[2]P$, imamo da je $x([2]P) = \frac{\varphi(x)}{4f(x)}$, gdje je φ polinom stupnja 4. Može se pokazati da postoje polinomi F, Φ, $\operatorname{st} F = 3$, $\operatorname{st} \Phi = 2$, takvi da vrijedi

$$F(x)f(x) + \Phi(x)\varphi(x) = D.$$

Sada da je jasno da $y^2 = f(x)$ dijeli i $f(x)$ i $\varphi(x)$, pa dijeli i D.

Pitanja koja se tiču ranga su puno teža, a zadovoljavajući odgovori još uvijek nisu poznati. Vjeruje se da rang može biti proizvoljno velik, tj. da za svaki $M \in \mathbb{N}$ postoji eliptička krivulja nad $\mathbb{Q}$ takva da je $\operatorname{rank}(E) \geq M$. No, danas se tek zna da postoji eliptička krivulja ranga ≥ 28. Tu je krivulju 2006. godine pronašao Noam Elkies. Nadalje, nije poznat niti jedan algoritam na računanje ranga koji bezuvjetno radi. Ipak, pokazat ćemo jednu metodu za računanje ranga koja je ponekad uspješna (vidjet ćemo o čemu ovisi "uspješnost").

Pretpostavimo da E ima točku reda 2. U tom slučaju je računanje ranga obično lakše nego u općem slučaju. Opisat ćemo metodu za računanje ranga koja se naziva "silazak pomoću 2-izogenije". Ako krivulja E dana jednadžbom $y^2 = f(x)$ ima točku reda 2, onda polinom $f(x)$ ima racionalnu nultočku. Bez smanjenja općenitosti možemo pretpostaviti da je ta racionalna nultočka upravo jednaka 0. To znači da E ima jednadžbu oblika

$$y^2 = x^3 + ax^2 + bx.$$

Za krivulju E' koja ima jednadžbu

$$y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$$

kažemo da je 2-izogena krivulji E. Općenito, izogenijom zovemo homomorfizam između dvije eliptičke krivulje koji je dan pomoću racionalnih funkcija.

U našem slučaju, radi se o preslikavanju $\varphi : E \to E'$, $\varphi(P) = (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2})$ za $P = (x, y) \neq \mathcal{O}, (0, 0)$, a $\varphi(P) = \mathcal{O}$ inače. Analogno se može definirati $\psi : E' \to E$. Vrijedi $\psi \circ \varphi(P) = [2]P$ i ova dva preslikavanja se koriste u prvom koraku dokaza Mordell-Weilovog teorema.

Zapišimo x i y u obliku $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$, te ih uvrstimo u jednadžbu od E. Dobivamo:

$$n^2 = m(m^2 + ame^2 + be^4).$$

Stavimo $b_1 = \pm(m, b)$, gdje je (m, b) najveći zajednički djelitelj od m i b, s time da je predznak odabran tako da je $mb_1 > 0$. Tada je $m = b_1 m_1$, $b = b_1 b_2$, $n = b_1 n_1$, pa dobivamo

$$n_1^2 = m_1(b_1 m_1^2 + am_1 e^2 + b_2 e^4).$$

Budući da su faktori na desnoj strani posljednje jednadžbe relativno prosti, zaključujemo da postoje cijeli brojevi M i N tako da vrijedi $m_1 = M^2$, $b_1 m_1^2 + am_1 e^2 + b_2 e^4 = N^2$, te tako konačno dobivamo jednadžbu

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4 \tag{4.22}$$

u kojoj su nepoznanice M, e i N. Pritom moraju biti ispunjeni sljedeći uvjeti: $(M, e) = (N, e) = (b_1, e) = (b_2, M) = (M, N) = 1$.

Rang eliptičke krivulje E može se izračunati na sljedeći način. Za svaku faktorizaciju $b = b_1 b_2$, gdje je b_1 kvadratno slobodan cijeli broj, napišemo jednadžbu (4.22). Pokušamo odrediti ima li ta jednadžba netrivijalnih cjelobrojnih rješenja (uočimo da za ovakve jednadžbe ne mora vrijediti lokalno-globalni princip Hassea i Minkowskog, što znači da zapravo nemamo algoritam koji bi sa sigurnošću odgovorio na ovo pitanje). Svako rješenje (M, e, N) jednadžbe (4.22) inducira točku na krivulji E s koordinatama $x = \frac{b_1 M^2}{e^2}$, $y = \frac{b_1 MN}{e^3}$. Neka je r_1 broj faktorizacija za koje pripadna jednadžba (4.22) ima rješenja, te neka je r_2 broj definiran na isti način za krivulju E'. Tada postoje nenegativni cijeli brojevi e_1 i e_2 takvi da je $r_1 = 2^{e_1}$, $r_2 = 2^{e_2}$ i pritom vrijedi da je

$$\operatorname{rank}(E) = e_1 + e_2 - 2.$$

U slučaju kada je rang jednak 0 (i mi to uspijemo dokazati), pomoću Lutz-Nagellovog teorema mogu se naći sve racionalne, pa onda i sve cjelobrojne točke na toj eliptičkoj krivulji.

U općem slučaju se primjenom tzv. eliptičkih logaritama može dobiti ocjena $N \leq N_0$ za $N = \max\{|n_1|, \ldots, |n_r|\}$ u prikazu cjelobrojne točke $P = T + [n_1]P_1 + \cdots + [n_r]P_r$. Potom se ova ograda, na standardan način, može smanjiti pomoću LLL-algoritma. No, za ovu metodu je nužno poznavati i rang i generatore $P_1, \ldots, P_r$, što može biti vrlo težak problem.

Primjer 4.5. *Promotrimo skup* $\{1,2,5\}$*. On ima svojstvo slično onomu iz definicije Diofantovih trojki. Naime,* $1\cdot 2-1$*,* $1\cdot 5-1$ *i* $2\cdot 5-1$ *su potpuni kvadrati. Postavlja se pitanje, može li se ovaj skup proširiti do četvorke s istim svojstvom, tj. postoji li* $x\in\mathbb{Z}$ *takav da su*

$$1\cdot x-1,\quad 2\cdot x-1,\quad 5\cdot x-1$$

kvadrati cijelih brojeva. Pokazat ćemo da je jedino rješenje $x=1$*, pa jer je* $1\in\{1,2,5\}$*, to će značiti da se skup* $\{1,2,5\}$ *ne može proširiti to četvorke s traženim svojstvom (*$D(-1)$*-četvorke). To bismo mogli dokazati analogno kao u slučaju Diofantove trojke* $\{1,3,8\}$*, tj. rješavanjem sustava pellovskih jednadžbi Bakerovom metodom. No, mi ćemo ovdje riješiti i nešto općenitiji problem nalaženja svih cjelobrojnih (čak svih racionalnih) točaka na eliptičkoj krivulji*

$$y^2=(x-1)(2x-1)(5x-1). \tag{4.23}$$

Rješenje: Dovedimo najprije krivulju u Weierstrassov oblik, množenjem obje strane jednadžbe s 10^2 i supstitucijom $10y\mapsto y$, $10x\mapsto x$. Dobivamo

$$y^2=x^3-17x^2+80x-100.$$

Translacijom $x\mapsto x+5$, dovedimo krivulju u oblik prikladan za računanje ranga:

$$E\,;\quad y^2=x^3-2x^2-15x.$$

Njezina 2-izogena krivulja je

$$E'\,:\quad y^2=x^3+4x^2+64x.$$

Za krivulju E, mogućnosti za broj b_1 su ±1, ±3, ±5, ±15. Pripadne diofantske jednadžbe su $N^2=M^4-2M^2e^2-15e^4$, $N^2=-M^4-2M^2e^2+15e^4$, $N^2=3M^4-2M^2e^2-5e^4$, $N^2=-3M^4-2M^2e^2+5e^4$, $N^2=5M^4-2M^2e^2-3e^4$, $N^2=-5M^4-2M^2e^2+3e^4$, $N^2=15M^4-2M^2e^2-e^4$, $N^2=-15M^4-2M^2e^2+e^4$. Zbog simetričnosti, dovoljno je ispitati rješivost prve četiri jednadžbe. Prva jednadžba ima rješenje $M=1,e=0,N=1$, a četvrta ima rješenje $M=1$, $e=1$, $N=0$. Druga jednadžba je ekvivalentna sa $N^2=(3e^2-M^2)(5e^2+M^2)$. Lako se vidi da je $(3e^2-M^2,5e^2+M^2)\in\{1,2\}$, pa imamo dvije mogućnosti: ili su oba faktora kvadrati ili su oba dvostruki kvadrati. No, $3e^2-M^2=s^2$ je nemoguće modulo 3, jer je $(\frac{-1}{3})=-1$, dok je $5e^2+M^2=2t^2$ nemoguće modulo 5, jer je $(\frac{2}{5})=-1$. Treća jednadžba je ekvivalentna sa $N^2=(M^2+e^2)(3M^2-5e^2)$. Ponovo imamo iste dvije mogućnosti za faktore u zadnjem izrazu, i ponovo obje mogućnosti otpadaju: $3M^2-5e^2=t^2$ je nemoguće modulo 5, jer je $(\frac{3}{5})=-1$, dok je $3M^2-5e^2=2t^2$ nemoguće modulo 8, jer je $3M^2-5e^2\equiv 6 \pmod 8$, a $2t^2\equiv 2 \pmod 8$. Dakle, $e_1=2$.

Za E' je $b_1' \in \{\pm 1, \pm 2\}$, pa su pripadne diofantske jednadžbe $N^2 = M^4+4M^2e^2+64e^4$, $N^2 = -M^4+4M^2e^2-64e^4$, $N^2 = 2M^4+4M^2e^2+32e^4$ i $N^2 = -2M^4+4M^2e^2-32e^4$. Prva jednadžba ima rješenje $M = 1$, $e = 0$, $N = 1$. Druga i četvrta jednadžba su ekvivalentna s $N^2 = -(M^2 - 2e^2)^2 - 60e^4$, odnosno $N^2 = -2(M^2 - e^2)^2 - 30N^2$, te očito nemaju netrivijalnih rješenja. Treća jednadžba je ekvivalentna sa $2 \cdot (N/2)^2 = (M^2 + e^2)^2 + 15e^4$, te nema rješenja modulo 5, jer je $(\frac{2}{5}) = 1$. Dakle, $e_2 = 0$.

Zaključak: $\operatorname{rank} E = 2 + 0 - 2 = 0$.

Dakle, treba još samo naći torzijske točke na E. Ona ima tri točke reda 2: $(0,0)$, $(-3,0)$, $(5,0)$. Za ostale torzijske točke (x,y) bi trebalo vrijediti $y^2|D = 14400$, tj. $y|120$. Provjeravamo imaju li jednadžbe $x(x-3)(x+5) = 1, 4, 9, \ldots, 144000$ cjelobrojnih rješenja, i vidimo da nemaju (alternativno možemo uočiti da je $\#E(\mathbb{F}_7) = 4$). Dakle, jedine racionalne točke na E su $(0,0)$, $(-3,0)$, $(5,0)$, pa su jedine racionalne točke na krivulji (4.23): $\mathcal{O}$, $(1,0)$, $(\frac{1}{2},0)$, $(\frac{1}{5},0)$. Stoga je jedini cijeli broj x sa svojstvom da su $1 \cdot x - 1$, $2 \cdot x - 1$ i $5 \cdot x - 1$ potpuni kvadrati, broj $x = 1$. ♢

Napomena 4.3. Krivulja

$$y^2 = (x+1)(3x+1)(8x+1)$$

ima rang jednak 1, pa se Diofantova trojka $\{1, 3, 8\}$ može proširiti s beskonačno mnogo racionalnih brojeva (npr. s $x = \frac{777480}{8288641}$).