Sveučilište u Zagrebu
PMF – Matematički odjel

Vinko Petričević

KONGRUENTNI BROJEVI I ELIPTIČKE KRIVULJE

Diplomski rad

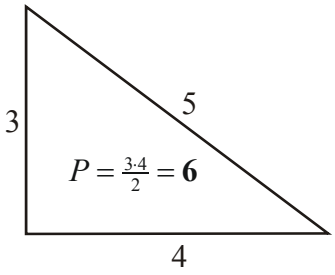
Voditelj rada:
prof.dr.sc. Andrej Dujella

Zagreb, listopad 2003.

Sadržaj

1. Uvod

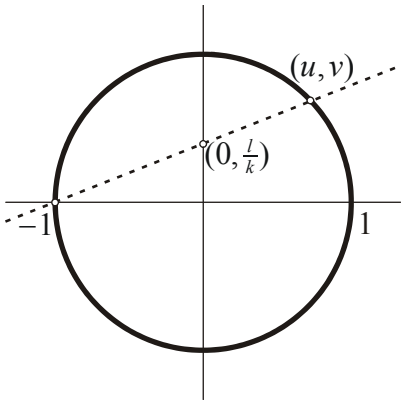
Za prirodan broj n kažemo da je **kongruentan** ako postoji pravokutni trokut površine n kojem su duljine svih triju stranica racionalni brojevi. Na primjer, 6 je kongruentan broj, jer je trokut sa stranicama 3–4–5 pravokutan, a njegova površina je 6 (Slika 1).



Slika 1

Pravokutne trokute s cjelobrojnim stranicama $a,\ b,\ c$ ("Pitagorine trojke") su još u drevnoj Grčkoj proučavali Pitagora, Euklid, Diofant i mnogi drugi. Njihovo je glavno otkriće bilo jednostavan način generiranja svih takvih trokuta. Naime, uzmimo bilo koja dva prirodna broja k i l, $k > l$, i povucimo pravac u xy-ravnini točkom $(-1,0)$, s koeficijentom smjera $\frac{l}{k}$. Neka je (u,v) druga točka presjeka tog pravca i jedinične kružnice (Slika 2). Onda je $u = \frac{k^2-l^2}{k^2+l^2}$ i $v = \frac{2kl}{k^2+l^2}$. Nije teško vidjeti da su tada cijeli brojevi $a = k^2 - l^2,\ b = 2kl,\ c = k^2 + l^2$ stranice pravokutnog trokuta. Činjenica $a^2 + b^2 = c^2$ slijedi iz $u^2 + v^2 = 1$ (točka (u,v) je na jediničnoj kružnici). Ako k i l prolaze svim mogućim prirodnim brojevima $k > l$, dobiju se sve moguće Pitagorine trojke (za dokaz vidi Lemu prije Propozicije 3).

Iako je proučavanje brojeva n koji se pojavljuju kao površine racionalnih pravokutnih trokuta interesiralo Grke u specijalnim slučajevima, čini se da su kongruentne brojeve prvi sistematski proučavali arapski matematičari desetog stoljeća. Arapi su taj problem preformulirali u ekvivalentan oblik: Da li je za dani n moguće naći racionalni broj x, takav da su i $x^2 + n$ i $x^2 - n$ kvadrati racionalnih brojeva? (Ekvivalentnost tih dvaju oblika bila je poznata i Grcima i Arapima; za dokaz te činjenice, vidi Propoziciju 1.)



Slika 2

Otada su mnogi slavni matematičari posvetili priličan trud nekim specijalnim slučajevima. Na primjer, Euler je prvi dokazao da je 7 kongruentan broj. Fermat je dokazao da 1 nije (taj je rezultat u biti ekvivalentan Velikom Fermatovom teoremu[1] za eksponent 4, tj. činjenici da jednadžba $a^4 + b^4 = c^4$ nema

[1] Veliki Fermatov teorem kaže da za $n \geq 3$ jednadžba $a^n + b^n = c^n$ nema rješenja u prirodnim brojevima.

netrivijalna cjelobrojna rješenja). Da je 5 kongruentan, znao je i Fibonacci (Slika 3).

Naposljetku je postalo jasno da brojevi $1, 2, 3, 4, 8, 9, 10$ nisu kongruentni, dok $5, 6, 7$ jesu. Pa ipak, činilo se beznadno tražiti direktan kriterij koji će reći dali je dani broj n kongruentan. Glavni je napredak u dvadesetom stoljeću bio stavljanje tog problema u kontekst aritmetičke teorije eliptičkih krivulja. U tom je kontekstu J. Tunnell 1983. dokazao svoj znameniti teorem. Dio tog teorema kaže:

Teorem (Tunnell). *Neka je n kvadratno slobodan prirodan broj, te neka je $k = 1$ ako je n neparan, a $k = 2$ ako je n paran. Razmotrimo sljedeća dva uvjeta:*

(A) n je kongruentan;

(B) broj trojki cijelih brojeva (x, y, z) koje zadovoljavaju $2kx^2 + y^2 + 8z^2 = \frac{n}{k}$ je točno dvostruko veći od broja trojki koje zadovoljavaju $2kx^2 + y^2 + 32z^2 = \frac{n}{k}$.

Tada (A) povlači (B); i ako je slabi oblik takozvane Birch-Swinnerton-Dyerove slutnje[2] točan, tada i (B) povlači (A). ■

Tunnelov teorem daje gotovo potpuni odgovor na prastari problem: Naći jednostavan kriterij koji određuje da li je ili nije dani cijeli broj n površina nekog pravokutnog trokuta, čije stranice su racionalni brojevi.

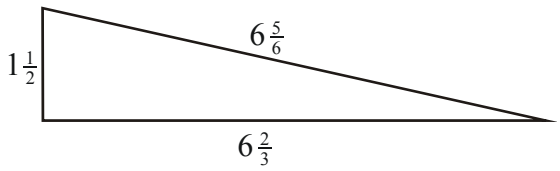
Neki dijelovi tog teorema nadilaze naše domete, pa ćemo se bazirati na vezu kongruentnih brojeva i određene porodice eliptičkih krivulja, te dati definicije nekih osnovnih pojmova i svojstava eliptičikih krivulja.

[2] Birch-Swinnerton-Dyerova slutnja povezuje broj generatora (rang) eliptičke krivulje nad poljem $\mathbb{Q}$ s brojem točaka na toj krivulji kad se ona promatra nad konačnim poljem $\mathbb{F}_p$. To je jedan od sedam tzv. Milenium Prize Problems.

2. Kongruentni brojevi

Za pozitivan racionalan broj r kažemo da je **kongruentan**, ako je jednak površini nekog pravokutnog trokuta s racionalnim stranicama.

Pretpostavimo da je r kongruentan, i da su $a, b, c \in \mathbb{Q}$ stranice pravokutnog trokuta površine r. Za svaki $r \in \mathbb{Q},\ r > 0$ može se naći $s \in \mathbb{Q}$, takav da je $s^2 r$ kvadratno slobodan prirodan broj. Trokut sa stranicama $sa,\ sb,\ sc$ ima površinu $s^2 r$. Dakle, bez smanjenja općenitosti možemo podrazumijevati da je r kvadratno slobodan prirodan broj. U daljnjem tekstu ćemo to i podrazumijevati.



Slika 3

Uočimo da definicija kongruentnosti ne zahtijeva da stranice trokuta budu cjelobrojne, samo racionalne. Dok je 6 najmanja površina pravokutnog trokuta cjelobrojnih stranica, moguće je naći pravokutni trokut racionalnih stranica površine 5 (na primjer, $\frac{3}{2}, \frac{20}{3}, \frac{41}{6}$ – Slika 3). Pokazuje se da je 5 najmanji kongruentni broj. Uočimo da je 7 kongruentan broj zbog pravokutnog trokuta $\frac{24}{5}, \frac{35}{12}, \frac{337}{60}$.

Postoji jednostavni algoritam, koji koristeći Pitagorine trojke generira sve kongruentne brojeve. Na nesreću, za dani n, ne može se reći koliko dugo moramo čekati, da utvrdimo njegovu kongruentnost (ako nije utvrđeno, ne znamo da li to znači da n nije kongruentan ili nismo dovoljno dugo čekali. Na primjer, najjednostavniji racionalni pravokutni trokut površine 157 ima stranice $\frac{6\,803\,298\,487\,826\,435\,051\,217\,540}{411\,340\,519\,227\,716\,149\,383\,203}, \frac{411\,340\,519\,227\,716\,149\,383\,203}{21\,666\,555\,693\,714\,761\,309\,610}, \frac{224\,403\,517\,704\,336\,969\,924\,557\,513\,090\,674\,863\,160\,948\,472\,041}{8\,912\,332\,268\,928\,859\,588\,025\,535\,178\,967\,163\,570\,016\,480\,830}$). S praktičnog gledišta, ljepota Tunnellovog teorema je u tome štos e njegov uvjet (B) može vrlo jednostavno i brzo provjeriti efektivnim algoritmom. Stoga taj teorem olakšava problem kongruentnog broja, tj. problem nalaženja provjerljivog kriterija da li je n kongruentan broj. Bolje rečeno "skoro olakšava", jer u jednom smjeru kriterij vrijedi uvijek, a u drugom samo ako prihvatimo slutnju o eliptičkim krivuljama.

Pretpostavimo da su a, b, c stranice pravokutnog trokuta površine n. To znači: $a^2 + b^2 = c^2$, i $\frac{1}{2}ab = n$. Algebarski govoreći, uvjet da je n kongruentan znači da te dvije jednadžbe imaju zajednička rješenja $a, b, c \in \mathbb{Q}$. U sljedećoj propoziciji izvodi se alternativni uvjet da je n kongruentan broj. U listi trokuta sa stranicama a, b, c ne želimo shvaćati trokute a, b, c i b, a, c kao različite. Zato odredimo uređaj tako da je $a < b < c$ (c je hipotenuza).

Propozicija 1. *Neka je* n *čvrst kvadratno slobodan prirodan broj. Neka* a, b, c, x *označava pozitivne racionalne brojeve, takve da je* $a < b < c$. *Tada postoji bijekcija između trokuta stranica* a, b, c, *površine* n *i brojeva* x *za koji je svaki od brojeva* $x,\ x+n,\ x-n$ *kvadrat racionalnog broja. Veza je:*

$$a, b, c \mapsto x = \left(\tfrac{c}{2}\right)^2$$
$$x \mapsto a = \sqrt{x+n} - \sqrt{x-n}, \quad b = \sqrt{x+n} + \sqrt{x-n}, \quad c = 2\sqrt{x} \tag{2.1}$$

Specijalno, n *je kongruentan ako i samo ako postoji* x, *takav da su* $x,\ x+n,\ x-n$ *kvadrati racionalnih brojeva.*

Dokaz: Prvo pretpostavimo da je $a,\ b,\ c$ trojka sa željenim svojstvom: $a^2 + b^2 = c^2$, i $\frac{1}{2}ab = n$. Ako dodamo ili oduzmemo od prve jednadžbe četverostruku drugu, dobijemo: $(a \pm b)^2 = c^2 \pm 4n$. Podijelimo obadvije strane s 4, pa vidimo da broj $x = \left(\frac{c}{2}\right)^2$ ima svojstvo da su brojevi $x \pm n$ kvadrati od $\frac{a \pm b}{2}$. Obratno, ako je dan x s traženim svojstvom, lako se vidi da tri racionalna broja $a < b < c$ dana formulama (2.1) zadovoljavaju: $ab = 2n$ i $a^2 + b^2 = 4x = c^2$.

Da dokažemo bijektivnost, trebamo samo dokazati da n i x ne mogu dati dvije različite trojke. Zaista, fiksirajmo n i x (pa je fiksan i c). Trojku koja odgovara x-u dobijemo iz presjeka dvije konike $a^2 + b^2 = c^2$ i $ab = 2n$ u ab-ravnini. Doduše, imamo četiri točke presjeka, ali za danu točku presjeka (a,b), preostale tri su $(-a,-b),\ (b,a),\ (-b,-a)$, pa stoga dobivamo točno jednu trojku. ■

3. Neke kubne jednadžbe

U ovom ćemo poglavlju naći još jednu karakterizaciju kongruentnih brojeva.

U prošlom poglavlju, u dokazu Propozicije 1, došli smo do jednadžbi $\left(\frac{a \pm b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 \pm n$ za pravokutni trokut stranica $a,\ b,\ c$ i površine n. Ako te dvije jednadžbe međusobno pomnožimo dobijemo $\left(\frac{a^2 - b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$. To pokazuje da jednadžba $u^4 - n^2 = v^2$ ima racionalno rješenje ($u = \frac{c}{2}$ i $v = \frac{a^2 - b^2}{4}$). Pomnožimo sve sa u^2, pa dobijemo $u^6 - n^2u^2 = (uv)^2$. Ako uzmemo $x = u^2 = \left(\frac{c}{2}\right)^2$ (x je isti kao u Propoziciji 1) i $y = uv = \frac{(a^2 - b^2)c}{8}$, onda imamo par racionalnih brojeva (x,y) koji zadovoljavaju jednadžbu:

$$y^2 = x^3 - n^2x. \tag{3.1}$$

Na taj način, za dani pravokutni trokut s racionalnim stranicama $a,\ b,\ c$ površine n, dobijemo točku (x,y) u xy-ravnini s racionalnim koordinatama, koja leži na krivulji $y^2 = x^3 - n^2x$. Obratno, postavlja se pitanje možemo li reći da svaka točka (x,y), sa $x, y \in \mathbb{Q}$ koja leži na kubnoj krivulji mora nužno doći od

takvog pravokutnog trokuta. Očito ne, jer x-koordinata $x = u^2 = \left(\frac{c}{2}\right)^2$ mora ležati u $(\mathbb{Q}^+)^2$ ako se točka (x, y) može dobiti kao u prošlom odlomku. S druge strane, vidi se da x-koordinata takve točke mora imati nazivnik djeljiv s 2. Da bi to vidjeli, uočimo da se trokut a, b, c može dobiti počevši od primitivne Pitagorine trojke a', b', c' koja odgovara pravokutnom trokutu s cjelobrojnim stranicama a', b', c' i površinom $s^2 n$, i dijeleći stranice s s, da se dobije a, b, c. Ali u primitivnoj Pitagorinoj trojki a' i b' su suprotne parnosti, a c' je neparan (vidi dokaz sljedeće Leme). Zaključujemo: (1) $x = \left(\frac{c}{2}\right)^2 = \left(\frac{c'}{2s}\right)^2$ ima nazivnik djeljiv s 2, (2) potencija od 2 koja dijeli nazivnik od c jednaka je potenciji od 2 koja dijeli jednu katetu, dok je potencija od 2 koja dijeli nazivnik druge katete striktno manja. Na primjer, u trokutu površine 5, hipotenuza i kraća kateta imaju 2 u nazivniku, dok druga kateta nema. Zaključujemo da je nužan uvjet da točka (x, y) s racionalnim koordinatama na krivulji $y^2 = x^3 - n^2 x$ dođe od pravokutnog trokuta, da x bude kvadrat i da mu je nazivnik djeljiv s 2. Na primjer, za $n = 31$, točka $\left(\frac{41^2}{7^2}, \frac{29520}{7^3}\right)$ na krivulji $y^2 = x^3 - 31^2 x$ nije nastala od trokuta, iako joj je x-koordinata kvadrat.

Konačno, treći nužan uvjet je da brojnik od x nema zajedničkih faktora s n. Da se to uoči, pretpostavimo da je $p > 2$ prosti zajednički djelitelj od n i brojnika od x. Tada p dijeli brojnik od $x \pm n = \left(\frac{a \pm b}{2}\right)^2$, pa i brojnike od $\frac{a+b}{2}$ i $\frac{a-b}{2}$, tako da p dijeli brojnike njihovog zbroja (tj. a) i razlike (tj. b). Stoga, p^2 dijeli $n = \frac{1}{2}ab$. Ali, pretpostavili smo da je n kvadratno slobodan. Ova kontradikcija pokazuje da x mora biti kvadrat s parnim nazivnikom i brojnikom relativno prostim s n. Primjer koji pokazuje da prva dva uvjeta nisu dovoljna je točka $\left(\frac{25}{4}, \frac{75}{8}\right)$ na krivulji $y^2 = x^3 - 5^2 x$.

Dokažimo sada da su ta tri uvjeta ne samo nužna, nego i dovoljna da točka na krivulji nastane od trokuta.

Lema. *Sve primitivne Pitagorine trojke* (a, b, c) *u kojima je* b *paran, dane su formulama*

$$a = k^2 - l^2, \qquad b = 2kl, \qquad c = k^2 + l^2, \tag{3.2}$$

gdje je $k > l$ *i* k, l *su relativno prosti prirodni brojevi različite parnosti.*

D o k a z : Uočimo prvo da je u svakoj primitivnoj Pitagorinoj trojki točno jedan od brojeva a, b paran (a c je neparan). Zaista, ako bi i a i b bili parni, onda trojka ne bi bila primitivna, a ako bi i a i b bili neparni, onda bi iz $a^2 + b^2 \equiv 2 \pmod 4$ i $c^2 \equiv 0 \pmod 4$ dobili kontradikciju.

Jednadžbu $a^2 + b^2 = c^2$ možemo pisati u obliku $b^2 = (c + a)(c - a)$. Neka je $z = \frac{b}{2}$. Brojevi $c + a$ i $c - a$ su parni, pa su $x = \frac{c+a}{2}$ i $y = \frac{c-a}{2}$ prirodni brojevi. Sada je $z^2 = xy$.

Budući je $c = x + y,\ a = x - y$, zaključujemo da su x i y relativno prosti, pa su $k = \sqrt{x}$ i $l = \sqrt{y}$ prirodni brojevi, relativno prosti. Odavde je

$$a = k^2 - l^2, \qquad c = k^2 + l^2, \qquad b = 2kl.$$

Brojevi k i l moraju biti različite parnosti, jer je broj $c = k^2 + l^2$ neparan.

Obratno, lako se provjeri da brojevi $a,\ b,\ c$ definirani sa (3.2) zadovoljavaju $a^2 + b^2 = c^2$. Treba još provjeriti da su relativno prosti. Pretpostavimo da je $d > 1$ zajednički djelitelj od a i c. Tada je d neparan, $d \mid c + a = (k^2 + l^2) + (k^2 - l^2) = 2k^2$ i $d \mid c - a = (k^2 + l^2) - (k^2 - l^2) = 2l^2$. No, to je u kontradikciji s pretpostavkom da su k i l, pa stoga i k^2 i l^2 relativno prosti. ■

Propozicija 2. *Neka je (x, y) točka s racionalnim koordinatama na krivulji $y^2 = x^3 - n^2 x$. Pretpostavimo da x zadovoljava tri uvjeta: (a) on je kvadrat racionalnog broja, (b) nazivnik mu je paran, i (c) njegov brojnik nema zajedničkih faktora s n. Tada postoji pravokutni trokut racionalnih stranica površine n koji je povezan s x vezom iz Propozicije 1.*

D o k a z : Dokažimo to unatrag, nizom koraka s početka poglavlja. Neka je $u = \sqrt{x} \in \mathbb{Q}^+$ i $v = \frac{y}{u}$, pa je $v^2 = \frac{y^2}{x} = x^2 - n^2$, tj. $v^2 + n^2 = x^2$. Neka je sada t nazivnik od u, tj. najmanji prirodan broj takav da je $tu \in \mathbb{Z}$. Po pretpostavci, t je paran. Uočimo da v^2 i x^2 imaju isti nazivnik (jer je n cijeli broj, a $v^2 + n^2 = x^2$), koji je jednak t^4. Slijedi da je $t^2 v,\ t^2 n,\ t^2 x$ primitivna Pitagorina trojka, s parnim $t^2 n$. (Primitivnost trojke slijedi iz uvjeta (c).) Iz prethodne Leme slijedi da postoje cijeli brojevi k i l, takvi da je $t^2 n = 2kl,\ t^2 v = k^2 - l^2,\ t^2 x = k^2 + l^2$. Pravokutni trokut sa stranicama $\frac{2k}{t},\ \frac{2l}{t},\ 2u$ ima površinu $\frac{2kl}{t^2} = n$, kako smo željeli. Po vezi iz Propozicije 1 za taj trokut je $x = \left(\frac{2u}{2}\right)^2 = u^2$. ■

Kasnije ćemo dati drugu karakterizaciju točke $P = (x, y)$ na krivulji $y^2 = x^3 - n^2 x$ koja odgovara racionalnom pravokutnom trokutu površine n. Naime, to su točke $P = (x, y)$ za koje postoji racionalna točka $P' = (x', y')$ takva da je $P' + P' = P$, gdje "+" označava zbrajanje točaka na našoj krivulji, koje ćemo kasnije definirati. Točka $P = 2P'$ sigurno daje pravokutni trokut!

4. Eliptičke krivulje

Skup točaka $P = (x, y)$ koje zadovoljavaju $y^2 = x^3 - n^2 x$ specijalan je slučaj takozvane "eliptičke krivulje". Općenito, neka je K bilo koje polje, a $f(x) \in K[x]$ kubni polinom s koeficijentima iz K koji ima različite nultočke (možda u nekom proširenju od K). Pretpostavljat ćemo da K nije karakteristike 2. Tada rješenja jednadžbe

$$y^2 = f(x), \tag{4.1}$$

gdje su x i y u nekom proširenju K' od K, zovemo K'-točke na eliptičkoj krivulji definiranoj s (4.1). Do sada smo imali primjere $K = K' = \mathbb{Q}$, $f(x) = x^3 - n^2x$. Uočimo da taj primjer $y^2 = x^3 - n^2x$ zadovoljava uvjet za eliptičku krivulju nad svakim poljem K karakteristike p, ako p ne dijeli $2n$, jer su tada tri korijena 0, $\pm n$ od $f(x) = x^3 - n^2x$ različita.

Općenito, ako su $x_0, y_0 \in K'$ koordinate neke točke na krivulji C definiranoj jednadžbom $F(x, y) = 0$, kažemo da je C glatka u (x_0, y_0) ako je bar jedna parcijalna derivacija $\frac{\partial F}{\partial x}$ i $\frac{\partial F}{\partial y}$ različita od nule u (x_0, y_0). Ta definicija ne ovisi o osnovnom polju (parcijalna derivacija polinoma $F(x, y)$ je definirana po standardnoj formuli koja ima smisla u svakom polju). Ako je K' polje $\mathbb{R}$ realnih brojeva, to se poklapa sa standardnim zahtjevom da C ima tangentu. U našem slučaju $F(x, y) = y^2 - f(x)$, parcijalne derivacije su $2y_0$ i $-f'(x)$. Budući da K' nije polje karakteristike 2, obadvije iščezavaju ako i samo ako je $y_0 = 0$ i x_0 višestruka nultočka od $f(x)$. Prema tome, krivulja ima točaka u kojima nije glatka, ako i samo ako $f(x)$ ima višestruke nultočke. To je razlog zbog kojeg smo zahtijevali različite nultočke u definiciji eliptičke krivulje: eliptička krivulja je glatka u svim svojim točkama.

Uz točke (x, y) na eliptičkoj krivulji (4.1), vrlo je važna "**točka u beskonačnosti**" ($\mathcal{O}$), koju smatramo da je na krivulji, jer se u teoriji kompleksnih funkcija uz točke kompleksne ravnine ubacuje i točka u beskonačnosti. Da to pobliže objasnimo, uvedimo projektivne koordinate.

Pod "totalni stupanj monoma" $x^k y^l$ podrazumijevamo $k + l$. Pod "totalni stupanj polinoma" $F(x, y)$ podrazumijevamo najveći totalni stupanj monoma koji se pojavljuju s koeficijentima različitim od nule. Ako je n totalni stupanj od $F(x, y)$, definirajmo odgovarajući homogeni polinom $\widetilde{F}(x, y, z)$ s tri varijable tako da pomnožimo svaki monom $x^k y^l$ iz $F(x, y)$ sa z^{n-k-l}, da dovedemo njegov totalni stupanj u varijablama x, y, z do n. Drugim riječima:

$$\widetilde{F}(x, y, z) = z^n F\left(\frac{x}{z}, \frac{y}{z}\right).$$

Uočimo da je $F(x, y) = \widetilde{F}(x, y, 1)$. U našem slučaju $F(x, y) = y^2 - (x^3 - n^2x)$, dobivamo $\widetilde{F}(x, y, z) = y^2z - x^3 + n^2xz^2$.

Pretpostavimo da naš polinom ima koeficijente iz nekog polja K, i da nas zanimaju trojke $x, y, z \in K$, takve da je $\widetilde{F}(x, y, z) = 0$. Uočimo sljedeće:

(1) Za svaki $\lambda \in K$, $\widetilde{F}(\lambda x, \lambda y, \lambda z) = \lambda^n \widetilde{F}(x, y, z)$ (n je totalni stupanj od F);

(2) Za svaki $\lambda \in K$, različit od nule, $\widetilde{F}(\lambda x, \lambda y, \lambda z) = 0$ ako i samo ako je $\widetilde{F}(x, y, z) = 0$. Posebno za $z \neq 0$ vrijedi $\widetilde{F}(x, y, z) = 0$ ako i samo ako $F\left(\frac{x}{z}, \frac{y}{z}\right) = 0$.

Zbog (2) je prirodno promatrati klase ekvivalencije trojki x, y, z. Kažemo da su dvije trojke (x, y, z) i (x', y', z') ekvivalentne ako postoji $\lambda \in K$, različit od nule, takav da $(x', y', z') = \lambda(x, y, z)$. Izostavimo trivijalnu trojku $(0,0,0)$ i definirajmo "**projektivnu ravninu $\mathbb{P}_K^2$**" kao skup svih klasa ekvivalencije netrivijalnih trojki.

Prilično nam je neprirodno razmišljati u terminima "klase ekvivalencije". Srećom, postoje vizualniji načini razmišljanja o projektivnoj ravnini. Pretpostavimo da je K polje $\mathbb{R}$ realnih brojeva. U tom slučaju sve trojke (x, y, z) u nekoj klasi ekvivalencije odgovaraju točkama u trodimenzionalnom Euklidskom prostoru koje leže na pravcu kroz ishodište. Tako se $\mathbb{P}_{\mathbb{R}}^2$ geometrijski može shvatiti kao skup pravaca u trodimenzionalnom prostoru kroz ishodište.

Drugi način vizualizacije $\mathbb{P}_{\mathbb{R}}^2$ je da u trodimenzionalnom prostoru promatramo ravninu koja ne prolazi ishodištem, recimo ravninu paralelnu s xy-ravninom, na udaljenosti 1 od ishodišta, tj. ravninu $z = 1$. Svi pravci kroz ishodište, osim onih koji leže u xy-ravnini imaju jednu točku presjeka s ravninom. To znači da svaka klasa ekvivalencije s z-koordinatom različitom od nule ima jedinstvenu trojku oblika $(x, y, 1)$. Na taj način takve klase ekvivalencije promatramo kao točke u običnoj xy-ravnini. Preostale trojke, one oblika $(x, y, 0)$ čine "pravac u beskonačnosti".

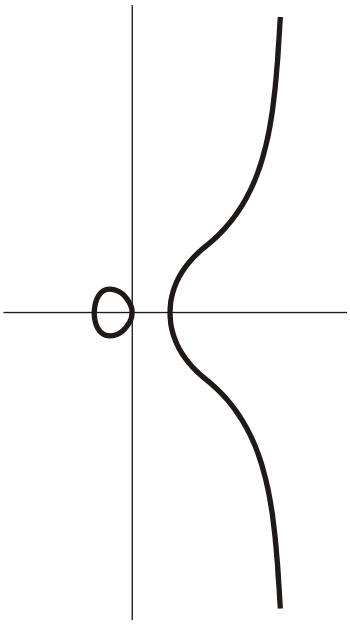
Pravac u beskonačnosti može se vizualizirati kao obični pravac (recimo pravac $y = 1$ u xy-ravnini) koji se sastoji od klasa ekvivalencije s y-koordinatom različitom od nule, dakle sadrži jedinstvene trojke oblika $(x, 1, 0)$, zajedno s običnom "točkom u beskonačnosti" $(1,0,0)$. Tj. projektivni pravac $\mathbb{P}_K^1$ nad poljem K definiramo kao skup svih klasa ekvivalencije parova (x, y) sa $(x, y) \sim (\lambda x, \lambda y)$. Tako se $\mathbb{P}_K^2$ može shvatiti kao obična ravnina $(x, y, 1)$ zajedno s projektivnim pravcem u beskonačnosti, za koji se pokaže da se sastoji od običnog pravca $(x, 1, 0)$ zajedno s njegovom točkom u beskonačnosti $(1,0,0)$.

Općenito, n-dimenzionalni projektivni prostor $\mathbb{P}_K^n$ definira se koristeći klase ekvivalencije $(n+1)$-torki, i možemo ga shvatiti kao obični prostor n-torki $(x_1, \ldots, x_n, 1)$ zajedno sa $\mathbb{P}_K^{n-1}$ u beskonačnosti oblika $(x_1, \ldots, x_n, 0)$. Na sreću, mi ćemo trebati samo $\mathbb{P}_K^1$ i $\mathbb{P}_K^2$.

Dan je homogeni polinom $\widetilde{F}(x, y, z)$ s koeficijentima iz K. Možemo promatrati skup rješenja koji se sastoji od točaka (x, y, z) u $\mathbb{P}_K^2$ (ustvari klasa ekvivalencije od (x, y, z)) za koje je $\widetilde{F}(x, y, z) = 0$. Točke skupa rješenja kojima je $z \neq 0$ su točke $(x, y, 1)$ za koje vrijedi $\widetilde{F}(x, y, 1) = F(x, y) = 0$. Preostale točke su na pravcu u beskonačnosti. Skup rješenja od $\widetilde{F}(x, y, z) = 0$ zove se "projektivna

nadopuna" krivulje $F(x,y)=0$. Odsad, kada budemo govorili o "pravcu", "koniki", "eliptičkoj krivulji", itd., uglavnom ćemo raditi u projektivnoj ravnini $\mathbb{P}^2_K$, i u tom će slučaju ti izrazi uvijek označavati projektivnu nadopunu obične krivulje xy-ravnine. Na primjer, pod pravcem $y=ax+b$ mislit ćemo na skup rješenja $y=ax+bz$ u $\mathbb{P}^2_K$, a pod eliptičkom krivuljom $y^2=x^3-n^2x$ podrazumijevat ćemo skup rješenja $y^2z=x^3-n^2xz^2$ u $\mathbb{P}^2_K$.

Promotrimo malo bolje naš omiljeni primjer: $F(x,y)=y^2-(x^3-n^2x)$, $\widetilde{F}(x,y,z)=y^2z-x^3+n^2xz^2$. Točke u beskonačnosti na toj eliptičkoj krivulji su klase ekvivalencije $(x,y,0)$, takve da je $0=\widetilde{F}(x,y,0)=-x^3$, tj. $x=0$. Postoji samo jedna takva klasa ekvivalencije $(0,1,0)$. Intuitivno, ako uzmemo $K=\mathbb{R}$, promatramo krivulju $y^2=x^3-n^2x$ koja se brzo uvećava kako se približava pravcu u beskonačnosti (Slika 4). Točke na pravcu u beskonačnosti odgovaraju pravcima xy-ravnine kroz ishodište, tj. postoji jedna za svaki mogući smjer $\frac{y}{x}$ takvog pravca. Kako odlazimo sve dalje našom krivuljom, približavamo se smjeru $\frac{y}{x}=\infty$, koji odgovara točki $(0,1,0)$ na pravcu u beskonačnosti. Uočimo da svaka eliptička krivulja $y^2=f(x)$ sadrži točno jednu točku u beskonačnosti $(0,1,0)$.



Slika 4

Svi uobičajeni načini računanja s krivuljama $F(x,y)=0$ u xy-ravnini prenose se do odgovarajućih projektivnih krivulja $\widetilde{F}(x,y,z)=0$. Svi izrazi kao tangenta u točki, točka infleksije, glatkost, singularitet ovise samo o tome što se događa u okolini točke ispitivanja. A svaka točka u $\mathbb{P}^2_K$ ima okolinu koja izgleda kao obična ravnina. Preciznije, ako nas zanimaju točke sa z-koordinatom različitom od nule, možemo raditi u običnoj xy-ravnini, gdje krivulja ima jednadžbu $F(x,y)=\widetilde{F}(x,y,1)=0$. Ako želimo proučavati točke na pravcu $z=0$, stavimo trojku u jedan od oblika $(x,1,0)$ ili $(1,y,0)$. U prvom slučaju gledamo je kao točku na krivulji $\widetilde{F}(x,1,z)=0$ u xz-ravnini, a u drugom kao točku na krivulji $\widetilde{F}(1,y,z)=0$ u yz-ravnini.

Na primjer, u blizini točke u beskonačnosti $(0,1,0)$ na eliptičkoj krivulji $y^2z-x^3+n^2xz^2=0$, sve točke imaju oblik $(x,1,z)$ i zadovoljavaju $z-x^3+n^2xz^2=0$. Posljednja nam jednadžba ustvari daje sve točke na eliptičkoj krivulji osim tri $(0,0,1)$, $(\pm n,0,1)$ koje imaju nula y-koordinatu (to su tri "točke u beskonačnosti" ako promatramo u xz-koordinatama).

5. Dvostruko periodične funkcije

Neka je L "**rešetka**" u kompleksnoj ravnini. Pod tim podrazumijevamo skup svih cjelobrojnih linearnih kombinacija dva kompleksna broja ω_1 i ω_2, koja ne leže na istom pravcu kroz ishodište. Za primjer, ako uzmemo $\omega_1 = i$ i $\omega_2 = 1$, dobijemo Gaussove cijele brojeve $\{mi + n \mid m, n \in \mathbb{Z}\}$. Primjer rešetke Gaussovih cijelih brojeva je blisko povezan s eliptičkim krivuljama $y^2 = x^3 - n^2 x$ koje se pojavljuju u problemu kongruentnih brojeva.

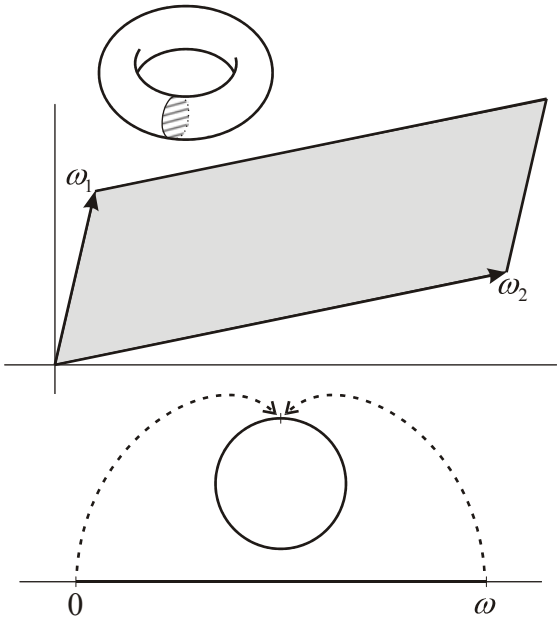
Fundamentalni paralelogram za ω_1 i ω_2 se definira kao skup

$$\Pi = \left\{ a\omega_1 + b\omega_2 \,\middle|\, 0 \le a \le 1, 0 \le b \le 1 \right\}.$$

Budući da ω_1 i ω_2 čine bazu za $\mathbb{C}$ nad $\mathbb{R}$, svaki se broj $x \in \mathbb{C}$ može zapisati u obliku $x = a\omega_1 + b\omega_2$, za neke $a, b \in \mathbb{R}$. Tako se x može na jedinstven način zapisati kao zbroj elementa u rešetki $L = \{m\omega_1 + n\omega_2\}$ i elementa u Π, ako a i b nisu cijeli brojevi, tj. ako Π-dio ne leži na rubu $\partial\Pi$.

ω_1 i ω_2 ćemo uvijek uzimati u smjeru kazaljke na satu, tako da ćemo pretpostavljati da ω_1/ω_2 ima pozitivan imaginarni dio.

Uočimo da izbor brojeva ω_1 i ω_2 koji daju rešetku L nije jedinstven. Na primjer, ista se rešetka dobije i ako uzmemo $\omega_1' = \omega_1 + \omega_2$ i ω_2. Općenito novu bazu ω_1', ω_2' za rešetku L možemo dobiti množeći staru s cjelobrojnom matricom determinante 1.



Slika 5

Neka je dana rešetka L. Za meromorfnu funkciju na $\mathbb{C}$ kažemo da je eliptička funkcija u odnosu na L, ako je $f(z + l) = f(z)$ za sve $l \in L$. Uočimo da je dovoljno to svojstvo provjeriti za $l = \omega_1$ i $l = \omega_2$. Drugim riječima, eliptička funkcija je periodička funkcija s dva perioda ω_1 i ω_2. Takva funkcija je potpuno određena vrijednostima na fundamentalnom paralelogramu Π, te su joj vrijednosti na suprotnim stranama paralelograma jednake, tj. $f(a\omega_1 + \omega_2) = f(a\omega_1)$, $f(\omega_1 + b\omega_2) = f(b\omega_2)$. Tako da na eliptičku funkciju $f(z)$ možemo gledati kao na funkciju na skupu Π sa slijepljenim nasuprotnim stranama. Taj je skup (preciznije "kompleksna mnogostrukost") poznat kao "**torus**".

Dvostruko periodične funkcije kompleksnih brojeva direktna su analogija običnih periodičnih funkcija realnih brojeva. Funkcija $f(x)$ na $\mathbb{R}$ koja zadovoljava $f(x+n\omega)=f(x)$ određena je vrijednostima na intervalu $[0,\omega]$. Vrijednosti u 0 i ω su joj jednake, pa se može shvatiti kao funkcija na intervalu $[0,\omega]$, sa slijepljenim rubnim točkama. "Realna mnogostrukost" dobivena lijepljenjem rubnih točaka je obična kružnica (Slika 5).

Vratimo se sada eliptičkim funkcijama na rešetki L. Skup tih funkcija označimo sa $\mathcal{E}_L$. Odmah se vidi da je $\mathcal{E}_L$ potpolje polja svih meromorfnih funkcija. Tj. zbroj, razlika, umnožak i kvocijent dvije eliptičke funkcije je eliptička funkcija. Uz to, potpolje je zatvoreno na deriviranje. Dajmo sada neka vrlo specifična svojstva koja mora imati eliptička funkcija. Uvjet dvostruke periodičnosti meromorfne funkcije puno je restriktivniji od realnog slučaja. Skup realnih analitičkih periodičnih funkcija s danim periodom puno je "veći" od skupa $\mathcal{E}_L$ svih eliptičkih funkcija za dani period mreže L.

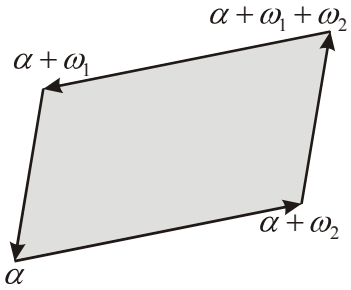
Propozicija 3. *Funkcija* $f(z)\in\mathcal{E}_L$, $L=\{m\omega_1+n\omega_2\}$, *koja nema pola u fundamentalnom paralelogramu* Π *je konstanta.*

Dokaz: Budući da je Π kompaktan, svaka takva funkcija je ograničena na Π, recimo, nekom konstantom M. Tada je $|f(z)|<M$ za sve $z\in\mathbb{C}$, jer su joj vrijednosti određene vrijednostima na Π. Po Liouvilleovom teoremu[3], f je konstanta. ■

Propozicija 4. *Uz istu notaciju kao gore, neka je* $\alpha+\Pi$ *translacija od* Π *za kompleksni broj* α, *tj.* $\{\alpha+z\mid z\in\Pi\}$. *Pretpostavimo da* $f(z)\in\mathcal{E}_L$ *nema polova na rubu* C *od* $\alpha+\Pi$. *Tada je zbroj reziduuma od* $f(z)$ *u* $\alpha+\Pi$ *nula.*

Dokaz: Po rezidualnom teoremu, taj zbroj je jednak:

$$\frac{1}{2\pi i}\int_C f(z)dz.$$



Slika 6

Integral na suprotnim stranama se poništava, budući da su vrijednosti od $f(z)$ jednake, dok dz mijenja smjer (Slika 6), jer je put integracije suprotan. Budući da je taj integral nula, i zbroj reziduuma je nula. ■

Uočimo da (budući da meromorfna funkcija može imati samo konačno mnogo polova u ograničenom području) je uvijek moguće izabrati takav α da

[3] Liouvilleov teorem kaže da je ograničena meromorfna funkcija na cijelom $\mathbb{C}$ je konstanta.

rubovi od $\alpha+\Pi$ promaše sve polove od $f(z)$. Također uočimo da nekonstantna funkcija $f(z)\in\mathcal{E}_L$ ima bar dva pola (ili višestruki pol), jer kad bi imala jedan jednostruki pol, onda zbroj reziduuma ne bi bio nula.

Propozicija 5. *U uvjetima Propozicije 4, pretpostavimo da* $f(z)$ *nema nultočaka ni polova na rubu od* $\alpha+\Pi$. *Neka je* $\{m_i\}$ *skup redova različitih nultočaka u* $\alpha+\Pi$, *a* $\{n_j\}$ *skup redova različitih polova. Tada je* $\sum m_i=\sum n_j$.

Dokaz: Primijenimo Propoziciju 4 na eliptičku funkciju $f'(z)/f(z)$. Prisjetimo se da logaritanska derivacija $f'(z)/f(z)$ ima pol točno gdje $f(z)$ ima nultočku ili pol, takav pol je jednostruk i reziduum mu je jednak redu nultočke ili pola originalne $f(z)$ (negativno ako je pol). (Ako je $f(z)=c_m(z-a)^m+\cdots$, tada je $f'(z)=c_m m(z-a)^{m-1}+\cdots$ tako da je $f'(z)/f(z)=m(z-a)^{-1}+\cdots$.) Zaključujemo da je zbroj reziduuma od $f'(z)/f(z)$ jednak $\sum m_i-\sum n_j=0$. ■

Definirajmo sada jednu eliptičku funkciju u odnosu na $L=\{m\omega_1+n\omega_2\}$, koju ćemo proučavati nadalje, a zove se Weierstrassova $\wp$-funkcija. Označava se sa $\wp(z;L)$ ili $\wp(z;\omega_1,\omega_2)$, ili jednostavno $\wp(z)$ ako je iz konteksta jasno o kojoj rešetki se radi. Dakle,

$$\wp(z)=\wp(z;L)\underset{\text{def}}{=}\frac{1}{z^2}+\sum_{\substack{l\in L\\ l\neq 0}}\left(\frac{1}{(z-l)^2}-\frac{1}{l^2}\right). \tag{5.1}$$

Navedimo prvo dvije leme, a onda dokažimo neka svojstva funkcije $\wp(z)$.

Lema 1. *Ako je* $\sum b_l$ *konvergentan red s pozitivnim članovima, gdje se sumira po svim elementima mreže* L *različitim od nule, i ako* $\sum f_l(z)$ *ima svojstvo da* $\left|\frac{f_l(z)}{b_l}\right|$ *teži nekom konačnom broju kada* $|l|\to\infty$, *uniformno za* z *iz nekog podskupa od* $\mathbb{C}$, *onda red* $\sum f_l(z)$ *konvergira apsolutno i uniformno za* z *iz tog skupa.* ■

Lema 2. $\sum|l|^{-s}$ *konvergira za* $s>2$.

Dokaz: Rastavimo red na dijelove po l, koji zadovoljavaju $n-1<|l|\le n$, za $n=1,2,\ldots$. Nije teško uočiti da je broj l-ova u ovom kružnom vijencu reda veličine n. Tako da je zbroj u lemi ograničen konstantom puta $\sum_{n=1}^{\infty}n\cdot n^{-s}=\sum n^{1-s}$, a drugi red konvergira za $s-1>1$. ■

Propozicija 6. *Zbroj u (5.1) konvergira apsolutno i uniformno za* z *iz bilo kojeg kompaktnog podskupa od* $\mathbb{C}-L$.

Dokaz: Dokaz konvergencije će biti rutinski ako imamo na umu jedno-dimenzionalnu analogiju. Ako umjesto iz L uzmemo brojeve iz $\mathbb{Z}$, a umjesto recipročnih kvadrata uzmemo recipročne brojeve, dobivamo realnu funkciju $f(x)=\frac{1}{x}+\sum\left(\frac{1}{x-l}+\frac{1}{l}\right)$, gdje se sumira po svim $l\in\mathbb{Z}$ koji su različiti od nule. Da dokažemo apsolutnu i uniformnu konvergenciju u bilo kojem kompaktnom podskupu od $\mathbb{R}-\mathbb{Z}$, prvo zapišimo sumand kao $\frac{x}{l(x-l)}$, i vidimo da se taj red ponaša isto kao l^{-2}.

Dokaz Propozicije 6 ide jednako. Prvo svedemo sumande na zajednički nazivnik:

$$\frac{1}{(z-l)^2}-\frac{1}{l^2}=\frac{2z-\frac{z^2}{l}}{(z-l)^2 l}.$$

Apsolutna i uniformna konvergencija slijedi uspoređivanjem s $|l|^{-3}$, gdje se sumira po svim $l\in\mathbb{Z}$ različitim od nule. ■

Propozicija 7. *$\wp(z)\in\mathcal{E}_L$, i njeni jedini polovi su dvostruki polovi u svakoj točki rešetke.*

Dokaz: Isti argument kao u Propoziciji 6 pokazuje da je za svaki čvrsti $l\in L$, funkcija $\wp(z)-(z-l)^{-2}$ neprekidna u $z=l$, tako da je $\wp(z)$ meromorfna funkcija s dvostrukim polovima u svakoj točki rešetke i bez drugih polova. Uočimo da je $\wp(z)=\wp(-z)$ jer desna strana od (5.1) ostaje nepromijenjena ako z zamijenimo s $-z$, a l sa $-l$; a sumiranje po $l\in L$ je isto kao sumiranje po $-l\in L$.

Da dokažemo dvostruku periodičnost, pogledajmo derivaciju. Derivirajući (5.1) član po član dobijemo:

$$\wp'(z)=-2\frac{1}{z^3}+\sum_{\substack{l\in L\\ l\neq 0}}\left(-2\frac{1}{(z-l)^3}+0\right)=-2\frac{1}{(z-0)^3}-2\sum_{\substack{l\in L\\ l\neq 0}}\frac{1}{(z-l)^3}$$

$$\wp'(z)=-2\sum_{l\in L}\frac{1}{(z-l)^3}.$$

Sada je očito $\wp'(z)$ dvostruko periodična jer mijenjanjem z sa $z+l_0$ za neki fiksni $l_0\in L$ samo mijenjamo redoslijed članova reda. Tako da je $\wp'(z)\in\mathcal{E}_L$. Da dokažemo da je $\wp(z)\in\mathcal{E}_L$, dovoljno je vidjeti da je $\wp(z+\omega_i)-\wp(z)=0$, za $i=1,2$. Dokažimo za $i=1$ (potpuno je jednako za $i=2$).

Budući je derivacija funkcije $\wp(z+\omega_1)-\wp(z)$ jednaka $\wp'(z+\omega_i)-\wp'(z)=0$, slijedi da je $\wp(z+\omega_1)-\wp(z)=C$, za neku konstantu C. Uvrštavanjem $z=-\frac{1}{2}\omega_1$ i korištenjem činjenice da je $\wp(z)$ parna funkcija, zaključujemo da je $C=\wp(\frac{1}{2}\omega_1)-\wp(-\frac{1}{2}\omega_1)=0$. Iz toga slijedi dokaz. ■

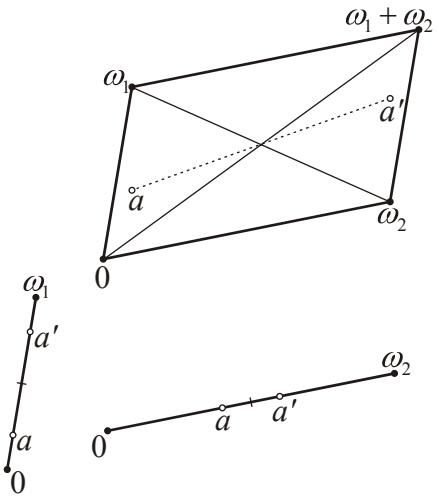
Uočimo da dvostruka periodičnost funkcije $\wp(z)$ nije bila očita iz definicije (5.1).

Kako funkcija $\wp(z)$ ima točno jedan dvostruki pol u fundamentalnoj domeni oblika $\alpha+\Pi$, po Propoziciji 5 ona tu ima i točno dvije nultočke (ili jednu dvostruku). Isto vrijedi za svaku eliptičku funkciju oblika $\wp(z)-u$, gdje je u konstanta. Nije teško vidjeti da $\wp(z)$ poprima sve vrijednosti $u\in\mathbb{C}\cup\{\infty\}$ točno dvaput na torusu (tj. na fundamentalnom paralelogramu sa spojenim suprotnim stranama), brojeći kratnost (što znači brojeći red od nultočke od $\wp(z)-u$); i da su vrijednosti shvaćene s kratnošću dva ∞, $\boldsymbol{e_1}\underset{\text{def}}{=}\wp(\frac{\omega_1}{2})$, $\boldsymbol{e_2}\underset{\text{def}}{=}\wp(\frac{\omega_2}{2})$, $\boldsymbol{e_3}\underset{\text{def}}{=}\wp(\frac{\omega_1+\omega_2}{2})$. Naime, $\wp(z)$ ima dvostruki pol u 0, dok su ostale tri točke nultočke od $\wp'(z)$.

6. Polje eliptičkih funkcija

Propozicija 7 nam daje konkretan primjer eliptičke funkcije. Kao što $\sin x$ i $\cos x$ (zbog Fourierovog razvoja) imaju osnovnu ulogu u teoriji periodičnih funkcija na $\mathbb{R}$, tako $\wp(z)$ i $\wp'(z)$ imaju osnovnu ulogu u proučavanju eliptičkih funkcija. Za razliku od realnog slučaja, ne trebamo beskonačne redove da prikažemo određenu eliptičku funkciju kao kombinaciju tih dviju osnovnih.

Propozicija 8. *Potpolje $\mathcal{E}_L^+\subset\mathcal{E}_L$ svih parnih eliptičkih funkcija na L generirano je s $\wp(z)$, tj. $\mathcal{E}_L^+=\mathbb{C}(\wp)$. Preciznije, za danu funkciju $f(z)\in\mathcal{E}_L^+$ postoji racionalna funkcija $g(x)$ takva da je $f(z)=g(\wp(z))$.*



Slika 7

Dokaz: Ideja dokaza je da koristeći samo funkcije oblika $\wp(z)-u$ (u konstanta) sastavimo funkciju koja ima iste nultočke i polove kao $f(z)$. Omjer $f(z)$ i takve funkcije je eliptička funkcija bez polova, pa je konstanta (Propozicija 3).

Neka je $f(z)\in\mathcal{E}_L^+$. Prvo pronađimo sve nultočke i polove. Neka je Π' fundamentalni paralelogram bez dva ruba:

$$\Pi'=\left\{a\omega_1+b\omega_2\,\middle|\,0\le a<1,\,0\le b<1\right\}.$$

Tada se svaka točka iz $\mathbb{C}$ razlikuje za element rešetke od točno jedne točke iz Π'. Pronađimo sve nultočke i polove u Π', osim 0 (čak i ako bude nultočka ili pol od $f(z)$). Svaku nultočku ili pol uzmimo onoliko puta koliki joj je red. Pa ipak, uzmimo ih samo pola; jer će biti poredane u parovima, a uzimamo samo jednu od svakog para. Opišimo sada detalje, i to za nultočke. Za polove sve ide analogno.

Prvo pretpostavimo da je $a \in \Pi', a \neq 0$, nultočka od $f(z)$ koja nije u polovini rešetke, tj. $a \neq \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$. Neka je točka $a' \in \Pi'$ "simetrična" točki a, tj. $a' = \omega_1 + \omega_2 - a$ ako je a u unutrašnjosti od Π', a $a' = \omega_1 - a$ ili $a' = \omega_2 - a$ ako je a na nekoj od dvije strane (Slika 7). Ako je a nultočka reda m, tvrdimo da je i njoj simetrična točka a' isto nultočka reda m, što slijedi iz dvostruke periodičnosti i parnosti od $f(z)$. Naime, zbog dvostruke periodičnosti vrijedi $f(a'-z) = f(-a-z)$, a zbog parnosti je to jednako $f(a+z)$. Ako je $f(a+z) = a_m z^m + \cdots$, slijedi da je $f(a'+z) = a_m(-z)^m + \cdots$, tj. a' je nultočka reda m.

Sada pretpostavimo da je $a \in \Pi'$ nultočka od $f(z)$ koja je na polovini rešetke. Na primjer, pretpostavimo da je $a = \frac{\omega_1}{2}$. U tom slučaju je red nultočke paran broj, recimo m. Zaista, ako je $f(a+z) = f(\frac{\omega_1}{2}+z) = a_m z^m + \cdots$, onda je $f(\frac{\omega_1}{2}-z) = f(-\frac{\omega_1}{2}+z) = f(\frac{\omega_1}{2}+z)$ zbog periodičnosti i parnosti. Tako da dobijemo $a_m z^m + \cdots = a_m(-z)^m + \cdots$, pa je m paran.

Sada možemo poredati nultočke i polove od $f(z)$. Neka je $\{a_i\}$ skup nultočki od $f(z)$ u Π' koje nisu na polovini mreže. Svaku uzmimo onoliko puta koliki joj je red, ali uzmimo samo jednu od svakog para simetričnih nultočki a i a'. Uz to, ako je neka od tri točke na polovini mreže nultočka od $f(z)$, ubacimo ju u skup pola puta od toga koliki joj je red. Neka je $\{b_j\}$ skup polova različitih od nule funkcije $f(z)$, brojenih isto kao nultočke (tj. samo njih pola).

Budući da su svi a_i i b_j različiti od nule, vrijednosti od $\wp(a_i)$ i $\wp(b_j)$ su konačne, te je dobro definirana eliptička funkcija

$$g(z) = \frac{\prod_i (\wp(z) - \wp(a_i))}{\prod_j (\wp(z) - \wp(b_j))}.$$

Tvrdimo da $g(z)$ ima iste nultočke i polove istih redova kao $f(z)$, iz čega slijedi da je $f(z) = c \cdot g(z)$ za neku konstantu c. Budući da je $g(z)$ racionalna funkcija u $\wp(z)$, to će dovršiti dokaz.

Da bismo dokazali tu tvrdnju, provjerimo prvo elemente od Π', različite od nule. Budući da je 0 samo pol brojnika ili nazivnika od $g(z)$, slijedi da nultočke od $g(z)$ različite od nule moraju doći od nultočki od $\wp(z) - \wp(a_i)$, dok polovi od $g(z)$ različiti od nule moraju doći od nultočki od $\wp(z) - \wp(b_j)$. Znamo da $\wp(z) - u$ (u konstanta) ima dvostruku nultočku u $z = u$ ako je u točka na polovini mreže, a u suprotnom ima par jednostrukih nultočki u u i simetričnoj točki u'. To su jedine nultočke od $\wp(z) - u$ u Π'. Našom konstrukcijom od a_i i b_j, vidimo da $g(z)$ i $f(z)$ imaju iste nultočke i polove istih redova svugdje u Π', osim možda u 0. Ostaje samo provjeriti da imaju i isti red nultočke ili pola u 0. To slijedi iz Propozicije 5. Naime, izaberimo α tako da ni točke mreže, ni nultočke, ni polovi od $f(z)$ i $g(z)$ nisu na rubu od $\alpha + \Pi$. Tada će $\alpha + \Pi$ sadržavati točno jednu točku mreže l. Znamo da $g(z)$ i $f(z)$ imaju iste nultočke i polove istih redova

svugdje u $\alpha+\Pi$, osim možda u l. Neka je m_f red nultočke od $f(z)$ u l (ako je pol, m_f je negativan), a m_g analogni red za $g(z)$. Tada je

$$m_f + (\text{zbroj redova nultočki od } f) - (\text{zbroj redova polova od } f) = \\ = m_g + (\text{zbroj redova nultočki od } g) - (\text{zbroj redova polova od } g).$$

Budući da su odgovarajući faktori u zagradama na suprotnim stranama jednaki, zaključujemo da je $m_g = m_f$. ■

Propozicija 9. *$\mathcal{E}_L = \mathbb{C}(\wp,\wp')$, tj. svaka eliptička funkcija na L racionalni je izraz u $\wp(z;L)$ i $\wp'(z;L)$. Preciznije, za danu funkciju $f(z)\in\mathcal{E}_L$ postoje racionalne funkcije $g_1(x)$ i $g_2(x)$ takve da je $f(z)=g_1(\wp(z))+\wp'(z)g_2(\wp(z))$.*

Dokaz: Neka je $f(z)$ eliptička funkcija na L. Tada su funkcije $f_1(z)=\frac{f(z)+f(-z)}{2}$ i $f_2(z)=\frac{f(z)-f(-z)}{2\wp'(z)}$ parne, pa po Propoziciji 8 postoje funkcije $g_1(x)$ i $g_2(x)$, takve da je $f_1(z)=g_1(\wp(z))$ i $f_2(z)=g_2(\wp(z))$. Budući da je $f(z)=f_1(z)+\wp'(z)\cdot f_2(z)$ slijedi tvrdnja. ■

Dokaz Propozicija 8 i 9 je konstruktivan, tj. daje nam algoritam za izražavanje neke eliptičke funkcije kao funkcije od $\wp(z)$, ako znamo njene nultočke i polove. Već sada možemo zaključiti da je:

(1) parna eliptička funkcija $\wp'(z)^2$ kubni polinom u $\wp(z)$ (jer $\wp'(z)$ ima trostruku nultočku u 0 i tri jednostruke nultočke, dakle imamo tri a_i, a nijedan b_j);

(2) parna eliptička funkcija $\wp(nz)$ (za bilo koji čvrsti $n\in\mathbb{N}$) je racionalna funkcija od $\wp(z)$.

Ove će dvije činjenice biti osnovne u nastavku. Prva nam govori da Weierstrassova $\wp$-funkcija zadovoljava jednu vrlo posebnu diferencijalnu jednadžbu. Ta jednadžba dat će nam vezu s eliptičkim krivuljama. Druga je početak proučavanja točaka konačnog reda na eliptičkim krivuljama.

7. Eliptičke krivulje u Weierstrassovom obliku

Kako je napomenuto na kraju prošlog poglavlja, iz Propozicije 8 odmah se može zaključiti da je $\wp'(z)^2$ kubni polinom u $\wp(z)$. Preciznije, pokazuje se da $\wp'(z)^2$ ima dvostruke nultočke u $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ i $\frac{\omega_1+\omega_2}{2}$. Tako da su ta tri broja a_i-evi, pa imamo

$$\wp'(z)^2 = c\cdot\left(\wp(z)-\wp\left(\tfrac{\omega_1}{2}\right)\right)\cdot\left(\wp(z)-\wp\left(\tfrac{\omega_2}{2}\right)\right)\cdot\left(\wp(z)-\wp\left(\tfrac{\omega_1+\omega_2}{2}\right)\right) \\ = c\cdot(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3),$$

gdje je c neka konstanta. c se lako nađe uspoređujući koeficijente uz najmanju potenciju od z Laurentovog razvoja oko ishodišta. Uočimo da je $\wp(z) - z^{-2}$ neprekidna u ishodištu, kao i $\wp'(z) - 2z^{-3}$. Tako da je vodeći koeficijent lijeve strane $\left(-2z^{-3}\right)^2 = 4z^{-6}$, dok na desnoj strani imamo $c \cdot \left(z^{-2}\right)^3 = c \cdot z^{-6}$. Zaključujemo da je $c = 4$. Tako da $\wp(z)$ zadovoljava diferencijalnu jednadžbu:

$$\wp'(z)^2 = f(\wp(z)), \qquad \text{gdje je } f(x) = 4(x - e_1)(x - e_2)(x - e_3) \in \mathbb{C}[x]. \tag{7.1}$$

Uočimo da kubni polinom f ima različite nultočke.

Dajmo sada još jedan neovisan izvod diferencijalne jednadžbe za $\wp(z)$ koji koristi samo Propoziciju 3. Pretpostavimo da znamo naći kubni polinom $f(x) = ax^3 + bx^2 + cx + d$ takav da se Laurentov razvoj u 0 eliptičke funkcije $f(\wp(z))$ poklapa u negativnim potencijama od z s Laurentovim razvojem od $\wp'(z)^2$. Tada je razlika $\wp'(z)^2 - f(\wp(z))$ eliptička funkcija bez pola u 0, pa zapravo i nigdje drugdje (budući da $\wp(z)$ i $\wp'(z)$ imaju polove samo u 0). Po Propoziciji 3 ta razlika je konstanta, pa možemo namjestiti da bude nula, ako izaberemo pogodan d u $f(x)$.

Da bi to napravili, moramo razviti $\wp(z)$ i $\wp'(z)^2$ oko ishodišta. Budući da su obe parne, samo parne potencije od z će se pojaviti.

Neka je c najmanja apsolutna vrijednost, različita od nule, točke na rešetki L. Uzmimo $r < 1$ i pretpostavimo da je z u krugu radijusa $r \cdot c$ oko ishodišta. Za svaki $l \in L$, razvijmo član koji odgovara l-u u definiciji (5.1) od $\wp(z)$. To možemo učiniti deriviranjem geometrijskog reda $\frac{1}{1-x} = 1 + x + x^2 + \cdots$ i uvrštavanjem z/l za x:

$$\frac{1}{(1 - \frac{z}{l})^2} = 1 + 2\frac{z}{l} + 3\frac{z^2}{l^2} + 4\frac{z^3}{l^3} + \cdots.$$

Ako od obadvije strane oduzmemo 1, podijelimo sve s l^2 i uvrstimo u (5.1) dobivamo:

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{l \in L \\ l \neq 0}} \left(2\frac{z}{l^3} + 3\frac{z^2}{l^4} + 4\frac{z^3}{l^5} + \cdots + (k-1)\frac{z^{k-2}}{l^k} + \cdots \right).$$

Tvrdimo da taj dvostruki red apsolutno konvergira za $|z| < rc$, te će tada zamjenom poretka sumacije biti:

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \cdots, \tag{7.2}$$

gdje je za $k > 2$

$$G_k = G_k(L) = G_k(\omega_1, \omega_2) \underset{\text{def}}{=} \sum_{\substack{l \in L \\ l \neq 0}} l^{-k} = \sum_{\substack{m,n \in \mathbb{Z} \\ m^2 + n^2 \neq 0}} \frac{1}{(m\omega_1 + n\omega_2)^k} \tag{7.3}$$

(uočimo da je G_k nula za neparni k, jer se član od l poništava s članom od $-l$; kao što smo i očekivali, samo parne potencije od z se pojavljuju u izrazu (7.2)). Da dokažemo tvrdnju apsolutne konvergencije dvostrukog reda, zapišimo zbroj apsolutnih vrijednosti članova u unutrašnjoj sumi u obliku:

$$2|z|\cdot|l|^{-3}\cdot\left(1+\frac{3}{2}r+\frac{4}{2}r^2+\frac{5}{2}r^3+\cdots\right)<\frac{2|z|}{(1-r)^2}\frac{1}{|l|^3},$$

i iskoristimo Lemu 2 kod Propozicije 6.

Iskoristimo (7.2) za izračunavanje prvih nekoliko članova u razvoju od $\wp(z)$, $\wp(z)^2$, $\wp(z)^3$, $\wp'(z)$ i $\wp'(z)^2$:

$$\wp'(z)=-\frac{2}{z^3}+6G_4z+20G_6z^3+42G_8z^5+\cdots; \tag{7.4}$$

$$\wp'(z)^2=\frac{4}{z^6}-24G_4\frac{1}{z^2}-80G_6+\left(36G_4^2-168G_8\right)z^2+\cdots; \tag{7.5}$$

$$\wp(z)^2=\frac{1}{z^4}+6G_4+10G_6z^2+\cdots; \tag{7.6}$$

$$\wp(z)^3=\frac{1}{z^6}+9G_4\frac{1}{z^2}+15G_6+\left(21G_8+27G_4^2\right)z^2+\cdots. \tag{7.7}$$

Jedino što trebamo, je naći koeficijente a, b, c, d kubnog polinoma $f(x)=ax^3+bx^2+cx+d$, takvog da je $\wp'(z)^2=a\wp(z)^3+b\wp(z)^2+c\wp(z)+d$, a za to je dovoljno da se obe strane slažu u razvojima do konstantnog člana. Ako pomnožimo jednadžbu (7.7) s a, jednadžbu (7.6) s b, a jednadžbu (7.2) s c, dodamo ih sve konstanti d, te izjednačimo koeficijente uz z^{-6}, z^{-4}, z^{-2} i konstantni član odgovarajućem koeficijentu u (7.5), dobijemo:

$$a=4;\qquad b=0;\qquad -24G_4=4(9G_4)+c;\qquad -80G_6=4(15G_6)+d.$$

Vidimo da vrijedi $c=-60G_4$, $D=-140G_6$. Tradicionalno se označava:

$$\begin{aligned}\boldsymbol{g_2}&=g_2(L)\underset{\text{def}}{=}60G_4=60\sum_{\substack{l\in L\\ l\neq 0}}l^{-4};\\ \boldsymbol{g_3}&=g_3(L)\underset{\text{def}}{=}140G_6=140\sum_{\substack{l\in L\\ l\neq 0}}l^{-6}.\end{aligned} \tag{7.8}$$

Odatle izvedimo drugi oblik diferencijalne jednadžbe (7.1):

$$\wp'(z)^2=f(\wp(z)),\qquad \text{gdje je } f(x)=4x^3-g_2x-g_3\in\mathbb{C}[x]. \tag{7.9}$$

Diferencijalna jednadžba (7.9) ima elegantnu i jednostavnu geometrijsku interpretaciju. Promatrajmo funkciju na torusu (tj. fundamentalnom paralelogramu sa slijepljenim suprotnim stranama) u $\mathbb{P}^2_{\mathbb{C}}$ definiranu s:

$$\begin{aligned}&z\mapsto(\wp(z),\wp'(z),1)\quad\text{za}\quad z\neq 0;\\ &0\mapsto(0,1,0).\end{aligned} \tag{7.10}$$

Slika z u $\mathbb{C}/L$ bilo koje točke različite od nule je točka u xy-ravnini (s kompleksnim koordinatama) čije x- i y-koordinate zadovoljavaju odnos $y^2 = f(x)$ zbog (7.9). Ovdje je $f(x) \in \mathbb{C}[x]$ kubni polinom s različitim nultočkama, pa se svaka točka u $\mathbb{C}/L$ preslikava u točku na eliptičkoj krivulji $y^2 = f(x)$ u $\mathbb{P}^2_{\mathbb{C}}$. Nije teško uočiti da je to preslikavanje bijekcija između $\mathbb{C}/L$ i eliptičke krivulje (uključujući njenu točku u beskonačnosti). Naime, svaka x-vrijednost, osim nultočki od $f(x)$ (i beskonačnosti), ima točno dva z-a takva da je $\wp(z) = x$. y-koordinate $y = \wp'(z)$ koje dolaze od ta dva z-a su kvadratni korijeni od $f(x) = f(\wp(z))$. Ako se ipak dogodi da x bude nultočka od $f(x)$, onda postoji samo jedna vrijednost za z, takva da je $\wp(z) = x$, a odgovarajuća y-koordinata je $y = \wp'(z) = 0$, tako da ponovo imamo rješenja jednadžbe $y^2 = f(x)$ za naš dani x.

Nadalje, preslikavanje iz $\mathbb{C}/L$ na našu eliptičku krivulju u $\mathbb{P}^2_{\mathbb{C}}$ je analitičko, što znači da ga u blizini bilo koje točke u $\mathbb{C}/L$ možemo zamijeniti trojkom analitičkih funkcija. Blizu točke iz $\mathbb{C}$ koja nije na rešetki, preslikavanje je dano sa $z \mapsto (\wp(z), \wp'(z), 1)$, a u blizini točke na rešetki dano je sa $z \mapsto \left(\frac{\wp(z)}{\wp'(z)}, 1, \frac{1}{\wp'(z)} \right)$, što je trojka analitičkih funkcija u blizini L.

Dokazali smo sljedeću propoziciju:

Propozicija 10. *Preslikavanje (7.10) je analitička bijekcija između* $\mathbb{C}/L$ *i eliptičke krivulje* $f(x) = 4x^3 - g_2(L)x - g_3(L)$ *u* $\mathbb{P}^2_{\mathbb{C}}$. ■

Nekoga će možda zanimati kako se može konstruirati inverzno preslikavanje sa eliptičke krivulje na $\mathbb{C}/L$. To se može postići integriranjem $dx/y = (4x^3 - g_2 x - g_3)^{-1/2} dx$ od čvrste početne točke s promjenjivom završnom točkom. Dobiveni integral ovisi o putu, ali se mijenja samo za "period", tj. za element rešetke, ako promijenimo put. Tako smo dobili dobro definirano preslikavanje u $\mathbb{C}/L$.

8. Zbrajanje točaka

U prošlom poglavlju vidjeli smo da Weierstrassova $\wp$-funkcija daje vezu između točaka na $\mathbb{C}/L$ i točaka na eliptičkoj krivulji $y^2 = f(x) = 4x^3 - g_2(L)x - g_3(L)$ u $\mathbb{P}^2_{\mathbb{C}}$. Imamo očigledno zbrajanje točaka u $\mathbb{C}/L$, dobiveno od običnog zbrajanja "modulo L". To je dvodimenzionalna analogija "zbrajanja modulo jedan" u grupi $\mathbb{R}/\mathbb{Z}$.

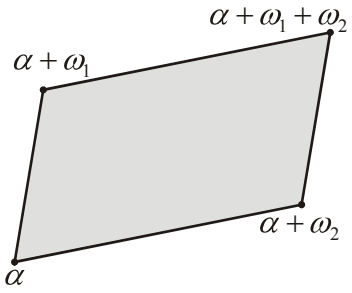
Možemo iskoristiti povezanost između $\mathbb{C}/L$ i eliptičke krivulje da dobijemo zbrajanje točaka na eliptičkoj krivulji. Tj. da bi zbrojili dvije točke

$P_1 = (x_1, y_1)$ i $P_2 = (x_2, y_2)$, po definiciji se vratimo u z-ravninu, nađemo z_1 i z_2 takve da je $P_1 = (\wp(z_1), \wp'(z_1))$ i $P_2 = (\wp(z_2), \wp'(z_2))$ i onda postavimo $P_1 + P_2 = (\wp(z_1 + z_2), \wp'(z_1 + z_2))$. To je uobičajeni način. Uvijek kada imamo bijekciju između elemenata komunitativne grupe i elemenata nekog drugog skupa, možemo iskoristiti bijekciju da definiramo operaciju grupe (zbrajanje) u tom drugom skupu.

Prekrasna svojstva zbrajanja koje smo na taj način dobili su da (1) postoji jednostavna geometrijska interpretacija "zbrajanja" točaka na eliptičkoj krivulji i (2) da se koordinate točke $P_1 + P_2$ mogu izraziti direktno kao jednostavna racionalna funkcija varijabli x_1, x_2, y_1, y_2. U ovom poglavlju ćemo sve to opisati.

Dokažimo prvo jednu opću lemu o eliptičkim funkcijama.

Lema. *Neka je* $f(z) \in \mathcal{E}_L$. *Neka je* $\Pi = \{a\omega_1 + b\omega_2 \mid 0 \le a, b \le 1\}$ *fundamentalni paralelogram rešetke* L. *Izaberimo* α *tako da* $f(z)$ *nema nultočaka ni polova na rubu od* $\alpha + \Pi$. *Neka je* $\{a_i\}$ *skup svih nultočki od* $f(z)$ *u* $\alpha + \Pi$, *svaka ponovljena onoliko puta koliki joj je red, a* $\{b_j\}$ *skup svih polova, svaki ponovljen onoliko puta koliki mu je red. Tada je* $\sum a_i - \sum b_i \in L$.



Slika 8

Dokaz: Sjetimo se da funkcija $\frac{f'(z)}{f(z)}$ ima polove u nultočkama i polovima od $f(z)$. Njen razvoj oko nultočke a reda m je $\frac{m}{z-a} + \cdots$, a razvoj blizu pola b reda $-m$ je $-\frac{m}{z-b} + \cdots$. Tada funkcija $\frac{zf'(z)}{f(z)}$ ima iste polove, ali ako uvrstimo $z = a + (z - a)$ vidimo da razvoj počinje sa $\frac{am}{z-a}$. Zaključujemo da je $\sum a_i - \sum b_i$ zbroj reziduuma od $\frac{zf'(z)}{f(z)}$ u unutrašnjosti $\alpha + \Pi$. Neka je C rub od $\alpha + \Pi$. Po rezidualnom teoremu vrijedi:

$$\sum a_i - \sum b_i = \frac{1}{2\pi i} \int_C \frac{zf'(z)}{f(z)} dz.$$

Izračunajmo prvo integral na suprotnim stranama od α do $\alpha + \omega_2$ i od $\alpha + \omega_1$ do $\alpha + \omega_1 + \omega_2$ (vidi Sliku 8). Taj dio je jednak

$$\frac{1}{2\pi i}\left(\int_{\alpha}^{\alpha+\omega_2} z\frac{f'(z)}{f(z)}dz - \int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz \right) =$$

$$= \frac{1}{2\pi i}\left(\int_{\alpha}^{\alpha+\omega_2} z\frac{f'(z)}{f(z)}dz - \int_{\alpha}^{\alpha+\omega_2} (z+\omega_1)\frac{f'(z)}{f(z)}dz \right) =$$

$$= -\omega_1 \frac{1}{2\pi i} \int_{\alpha}^{\alpha+\omega_2} \frac{f'(z)}{f(z)}dz.$$

Uvedimo zamjenu $u = f(z)$, $\frac{f'(z)}{f(z)}dz = \frac{du}{u}$. Neka je C_1 zatvoreni put od $f(\alpha)$ do $f(\alpha + \omega_2) = f(\alpha)$ parametriziran sa $u = f(z)$ kad z ide od α do $\alpha + \omega_2$. Tada je

$$\frac{1}{2\pi i}\int_{\alpha}^{\alpha+\omega_2} \frac{f'(z)}{f(z)}dz = \frac{1}{2\pi i}\int_{C_1}\frac{du}{u},$$

i to je neki cijeli broj n. Naime broj koliko puta zatvoreni put C_1 obiđe oko ishodišta (brojeći u smjeru kazaljke na satu). Tako da za taj dio našeg integrala dobivamo $-\omega_1 n$. Na isti način dobivamo da je integral na preostale dvije strane od C jednak $-\omega_2 m$, gdje je m neki cijeli broj. Tako da je $\sum a_i - \sum b_i = -\omega_1 n - \omega_2 m \in L$, kako smo i željeli. ■

Sada možemo izvesti geometrijski postupak za zbrajanje dviju točaka na eliptičkoj krivulji $y^2 = f(x) = 4x^3 - g_2(L)x - g_3(L)$. Za z iz $\mathbb{C}/L$, neka je P_z odgovarajuća točka $P_z = (\wp(z), \wp'(z), 1)$, $P_0 = (0,1,0)$ na eliptičkoj krivulji. Pretpostavimo da želimo zbrojiti $P_{z_1} = (x_1, y_1)$ i $P_{z_2} = (x_2, y_2)$ da bismo dobili $P_{z_1+z_2} = (x_3, y_3)$. Želimo znati kako od dvije točke doći do njihovog zbroja direktno, bez promatranja točaka nazad u z-ravnini.

Prvo pogledajmo neke specijalne slučajeve. Neutralni element je naravno slika od $z = 0$. Neka $\mathcal{O}$ označava točku u beskonačnosti $(0,1,0)$, tj. neutralni element naše grupe točaka. Zbrajanje je trivijalno ako je jedna točka $\mathcal{O}$, tj. ako je z_1 ili z_2 nula.

Pretpostavimo sada da P_{z_1} i P_{z_2} imaju istu x-koordinatu, ali nisu iste točke. To znači da $x_2 = x_1$, $y_2 = -y_1$. U tom slučaju $z_2 = -z_1$, jer samo "simetrične" vrijednosti od z (vrijednosti koje su negativne jedna drugoj modulo rešetka L, tj. z i z' iz šestog poglavlja) mogu imati istu $\wp$-vrijednost. U tom slučaju je $P_{z_1} + P_{z_2} = P_0 = \mathcal{O}$, tj. te su dvije točke aditivni inverzi jedna drugoj. Govoreći geometrijski, možemo reći da je zbroj dviju točaka na istom vertikalnom pravcu jednak $\mathcal{O}$. U specijalnom slučaju točke $P_{z_1} = P_{z_2}$ na x-osi, imamo $y_2 = -y_1 = 0$, i lako je provjeriti da još uvijek vrijedi $P_{z_1} + P_{z_2} = 2P_{z_1} = \mathcal{O}$. Dokazali smo:

Propozicija 11. *Aditivni inverz od* (x,y) *je* $(x,-y)$. ■

Neka su dane dvije točke $P_1 = P_{z_1} = (x_1, y_1)$ i $P_2 = P_{z_2} = (x_2, y_2)$ na eliptičkoj krivulji $y^2 = 4x^3 - g_2 x - g_3$ (nijedna nije točka u beskonačnosti $\mathcal{O}$). Postoji pravac $p = \overline{P_1 P_2}$ koji ih spaja. Ako je $P_1 = P_2$, tada je p tangenta na eliptičku krivulju u točki P_1. Ako je p vertikalni pravac, onda je $P_1 + P_2 = \mathcal{O}$. Pretpostavimo da p nije

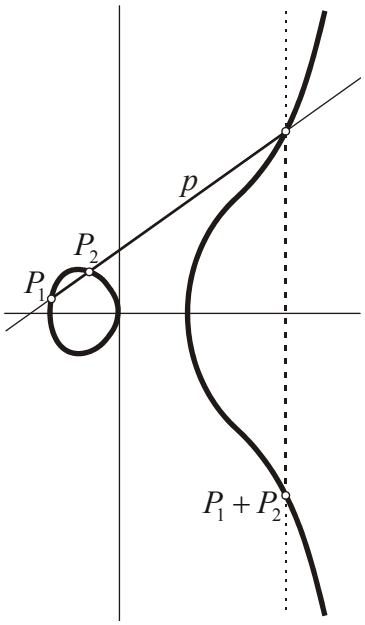
vertikalni pravac. Želimo naći $P_1 + P_2 = P_3 = (x_3, y_3)$. Tvrdimo da je $-P_3 = (x_3, -y_3)$ treća točka presjeka eliptičke krivulje i pravca p.

Zapišimo jednadžbu pravca $p = \overline{P_1P_2}$ u obliku $y = ax + b$. Točka (x, y) na pravcu p je na eliptičkoj krivulji ako i samo ako je $(ax+b)^2 = f(x) = 4x^3 - g_2x - g_3$, tj. ako i samo ako je x nultočka kubne jednadžbe $f(x) - (ax+b)^2$. Ta jednadžba ima tri nultočke – svaka daje točku presjeka. Ako je x dvostruka ili trostruka nultočka, tada p presjeca krivulju s redom dva ili tri u točki (x, y). U svakom slučaju, ukupan broj točaka presjeka je tri (brojeći red).

Uočimo da vertikalni pravac također siječe krivulju u tri točke, uključujući točku u beskonačnosti $\mathcal{O}$, a pravac u beskonačnosti ima trostruki presjek u $\mathcal{O}$. Na taj način svaki pravac u $\mathbb{P}^2_{\mathbb{C}}$ siječe krivulju u tri točke. To je specijalan slučaj od:

Bezoutov teorem. *Neka su $\widetilde{F}(x,y,z)$ i $\widetilde{G}(x,y,z)$ homogeni polinomi stupnjeva m i n, respektivno, nad algebarski zatvorenim poljem K. Pretpostavimo da $\widetilde{F}$ i $\widetilde{G}$ nemaju zajednički polinomski faktor. Tada krivulje u $\mathbb{P}^2_K$ definirane s $\widetilde{F}$ i $\widetilde{G}$ imaju $m \cdot n$ točaka presjeka, brojeći red svake nultočke.* ■

U našem slučaju je $\widetilde{F}(x,y,z) = y^2z - 4x^3 + g_2xz^2 + g_3z^3$ i $\widetilde{G}(x,y,z) = y - ax - bz$.



Slika 9

Propozicija 12. *Ako je $P_1 + P_2 = P_3$, tada je $-P_3$ treća točka presjeka pravca $p = \overline{P_1P_2}$ s eliptičkom krivuljom. Ako je $P_1 = P_2$, tada pod $\overline{P_1P_2}$ mislimo na tangentu u P_1.*

Dokaz: Već smo provjerili slučajeve kada je P_1 ili P_2 točka u beskonačnosti $\mathcal{O}$, i kada je $P_2 = -P_1$. Neka je pravac $p = \overline{P_1P_2}$ u obliku $y = ax + b$ i je $P_1 = P_{z_1}$, $P_2 = P_{z_2}$. Točka $P_z = (\wp(z), \wp'(z))$ leži na p ako $\wp'(z) = a\wp(z) + b$. Eliptička funkcija $\wp'(z) - a\wp(z) - b$ ima tri pola, pa i tri nultočke u $\mathbb{C}/L$. I z_1 i z_2 su nultočke. Prema prethodnoj lemi zbroj triju nultočki i tri pola je jednak 0 mudulo mreža L. Sva tri pola su u nuli (gdje $\wp'(z)$ ima trostruki pol), tako da je treća nultočka $-(z_1 + z_2)$ modulo mreža. Iz toga se vidi da je treća točka presjeka pravca p i krivulje točka $P_{-(z_1+z_2)} = -P_{z_3}$, kako smo tvrdili.

Argument u prošlom odlomku je dobar samo ako su tri točke presjeka pravca p s eliptičkom krivuljom različite, pa u tom slučaju nultočka od $\wp'(z) - a\wp(z) - b$ odgovara točno točki presjeka P_z. U suprotnom moramo pokazati da dvostruka ili trostruka nultočka na eliptičkoj funkciji uvijek odgovara dvostrukom ili trostrukom presjeku, respektivno, pravca p s krivuljom. Zato moramo pokazati da se ta dva značenja izraza "red" slažu: red nultočke na eliptičkoj krivulji variable z i red presjeka u xy-ravnini.

Neka su $z_1, z_2, -z_3$ tri nultočke od $\wp'(z) - a\wp(z) - b$, stavljene toliko puta koliki im je red. Uočimo da nijedna od tih točaka nije negativna druga, jer p nije vertikalan pravac. Budući da su $-z_1, -z_2, z_3$ tri nultočke od $\wp'(z) + a\wp(z) + b$, slijedi da su $\pm z_1, \pm z_2, \pm z_3$ šest nultočki od $\wp'(z)^2 - (a\wp(z) + b)^2 = f(\wp(z)) - (a\wp(z) + b)^2 = 4(\wp(z) - x_1)(\wp(z) - x_2)(\wp(z) - x_3)$, gdje su x_1, x_2, x_3 nultočke od $f(x) - (ax + b)^2$. Ako je, na primjer, $\wp(z_1) = x_1$, tada red od x_1 ovisi o broju $\pm z_2, \pm z_3$ koji su jednaki $\pm z_1$. Ali to je točno broj od $z_2, -z_3$ koji su jednaki z_1. Stoga "red" ima isto značenje u oba slučaja. ■

Propozicija 12 nam daje Sliku 9, koja prikazuje grupu realnih točaka na eliptičkoj krivulji $y = x^3 - x$. Da bismo zbrojili dvije točke P_1 i P_2, povučemo pravac koji ih spaja, nađemo treću točku presjeka tog pravca i krivulje, te uzmemo simetričnu točku s druge strane x-osi.

Zbrajanje smo mogli definirati u geometrijskom smislu otpočetka i direktno dokazati aksiome abelove grupe. Najteži dio bilo bi svojstvo asocijativnosti, koje bi zahtijevalo dublje istraživanje točaka presjeka.

Čini se da postoji prilična sloboda u definiranju zbrajanja. Na primjer, osim točke u beskonačnosti, za neutralni element smo mogli izabrati bilo koju točku infleksije.

Jedina mana našeg pristupa koristeći $\wp(z)$ je da se on apriori odnosi samo na eliptičke krivulje oblika $y^2 = 4x^3 - g_2(L)x - g_3(L)$ i krivulje koje se mogu transformirati u taj oblik linearnom zamjenom varijabli. (Uočimo da će geometrijski opis zbrajanja davati abelovu grupu i nakon linearne zamjene varijabli.) Ustvari, svaka eliptička krivulja nad kompleksnim brojevima može se transformirati u Weierstrassov oblik za neku mrežu L (dokaz nije baš jednostavan). Također se pokaže da naš omiljeni primjer $y^2 = x^3 - n^2x$ odgovara mreži Gaussovih cijelih brojeva.

Nije teško taj geometrijski postupak prenijeti u formule i izraziti koordinate (x_3, y_3) zbroja $P_1 = (x_1, y_1)$ i $P_2(x_2, y_2)$ kao funkciju od x_1, x_2, y_1, y_2 i koeficijenata jednadžbe eliptičke krivulje. Pa ipak, precizno govoreći, naš izvod je bio za eliptičke krivulje oblika $y^2 = f(x) = 4x^3 - g_2(L)x - g_3(L)$ za neku mrežu L, a postupak daje abelovu grupu za sve eliptičke krivulje $y^2 = f(x)$, kako je

navedeno gore. Pa neka je $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{C}[x]$ bilo koji polinom trećeg stupnja s različitim nultočkama.

Ubuduće ćemo pretpostavljati da ni P_1 ni P_2 nije točka u beskonačnosti $\mathcal{O}$, i da je $P_1 \neq -P_2$. Tada se pravac kroz P_1 i P_2 (ili tangenta u P_1, ako je $P_1 = P_2$) može zapisati u obliku $y = \alpha x + \beta$, gdje je $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$ ako je $P_1 \neq P_2$, a $\alpha = \left.\frac{dy}{dx}\right|_{(x_1, y_1)}$, ako je $P_1 = P_2$. U drugom slučaju, α se može izraziti preko x_1 i y_1 implicitnom derivacijom $y^2 = f(x)$; tako dobijemo da je $\alpha = \frac{f'(x_1)}{2y_1}$. U oba slučaja odsječak na y-osi je $\beta = y_1 - \alpha x_1$.

Tada je x_3, x-koordinata zbroja, treća nultočka kubika $f(x) - (\alpha x + \beta)^2$, čije dvije nultočke su x_1 i x_2. Budući je zbroj tri nultočke jednak negativnom koeficijentu uz x^2 podijeljenom s vodećim koeficijentom, imamo: $x_1 + x_2 + x_3 = -\frac{b - \alpha^2}{a}$, pa je i:

$$x_3 = -x_1 - x_2 - \frac{b}{a} + \frac{1}{a}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2, \text{ ako je } P_1 \neq P_2; \tag{8.1}$$

$$x_3 = -2x_1 - \frac{b}{a} + \frac{1}{a}\left(\frac{f'(x_1)}{2y_1}\right)^2, \qquad \text{ako je } P_1 = P_2. \tag{8.2}$$

y-koordinata y_3 je negativna vrijednost od $y = \alpha x_3 + \beta$, tj.

$$y_3 = -y_1 + \alpha(x_1 - x_3), \tag{8.3}$$

gdje je x_3 dan sa (8.1) i (8.2), i

$$\begin{aligned} \alpha &= \frac{y_2 - y_1}{x_2 - x_1}, \text{ ako je } P_1 \neq P_2; \\ \alpha &= \frac{f'(x_1)}{2y_1}, \text{ ako je } P_1 = P_2. \end{aligned} \tag{8.4}$$

Ako je naša krivulja u Weierstrassovom obliku $y^2 = 4x^3 - g_2 x - g_3$, tada imamo $a = 4$, $b = 0$ i $f'(x_1) = 12x_1^2 - g_2$ uz formule (8.1)–(8.4).

U načelu, mogli bismo jednostavno definirati zbrajanje po tim formulama i algebarski provjeriti da su aksiomi komutativne grupe zadovoljeni. Najteže bi bilo provjeriti asocijativnost. To bi bilo vrlo zamorno, ali imali bi i jednu prednost. Naime, nikad ne bi koristili činjenicu da je naše polje K nad kojim je eliptička krivulja definirana, polje kompleksnih brojeva, ni da je karakteristike nula. Tj. našli bi formule, koje imaju smisla u svakom polju karakteristike različite od 2, koje daju abelovu grupu. To znači: ako je $y^2 = f(x) = ax^3 + bx^2 + cx + d \in K[x]$ jednadžba eliptičke krivulje nad K i ako definiramo $f'(x) = 3ax^2 + 2bx + c$, onda se svake dvije točke koje imaju koordinate u nekom proširenju od K mogu

zbrajati koristeći formule (8.1)–(8.4). Ove činjenice ćemo koristiti ubuduće, iako, striktno govoreći, nismo izradili dosadnu algebarsku provjeru aksioma grupe.

Napomena: *Neka je* $P=(x_P,y_P)$ *i* $y=x^3-n^2x$. *Točka* $2P=P+P=(x_{2P},y_{2P})$ *zadovoljava:*

$$x_{2P}=\left(\frac{3x_P^2-n^2}{2y_P}\right)^2-2x_P,\qquad y_{2P}=-y_P+\left(x_P-x_{2P}\right)\frac{3x_P^2-n^2}{2y_P}. \tag{8.5}$$

9. Točke konačnog reda

U svakoj grupi, elemente razlučujemo na one konačnog reda i one beskonačnog. U abelovoj grupi, skup elemenata konačnog reda čini podgrupu, koju zovemo "**torziona podgrupa**". U slučaju grupe točaka u $\mathbb{P}^2_{\mathbb{C}}$ na eliptičkoj krivulji $y^2=f(x)$ odmah se vidi da je točka $P_z=(x,y)$ konačnog reda ako i samo ako je $nz\in L$, za neki n, tj. ako i samo ako je z racionalna linearna kombinacija od ω_1 i ω_2. U tom slučaju, najmanji n (koji je najmanji zajednički nazivnik koeficijenata od ω_1 i ω_2) je red od P_z. U izomorfizmu iz $\mathbb{R}/\mathbb{Z}\times\mathbb{R}/\mathbb{Z}$ na eliptičku krivulju danom s $(a,b)\mapsto P_{a\omega_1+b\omega_2}$, to je slika od $\mathbb{Q}/\mathbb{Z}\times\mathbb{Q}/\mathbb{Z}$ koja je torziona podgrupa eliptičke krivulje.

Ovo je dvodimenzionalna analogija kružne grupe, čija je torziona podgrupa upravo grupa svih korijena jedinica, tj. svi $e^{2\pi iz}$, za $z\in\mathbb{Q}/\mathbb{Z}$. Kao što su "ciklotomska polja" – polja proširenja od $\mathbb{Q}$ generirana korijenima jedinice – centralna u algebarskoj teoriji brojeva, za očekivati je da će polja dobivena dodavanjem koordinata točaka reda n eliptičke krivulje imati posebna svojstva. Može se pokazati da su te koordinate algebarski brojevi (ako su to koeficijenti od $f(x)$). Ta analogija između ciklotomskih polja i polja točaka konačnog reda na eliptičkim krivuljama zapravo je mnogo dublja nego što smo mogli pretpostaviti. Ustvari, glavno područje proučavanja algebarske teorije brojeva danas se sastoji od traženja i dokazivanja analogija za takva polja od rezultata koji vrijede za ciklotomska polja.

Neka je n čvrsti prirodni broj. Neka je $f(x)=ax^3+bx^2+cd+d=a(x-e_1)(x-e_2)(x-e_3)$ kubni polinom s koeficijentima iz polja K karakteristike $\neq 2$ s različitim nultočkama (možda u nekom proširenju od K). Nas zanima opis koordinata točaka reda n na eliptičkoj krivulji $y^2=f(x)$, gdje te koordinate mogu ležati u proširenju od K. Ako je $n=2$, točke reda n su točka u beskonačnosti $\mathcal{O}$ i $(e_i,0), i=1,2,3$. Sada pretpostavimo da je $n>2$. Ako je n neparan, netrivijalne točke reda n su točke $P\neq\mathcal{O}$ takvu da je $nP=\mathcal{O}$. Ako je n paran, to su točke P takve da je $nP=\mathcal{O}$, ali $2P\neq\mathcal{O}$.

Propozicija 13. *Neka je K' bilo koje polje proširenja od K (ne nužno algebarsko) i neka je $\sigma : K' \to \sigma K'$ bilo koji izomorfizam polja koji ostavlja fiksne sve elemente od K. Neka je $P \in \mathbb{P}^2_K$ točka reda n na eliptičkoj krivulji $y^2 = f(x)$, gdje je $f(x) \in K[x]$. Tada je σP također reda n (gdje za $P = (x, y, z) \in \mathbb{P}^2_{K'}$, označavamo $\sigma P = (\sigma x, \sigma y, \sigma z) \in \mathbb{P}^2_{\sigma K'}$).*

Dokaz: To slijedi iz adicionih formula $\sigma P_1 + \sigma P_2 = \sigma(P_1 + P_2)$, i zato što je $n(\sigma P) = \sigma(nP) = \sigma\mathfrak{O} = \mathfrak{O}$ (budući je $\sigma(0,1,0) = (0,1,0)$). Zaključujemo da je σP reda n. Mora biti reda točno n, jer ako postoji $n' < n$ takav da je $n'\sigma P = \mathfrak{O}$, imali bi $\sigma(n'P) = \mathfrak{O} = (0,1,0)$, tj. $n'P = \mathfrak{O}$, što je kontradikcija. To dokazuje propoziciju. ■

Propozicija 14. *U uvjetima Propozicije 13, neka je K podpolje od $\mathbb{C}$, te neka je $K_n \subset \mathbb{C}$ polje dobiveno dodavanjem K-u x- i y-koordinata svih točaka reda n. Neka je K_n^+ polje dobiveno dodavanjem samo njihovih x-koordinata. Tada su i K_n i K_n^+ konačna proširenja od K.*

Dokaz: U oba slučaja K_n i K_n^+, dodali smo konačan skup kompleksnih brojeva. Oni su permutirani po nekom automofrizmu $\mathbb{C}$-a, koji fiksira K. Iz toga slijedi propozicija. ■

Na primjer, ako je $n = 2$, tada je $K_2 = K_2^+$ polje razlaganja od $f(x)$ nad K. Grupa točaka reda n na eliptičkoj krivulji u $\mathbb{P}^2_{\mathbb{C}}$ je izomorfna sa $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. Jer svaki $\sigma \in \mathrm{Gal}\left(K_n/K\right)$ (to su oni σ iz Propozicije 13) poštuje zbrajanje točaka, što znači: $\sigma P_1 + \sigma P_2 = \sigma(P_1 + P_2)$. Slijedi da svaki σ daje invertibilno linearno preslikavanje sa $(\mathbb{Z}/n\mathbb{Z})^2$ na sebe.

Ako je R neki komutativni prsten, sa $GL_n(R)$ označimo grupu (uz matrično množenje) svih $n \times n$ invertibinih matrica s članovima iz R. Ovdje je invertibilnost matrice A ekvivalentna sa $\det A \in R^*$, gdje je R^* multiplikativna grupa invertibilnih elemenata prstena. Na primjer:

(1) $GL_1(R) = R^*$;

(2) $GL_2\left(\mathbb{Z}/n\mathbb{Z}\right) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}/n\mathbb{Z}, ad - bc \in \left(\mathbb{Z}/n\mathbb{Z}\right)^* \right\}$.

Lako je konstruirati prirodnu bijekciju među invertibilnim linearnim preslikavanjima $R^n \to R^n$ i elementima od $GL_n(R)$. Nema nikakvih razlika od slučaja kada je R polje.

U našem slučaju točaka reda n na eliptičkoj krivulji vidjeli smo da je $\mathrm{Gal}\left(K_n/K\right)$ izomorfan podgrupi grupe svih invertibilnih linearnih preslikavanja $(\mathbb{Z}/n\mathbb{Z})^2 \to (\mathbb{Z}/n\mathbb{Z})^2$. Stoga, svaki $\sigma \in \mathrm{Gal}\left(K_n/K\right)$ odgovara matrici $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z}/n\mathbb{Z})$. Matrični elementi mogu se naći rješavanjem

$$\sigma P_{\frac{\omega_1}{n}} = P_{\frac{a\omega_1}{n}+\frac{c\omega_2}{n}}, \qquad \sigma P_{\frac{\omega_2}{n}} = P_{\frac{b\omega_1}{n}+\frac{d\omega_2}{n}}.$$

Uočimo da je to direktna generalizacija slučaja s n-tim cikličkim poljem $\mathbf{Q}_n \underset{\text{def}}{=} \mathbb{Q}\left(\sqrt[n]{1}\right)$. Sjetimo se da je $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \approx (\mathbb{Z}/n\mathbb{Z})^* = GL_1(\mathbb{Z}/n\mathbb{Z})$ s elementom a koji odgovara σ određenim s

$$\sigma\left(e^{\frac{2\pi i}{n}}\right) = e^{\frac{2\pi i a}{n}}.$$

Jedina razlika u našem dvodimenzionalnom slučaju dijeljenja točaka na eliptičkoj krivulji je ta da je $\mathrm{Gal}(K_n/K) \to GL_2(\mathbb{Z}/n\mathbb{Z})$ općenito samo injekcija, a ne izomorfizam.

U slučaju $K \subset \mathbb{C}$, recimo $K = \mathbb{Q}(g_2, g_3)$, gdje je $y^2 = f(x) = 4x^3 - g_2 x - g_3$ u Weierstrassovom obliku, iskoristit ćemo $\wp$-funkciju da odredimo polinome čije nultočke su x-koordinate točaka reda n. Tj. K_n^+ je polje razlaganja takvih polinoma.

Prvo konstruirajmo eliptičku funkciju $f_n(z)$ čije nultočke su točno vrijednosti od z, različite od nule, takve da je P_z točka reda n. Slijedimo postupak kao u dokazu Propozicije 8. Ako je $u \in \mathbb{C}/L$ točka reda n, tada je i simetrična točka $-u$ (koju smo označavali sa u') reda n. Imamo dva slučaja:

(1) n je neparan. Tada su točke u i $-u$ uvijek različite modulo L. Drugim riječima, u ne može biti $\frac{\omega_1}{2}, \frac{\omega_2}{2}$ ni $\frac{\omega_1+\omega_2}{2}$ ako je neparnog reda. Definirajmo

$$f_n(z) = n\prod(\wp(z) - \wp(u)). \tag{9.1}$$

gdje se množi po svim $u \in \mathbb{C}/L$ različitim od nule, tako da je $nu \in L$, s uzetim jednim u od svakog para $u, -u$. Tada je $f_n(z) = F_n(\wp(z))$, gdje je $F_n(x) \in \mathbb{C}[x]$ polinom stupnja $\frac{n^2-1}{2}$. Parna eliptička funkcija $f_n(z)$ ima n^2-1 jednostrukih nultočaka i uklonjivi pol u nuli reda n^2-1. Njegov vodeći koeficijent u $z=0$ je $\frac{n}{z^{n^2-1}}$.

(2) n je paran. Neka u ide po svim $u \in \mathbb{C}/L$ takvim da je $nu \in L$, ali u nije reda 2, tj. $u \neq 0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$. Definirajmo $\widetilde{f}_n(z)$ kao produkt (9.1). Tada je $\widetilde{f}_n(z) = F_n(\wp(z))$, gdje je $F_n(x) \in \mathbb{C}[x]$ polinom stupnja $\frac{n^2-4}{2}$. Parna eliptička funkcija $\widetilde{f}_n(z)$ ima n^2-4 jednostrukih nultočaka i uklonjivi pol u nuli reda n^2-4. Njegov vodeći koeficijent u $z=0$ je $\frac{n}{z^{n^2-4}}$.

Ako je n neparan, tada funkcija $f_n(z)$ ima svojstvo

$$f_n(z)^2 = n^2 \prod_{0 \neq u \in \mathbb{C}/L, nu \in L} (\wp(z) - \wp(u)).$$

Ako je n paran, tada funkcija $f_n(z) \underset{\text{def}}{=} -\frac{1}{2}\wp'(z)\widetilde{f}_n(z)$ ima svojstvo

$$\begin{aligned} f_n(z)^2 &= \tfrac{1}{4}\wp'(z)^2 \widetilde{f}_n(z)^2 \\ &= n^2(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3) \prod_{u \in \mathbb{C}/L, nu \in L, 2u \notin L} (\wp(z) - \wp(u)) \\ &= n^2 \prod_{0 \neq u \in \mathbb{C}/L, nu \in L} (\wp(z) - \wp(u)). \end{aligned}$$

Vidimo da je točka $(x, y) = (\wp(z), \wp'(z))$ reda n ako i samo ako je $f_n(x) = 0$. Ona je parnog reda n ako i samo ako je ili $y = 0$ (tj. točka reda 2) ili $f_n(x) = 0$.

Zbog Propozicija 13 i 14, znamo da svaki automorfizam od $\mathbb{C}$ koji fiksira $K = \mathbb{Q}(g_2, g_3)$ permutira nultočke od f_n. Stoga su koeficijenti od f_n u $K = \mathbb{Q}(g_2, g_3)$.

Da nismo krenuli od eliptičke krivulje u Weierstrassovom obliku, nego recimo od $y^2 = f(x) = ax^3 + bx^2 + cx + d$, i da smo željeli izbjeći korištenje $\wp$-funkcije, mogli smo više puta primijeniti adicione formule (8.1)–(8.4) i za x-koordinatu od nP dobiti racionalnu funkciju od x i y, gdje je $P = (x, y)$. Mogli smo to pojednostaviti algebarski, iskoristivši odnos $y^2 = f(x)$. Završili bismo s izrazom u nazivniku koji iščezava ako i samo ako je nP točka u beskonačnosti, tj. ako i samo ako je P reda n.

Kakav oblik izraza bismo imali da dobijemo nazivnik x-koordinate od nP? Pretpostavimo na primjer, da je n neparan. Tada bi taj nazivnik bio izraz u $K[x, y]$ (y se pojavljuje s potencijom najviše 1), gdje je $K = \mathbb{Q}(a, b, c, d)$, i iščezava ako i samo ako je x jedna od $\frac{n^2-1}{2}$ vrijednosti x-koordinata netrivijalnih točaka reda n. Iz toga slijedi da izraz mora biti polinom u samo x s $\frac{n^2-1}{2}$ nultočaka. Slično, ako je n paran, taj nazivnik je oblika $y \cdot$(polinom samo u x), gdje taj polinom u $K[x]$ ima $\frac{n^2-4}{2}$ nultočaka.

Važno je napomenuti da je algebarski postupak opisan u posljednja dva odlomka primjenjiv na svaku eliptičku krivulju $y^2 = f(x)$ nad svakim poljem K karakteristike $\neq 2$, a ne samo na potpoljima kompleksnih brojeva. Tako da za svako polje K završavamo s izrazom u nazivniku x-koordinate od nP koji iščezava za najviše $n^2 - 1$ vrijednosti (x, y).

Za općenito polje, ipak, ne dobivamo nužno svih $n^2 - 1$ netrivijalnih točaka reda n. Naravno, ako K nije algebarski zatvoreno, koordinate točaka reda n mogu ležati u nekom proširenju od K. Osim toga, ako je K karakteristike p, tada može biti manje točaka reda n zbog drugog razloga:

vodeći koeficijent izraza u nazivniku iščezava modulo p, pa stupanj polinoma pada.

Ta diskusija dovodi do sljedeće propozicije:

Propozicija 15. *Neka je* $y^2 = f(x)$ *eliptička krivulja nad nekim poljem* K *karakteristike različite od* 2. *Tada postoji najviše* n^2 *točaka reda* n *nad bilo kojim proširenjem* K' *od* K. ■

Da bi pokazali jednu primjenu Propozicije 15, obratimo pažnju na slučaj kada je K konačno polje. Kasnije ćemo se detaljnije vratiti eliptičkom krivuljama nad konačnim poljima.

Budući je samo konačno mnogo točaka u $\mathbb{P}^2_{\mathbb{F}_q}$ (naime, q^2+q+1), sigurno postoji samo konačno mnogo $\mathbb{F}_q$-točaka na eliptičkoj krivulji $y^2 = f(x)$, gdje je $f(x) \in \mathbb{F}_q[x]$. Stoga je grupa $\mathbb{F}_q$-točaka konačna abelova grupa.

Pod "**tipom**" konačne abelove grupe mislimo na njen prikaz kao produkta cikličkih grupa reda potencije prostog broja. Promotrimo redove svih cikličkih grupa: $2^{\alpha_2}, 2^{\beta_2}, 2^{\gamma_2}, \ldots, 3^{\alpha_3}, 3^{\beta_3}, 3^{\gamma_3}, \ldots, 5^{\alpha_5}, 5^{\beta_5}, \ldots$. Propozicija 15 povlači da se samo određeni tipovi mogu pojaviti u slučaju grupe $\mathbb{F}_q$-točaka na $y^2 = f(x)$. Naime, za svaki prosti l postoje najviše dvije komponente l-te potencije l^{α_l} i l^{β_l}, jer bi u suprotnom imali više od l^2 točaka reda l. I dakako $l^{\alpha_l+\beta_l}$ mora biti jednako potenciji od l koja dijeli red grupe.

Kao primjer kako to radi, uzmimo eliptičku krivulju $y^2 = x^3 - n^2x$ nad $K = \mathbb{F}_q$ (konačno polje sa $q = p^f$ elemenata), gdje pretpostavljamo da p ne dijeli $2n$. U slučaju $q \equiv 3 \pmod 4$, prilično je jednostavno izračunati broj $\mathbb{F}_q$-točaka.

Propozicija 16. *Neka je* $q = p^f$, $p \nmid 2n$. *Pretpostavimo da je* $q \equiv 3 \pmod 4$. *Tada na eliptičkoj krivulji* $y^2 = x^3 - n^2x$ *ima* $q+1$ $\mathbb{F}_q$*-točaka.*

Dokaz: Prvo, postoje četiri točke reda 2: $\mathcal{O}$, $(0,0)$ i $(\pm n, 0)$. Izbrojimo sada sve parove (x,y) gdje je $x \neq 0, n, -n$. Poredajmo sada tih $q-3$ x-eva u parove $\{x,-x\}$. Budući da je $f(x) = x^3 - n^2x$ neparna funkcija, a -1 nije kvadrat u $\mathbb{F}_q$ (jer smo pretpostavili da je $q \equiv 3 \pmod 4$), slijedi da je točno jedan od brojeva $f(x)$ i $f(-x) = -f(x)$ kvadrat u $\mathbb{F}_q$. (Sjetimo se: U multiplikativnoj grupi konačnog polja, kvadrati čine podgrupu indeksa 2, pa je tako umnožak dva nekvadrata kvadrat, dok je umnožak kvadrata i nekvadrata nekvadrat.) U svakom slučaju, par $\{x,-x\}$ daje jedan kvadrat, pa dobivamo točno dvije točke: ili $\left(x, \pm\sqrt{f(x)}\right)$ ili

$\left(-x,\pm\sqrt{-f(x)}\right)$. Tako da nam tih $\frac{q-3}{2}$ parova daje $q-3$ točaka. Zajedno sa četiri točke reda dva, imamo ukupno $q+1$ $\mathbb{F}_q$-točaka. ■

Uočimo, kada je $q \equiv 3 \pmod 4$, broj $\mathbb{F}_q$-točaka na eliptičkoj krivulji $y^2 = x^3 - n^2 x$ ne ovisi o n. To ne vrijedi kada je $q \equiv 1 \pmod 4$.

Na primjer, Propozicija 16 govori nam da za $q = 7^3$ imamo $344 = 2^3 \cdot 43$ točaka. Budući da imamo četiri točke reda dva, tip grupe $\mathbb{F}_{343}$-točaka na $y^2 = x^3 - n^2 x$ je $(2,2^2,43)$.

10. Točke nad konačnim poljima i problem kongruentnih brojeva

Do sada su nas uglavnom zanimale eliptičke krivulje E nad $\mathbb{Q}$, specijalno eliptička krivulja $y^2 = x^3 - n^2 x$ koju ćemo označavati sa $\boldsymbol{E_n}$. Ako je K bilo koje polje karakteristike p koji ne dijeli $2n$, ista jednadžba (gdje podrazumijevamo n modulo p) je eliptička krivulja nad K. Neka $E_n(K)$ označava skup točaka na krivulji s koordinatama iz K, tako da Propozicija 16 glasi: Ako je $q \equiv 3 \pmod 4$, tada je $\#E_n(\mathbb{F}_q) = q+1$.

Eliptičku krivulju E_n, kako smo je definirali nad $\mathbb{F}_p$, zovemo "**redukcija**" modulo p. Kažemo da E_n ima "**dobru redukciju**" ako p ne dijeli $2n$, tj. ako $y^2 = x^3 - n^2 x$ daje eliptičku krivulju nad $\mathbb{F}_p$.

Na prvi se pogled čini da eliptičke krivulje nad konačnim poljima – koje dovode samo do konačnih abelovih grupa – nisu ozbiljan problem i da je redukcija modulo p besposlena igra koja nam neće pomoći u našem proučavanju $\mathbb{Q}$-točaka na $y^2 = x^3 - n^2 x$, to je daleko od stvarnosti. Često se informacije iz različitih redukcija modulo p mogu skupiti zajedno i dati informaciju o $\mathbb{Q}$-točkama. To su teška razmatranja. Pa ipak, postoji jedna posljedica tog tipa koja je dovoljno jednostavna za nas. Naime, koristit ćemo redukciju modulo p za različite proste p-ove da odredimo torzionu podgrupu od $E_n(\mathbb{Q})$, grupu $\mathbb{Q}$-točaka na $y^2 = x^3 - n^2 x$.

U svakoj abelovoj grupi elementi konačnog reda čine podgrupu koju zovemo "torziona podgrupa". Na primjer, grupa $E(\mathbb{C})$ kompleksnih točaka na eliptičkoj krivulji izomorfna je sa $\mathbb{C}/L$, koji je za svaku rešetku L izomorfan $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. Njegova torziona grupa odgovara podgrupi $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$, tj. u $\mathbb{C}/L$ se sastoji od svih racionalnih kombinacija od ω_1 i ω_2.

Osnovni Mordellov teorem kaže da je grupa $E(\mathbb{Q})$ (grupa $\mathbb{Q}$-točaka na eliptičkoj krivulji E) konačno generirana abelova grupa. To znači da je (1) torziona podgrupa $E(\mathbb{Q})_{\text{tors}}$ konačna, i (2) $E(\mathbb{Q})$ je izomorfna direktnom zbroju $E(\mathbb{Q})_{\text{tors}}$ i konačnog broja kopija od $\mathbb{Z}$: $E(\mathbb{Q}) \approx E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$. Nenegativni cijeli broj r se zove "**rang**" od $E(\mathbb{Q})$. Veći je od nule ako i samo ako E ima beskonačno mnogo $\mathbb{Q}$-točaka. Mordellov teorem također je istinit, ako $\mathbb{Q}$ zamijenimo bilo kojim poljem algebarskih brojeva. Ta generalizacija, koju je dokazao André Weil, poznata je kao Mordell–Weilov teorem. Taj teorem neće nam trebati, čak ni u obliku koji je dao Mordell.

Mi ćemo samo dokazati da su jedine racionalne točke konačnog reda na E_n četiri točke reda 2: $\mathcal{O}$ (točka u beskonačnosti), $(0,0)$, $(\pm n,0)$.

Propozicija 17. $\#E_n(\mathbb{Q})_{\text{tors}} = 4$.

Dokaz: Ideja dokaza je konstruirati homomorfizam s $E_n(\mathbb{Q})_{\text{tors}}$ na $E_n(\mathbb{F}_p)$ koji je injektivan za većinu p-ova. To će povlačiti da red od $E_n(\mathbb{Q})_{\text{tors}}$ dijeli red od $E_n(\mathbb{F}_p)$ za takav p. Nema broja većeg od 4 koji bi dijelio sve takve brojeve $\#E_n(\mathbb{F}_p)$, jer znamo da $\#E_n(\mathbb{F}_p)$ ide brojevima oblika $p+1=4k$ za p prost broj oblika $4k-1$ (vidi Propoziciju 16).

Dokaz započinjemo konstrukcijom homomorfizma s grupe $\mathbb{Q}$-točaka na E_n u grupu $\mathbb{F}_p$-točaka. Općenitije, jednostavno konstruiramo preslikavanje s $\mathbb{P}^2_{\mathbb{Q}}$ na $\mathbb{P}^2_{\mathbb{F}_p}$. Ubuduće ćemo uvijek birati trojku (x,y,z) za točku u $\mathbb{P}^2_{\mathbb{Q}}$ na takav način da su x, y, z cijeli brojevi bez zajedničkog faktora. Samo je jedna takva trojka u svakoj klasi ekvivalencije, do na množenje s ± 1. Za svaki fiksni prosti p, definirajmo sliku $\overline{P}$ od $P=(x,y,z)\in\mathbb{P}^2_{\mathbb{Q}}$ kao točku $\overline{P}=(\overline{x},\overline{y},\overline{z})\in\mathbb{P}^2_{\mathbb{F}_p}$, gdje povlaka označava redukciju cijelog broja modulo p. Uočimo da $\overline{P}$ nije jednak trojci nula, jer p ne dijeli sva tri broja x, y, z. Također uočimo da smo trojku (x,y,z) mogli zamijeniti umnoškom s bilo kojim brojem relativno prostim s p bez da to utječe na $\overline{P}$ (što ćemo koristiti u dokazu sljedeće Leme).

Lako se vidi da ako se dogodi da je $P=(x,y,z)$ u $E_n(\mathbb{Q})$, tj. ako je $y^2z=x^3-n^2xz^2$, tada je $\overline{P}$ u $E_n(\mathbb{F}_p)$. Nadalje, slika od P_1+P_2 pod tim preslikavanjem je $\overline{P}_1+\overline{P}_2$, jer nema razlike da li prvo koristimo adicione formule (8.1)–(8.4) da nađemo zbroj i tada reduciramo modulo p, ili prvo reduciramo modulo p pa tada koristimo adicione formule. Drugim riječima, naše preslikavanje je homomorfizam s $E_n(\mathbb{Q})$ na $E_n(\mathbb{F}_p)$, za svaki prost p koji ne dijeli $2n$.

Odredimo sada kada to preslikavanje nije injektivno, tj. kada dvije točke $P_1=(x_1,y_1,z_1)$ i $P_2=(x_2,y_2,z_2)$ u $\mathbb{P}^2_{\mathbb{Q}}$ imaju istu sliku $\overline{P}_1=\overline{P}_2$ u $\mathbb{P}^2_{\mathbb{F}_p}$.

Lema. *$\overline{P}_1 = \overline{P}_2$ ako i samo ako je vektorski produkt od P_1 i P_2 (shvaćenih kao vektori u $\mathbb{R}^3$) djeljiv s p, tj. ako i samo ako p dijeli $y_1z_2 - y_2z_1$, $x_2z_1 - x_1z_2$ i $x_1y_2 - x_2y_1$.*

Dokaz leme. Prvo pretpostavimo da p dijeli vektorski produkt. Imamo dva slučaja:

(1) p dijeli x_1. Tada p dijeli x_2z_1 i x_2y_1, stoga dijeli i x_2, jer ne može dijeliti x_1, y_1 i z_1. Pretpostavimo da $p \nmid y_1$ (isti argument vrijedi ako $p \nmid z_1$). Uočimo da u tom slučaju $p \nmid y_2$ (jer bi u suprotnom p dijelio x_2, y_2 i z_2), pa u $\mathbb{F}_p$ postoji multiplikativni inverz od y_2. Vrijedi: $\overline{P}_2 = (0, \bar{y}_1\bar{y}_2, \bar{y}_1\bar{z}_2) = (0, \bar{y}_1\bar{y}_2, \bar{y}_2\bar{z}_1) = (0, \bar{y}_1, \bar{z}_1) = \overline{P}_1$ (koristili smo činjenicu da p dijeli $y_1z_2 - y_2z_1$).

(2) p ne dijeli x_1. Tada $\overline{P}_2 = (\bar{x}_1\bar{x}_2, \bar{x}_1\bar{y}_2, \bar{x}_1\bar{z}_2) = (\bar{x}_1\bar{x}_2, \bar{x}_2\bar{y}_1, \bar{x}_2\bar{z}_1) = (\bar{x}_1, \bar{y}_1, \bar{z}_1) = \overline{P}_1$.

Obratno, pretpostavimo da je $\overline{P}_1 = \overline{P}_2$. Bez smanjenja općenitosti možemo pretpostaviti da $p \nmid x_1$ (isti argument vrijedi ako $p \nmid y_1$ ili $p \nmid z_1$). Tada, jer je $\overline{P}_1 = \overline{P}_2 = (\bar{x}_2, \bar{y}_2, \bar{z}_2)$, pa i $p \nmid x_2$. Stoga je $(\bar{x}_1\bar{x}_2, \bar{x}_1\bar{y}_2, \bar{x}_1\bar{z}_2) = \overline{P}_2 = \overline{P}_1 = (\bar{x}_2\bar{x}_1, \bar{x}_2\bar{y}_1, \bar{x}_2\bar{z}_1)$. Budući su im prve koordinate jednake, te dvije točke su jednake samo ako su i druga i treća koordinata jednake, tj. ako p dijeli $x_1y_2 - x_2y_1$ i $x_1z_2 - x_2z_1$. Napokon, moramo dokazati da p dijeli $y_1z_2 - y_2z_1$. Ako su i y_1 i z_1 djeljivi s p, tada je to trivijalno. U suprotnom, zaključak slijedi ponavljanjem gornjeg argumenta s x_1, x_2 zamijenjenim s y_1, y_2 ili s z_1, z_2. ■

Sada smo spremni dokazati Propoziciju 17. Pretpostavimo da propozicija ne vrijedi, tj. da $E_n(\mathbb{Q})$ sadrži točku konačnog reda većeg od 2. Tada ili sadrži element neparnog reda, ili grupa točaka reda 4 sadrži ili 8 ili 16 elemenata. U oba slučaja imamo podgrupu $S = \{P_1, P_2, \ldots, P_m\} \subset E_n(\mathbb{Q})_{\text{tors}}$, gdje je $m = \#S$ ili 8 ili neparan broj.

Zapišimo sve točke $P_i, i = 1, \ldots, m$, u obliku leme: $P_i = (x_i, y_i, z_i)$. Za svaki par točaka P_i i P_j promotrimo vektorski produkt $(y_iz_j - y_jz_i,\ x_jz_i - x_iz_j,\ x_iy_j - x_jy_i) \in \mathbb{R}^3$. Budući da su P_i i P_j različite točke, kao vektori u $\mathbb{R}^3$ nisu proporcionalni, pa njihov vektorski produkt nije nul-vektor. Neka je n_{ij} najveći zajednički djelitelj koordinata u tom vektorskom produktu. Po lemi, točke P_i i P_j imaju istu sliku $\overline{P}_i = \overline{P}_j$ u $E_n(\mathbb{F}_p)$ ako i samo ako p dijeli n_{ij}. Tako, ako je p prost broj dobre redukcije (koji je veći od svih n_{ij}), slijedi da su sve slike različite. Zaključimo: preslikavanje redukcija modulo p je injekcija sa S u $E_n(\mathbb{F}_p)$, za sve proste brojeve p osim možda njih konačno mnogo (koji dijele n_{ij}).

To znači da broj m dijeli $\#E_n(\mathbb{F}_p)$ za sve proste brojeve p, osim njih konačno mnogo, jer je slika od S podgrupa reda m. Tada je za sve osim konačno mnogo prostih oblika $4k - 1$ (po Propoziciji 16) $p \equiv -1 \pmod{m}$. Ali to je kontradikcija

Dirichletovom teoremu za proste brojeve u aritmetičkom nizu[4]. Naime, ako je $m = 8$, to bi značilo da ima samo konačno mnogo prostih brojeva oblika $8k + 3$. Ako je m neparan, to bi značilo da postoji samo konačno mnogo prostih brojeva oblika $4mk + 3$ ako $3 \nmid m$ i da postoji samo konačno mnogo prostih brojeva oblika $4mk + 7$ ako $3 \mid m$. U svakom slučaju, Dirichletov teorem nam kazuje da postoji beskonačno mnogo prostih brojeva danog tipa, pa dobivamo kontradikciju. Dakle, $E_n(\mathbb{Q})_{\text{tors}}$ se sastoji od 4 točke reda 2. ■

Uočimo kako metoda redukcije modulo p (preciznije, korištenje Propozicije 16 za beskonačno mnogo prostih brojeva p) dovodi do lakšeg dokaza teške tvrdnje: ne postoje netrivijalne točke konačnog reda na E_n. Kako ćemo vidjeti, ta činjenica je vrlo korisna za rješavanje problema kongruentnih brojeva. Doduše, daleko interesantnije i teže pitanje je postojanje točaka beskonačnog reda, tj. da li je rang od $E_n(\mathbb{Q})$ različit od nule. Kako ćemo vidjeti, to je ekvivalentno pitanju da li je n kongruentan broj ili ne.

Dakle, normalno je pitati se može li $\bmod p$ podatak dati informaciju o rangu eliptičke krivulje. Ta razmatranja dovode do Birch–Swinnerton–Dyerove slutnje o oliptičkim krivuljama.

Propozicija 18. *n je kongruentan ako i samo ako $E_n(\mathbb{Q})$ ima rang veći od nule.*

Dokaz: Prvo pretpostavimo da je n kongruentan broj. Na početku trećeg poglavlja vidjeli smo da nam postojanje pravokutnog trokuta s racionalnim stranicama površine n daje racionalnu točku na $E_n(\mathbb{Q})$ čija x-koordinata leži u $\left(\mathbb{Q}^+\right)^2$. Budući da su x-koordinate tri netrivijalne točke reda 2 $0, \pm n$, to znači da postoji racionalna točka koja nije reda 2. Po Propoziciji 17, takva točka je beskonačnog reda, tj. $r \geq 1$.

Obratno, pretpostavimo da je $P = (x_P, y_P)$ točka beskonačnog reda. Po (8.5), x-koordinata točke $2P$ je $x_{2P} = \left(\frac{3x_P^2 - n^2}{2y_P}\right)^2 - 2x_P = \frac{x_P^4 + 2n^2x_P^2 + n^4}{4y_P^2} = \left(\frac{x_P^2 + n^2}{2y_P}\right)^2$, pa imamo:

$$x_{2P} + n = \left(\frac{x_P^2 + 2nx_P - n^2}{2y_P}\right)^2$$

$$x_{2P} - n = \left(\frac{x_P^2 - 2nx_P - n^2}{2y_P}\right)^2.$$

Sada po Propoziciji 1, točka $2P$ odgovara pravokutnom trokutu s racionalnim stranama površine n. ■

[4] Dirichletov teorem za proste brojeve u aritmetičkom nizu kaže da ako su a i b relativno prosti brojevi, tada u nizu $x_n = an + b$ postoji beskonačno mnogo prostih brojeva.

Uočimo važnost Propozicije 17 u dokazu Propozicije 18. Ona nam govori kako je jedini način da dobijemo netrivijalnu racionalnu točku oblika $2P$ od točke beskonačnog reda. Neka $2E_n(\mathbb{Q})$ označava podgrupu od $E_n(\mathbb{Q})$ koja se sastoji od dvostrukih racionalnih točaka. Tada je Propozicija 17 jednaka tvrdnji da je $2E_n(\mathbb{Q})$ abelova grupa bez torzionog dijela, tj. izomorfna je određenom broju (naime r) kopija od $\mathbb{Z}$. Skup $2E_n(\mathbb{Q}) - \mathcal{O}$ je prazan ako i samo je $r = 0$.

Vidimo da vezom iz Propozicije 1 točke u skupu $2E_n(\mathbb{Q}) - \mathcal{O}$ daju pravokutne trokute s racionalnim stranicama površine n. Prirodno je pitati se da li su sve točke koje zadovoljavaju uvjete Propozicije 2, tj. koje odgovaraju trokutima, dvostruke točke. Dokazat ćemo sada da jesu. U isto vrijeme, dat ćemo drugu provjeru Propozicije 18.

Propozicija 19. *Neka je E eliptička krivulja $y^2 = (x-e_1)(x-e_2)(x-e_3)$, gdje su $e_1, e_2, e_3 \in \mathbb{Q}$. Neka je $P = (x_0, y_0) \in E_n(\mathbb{Q}) - \mathcal{O}$. Tada je $P \in 2E_n(\mathbb{Q}) - \mathcal{O}$ ako i samo ako su svi $x_0 - e_1,\ x_0 - e_2,\ x_0 - e_3$ kvadrati racionalnih brojeva.*

Dokaz: Uočimo prvo da bez smanjenja općenitosti možemo pretpostaviti da je $x_0 = 0$. Da se to uoči, uvedimo supstituciju $x' = x - x_0$. Jednostavnom translacijom geometrijske slike za zbrajanje točaka, vidimo da je točka $P' = (0, y_0)$ na krivulji E' s jednadžbom $y^2 = (x - e_1')(x - e_2')(x - e_3')$ (gdje je $e_i' = e_i - x_0$) u $2E'(\mathbb{Q}) - \mathcal{O}$ ako i samo ako je naša originalna točka P bila u $2E(\mathbb{Q}) - \mathcal{O}$. Trivijalno, svi $x_0 - e_i$ su kvadrati ako i samo ako su to $(0 - e_i')$. Dakle, dovoljno je dokazati propoziciju za $x_0 = 0$.

Sljedeće, uočimo da ako postoji točka $Q \in E(\mathbb{Q})$ takva da je $2Q = P$, tada postoje točno četiri točke $Q, Q_1, Q_2, Q_3 \in E(\mathbb{Q})$ takve da je $2Q_i = P$. Da dobijemo Q_i, jednostavno dodamo točki Q točku reda dva $(e_i, 0) \in E(\mathbb{Q})$.

Izaberimo točku $Q = (x, y)$ takvu da je $2Q = P = (0, y_0)$. Želimo naći uvjet za koordinate jednog takvog racionalnog Q (a stoga i sva četiri). Sada točka Q na krivulji zadovoljava $2Q = P$ ako i samo ako tangenta na krivulju u točki Q prolazi kroz $-P = (0, -y_0)$. Tj. četiri moguće točke Q dobiju se geometrijski, crtanjem četiri različita pravca koja izlaze iz $-P$ i tangente su na krivulju.

Provjerimo da su koordinate (x, y) racionalne ako i samo ako je smjer pravca od $-P$ do Q racionalan. "Samo ako" se odmah vidi. Obratno, ako je taj smjer α racionalan, tada x-koordinata od Q, koja je dvostruka nultočka kubike $(\alpha x - y_0)^2 = (x - e_1)(x - e_2)(x - e_3)$ mora biti racionalna. (Eksplicitno, $x = \frac{e_1 + e_2 + e_3 + \alpha^2}{2}$.) U tom slučaju y-koordinata od Q također je racionalna: $y = \alpha x - y_0$. Iz toga se vidi da nam je dovoljno znati kada je racionalan jedan (pa stoga i sva četiri) smjer pravca od $-P$, koji je tangenta na E.

Broj $\alpha \in \mathbb{C}$ je smjer pravca od $-P$, koji je tangenta na E ako i samo ako sljedeća jednadžba ima dvostruku nultočku:

$$(\alpha x - y_0)^2 = (x - e_1)(x - e_2)(x - e_3) = x^3 + ax^2 + bx + c, \tag{10.1}$$

sa

$$a = -e_1 - e_2 - e_3, \qquad b = e_1e_2 + e_1e_3 + e_2e_3, \qquad c = -e_1e_2e_3 = y_0^2, \tag{10.2}$$

gdje posljednja jednakost $c = y_0^2$ slijedi iz činjenice da je $(0, y_0)$ na krivulji $y^2 = x^3 + ax^2 + bx + c$. Ako pojednostavimo (10.1) i izlučimo x, naš uvjet postaje da sljedeća kvadratna jednadžba ima dvostruku nultočku:

$$x^2 + (a - \alpha^2)x + (b + 2\alpha y_0) = 0.$$

To je ekvivalentno da njena diskriminanta iščezava, tj.

$$(a - \alpha^2)^2 - 4(b + 2\alpha y_0) = 0. \tag{10.3}$$

Tako da je naš zadatak odrediti kada je jedna (pa stoga i sve četiri) nultočka tog kvadratnog polinoma u α racionalna.

Želimo naći uvjet u terminima e_i-ova (naime, naša je tvrdnja da je ekvivalentan uvjet: $\sqrt{-e_i} \in \mathbb{Q}$). U (10.3), a i b su simetrični polinomi u e_i, ali y_0 nije; y_0 je simetrični polinom u $\sqrt{-e_i}$. Uvodimo f_i-ove koji zadovoljavaju $f_i^2 = -e_i$. Ako je $e_i \neq 0$, postoje dva moguća izbora za f_i. Izaberimo za f_i bilo koji, ali tako da dobijemo $y_0 = f_1f_2f_3$. Ako su svi e_i različiti od nule, to znači da je predznak od f_1 i f_2 proizvoljan, ali je predznak od f_3 izabran tako da su y_0 i $f_1f_2f_3$ isti korijeni od $-e_1e_2e_3$. Ako je, recimo, $e_3 = 0$, onda se može uzeti bilo koji predznak za f_1 i f_2, i naravno $f_3 = 0$. U svakom slučaju, imamo četiri moguća izbora za f_i, da dobijemo $y_0 = f_1f_2f_3$. Kada fiksiramo jedan takav izbor $f_1,\ f_2,\ f_3$, možemo poredati četiri izbora (pretpostavljamo da su e_1 i e_2 različiti od nule):

$$f_1, f_2, f_3; \qquad f_1, -f_2, -f_3; \qquad -f_1, f_2, -f_3; \qquad -f_1, -f_2, f_3. \tag{10.4}$$

Prednost prelaženja sa e_i-eva na f_i-eve je da su sada koeficijenti u našoj jednadžbi (10.3) simetrične funkcije od $f_1,\ f_2,\ f_3$. Preciznije, ako uzmemo da su $s_1 = f_1 + f_2 + f_3$, $s_2 = f_1f_2 + f_1f_3 + f_2f_3$, $s_3 = f_1f_2f_3$, elementarne simetrične funkcije, tada je

$$\begin{aligned} a &= f_1^2 + f_2^2 + f_3^2 = s_1^2 - 2s_2; \\ b &= f_1^2f_2^2 + f_1^2f_3^2 + f_2^2f_3^2 = s_2^2 - 2s_1s_3; \\ y_0 &= s_3. \end{aligned}$$

Tako da jednadžba (10.3) postaje

$$\begin{aligned} 0 &= (\alpha^2 - s_1^2 + 2s_2)^2 - 4(s_2^2 - 2s_1s_3 + 2\alpha s_3) \\ &= (\alpha^2 - s_1^2)^2 + 4s_2(\alpha^2 - s_1^2) - 8s_3(\alpha - s_1). \end{aligned} \tag{10.5}$$

Odmah se vidi da je polinom u (10.5) djeljiv sa $\alpha - s_1$, tj. Da mu je $\alpha = s_1 = f_1 + f_2 + f_3$ nultočka. Budući da smo mogli izabrati tri druga načina za

predznake od f_i, ostale nultočke moraju odgovarati tim izborima. Tj. četiri rješenja jednadžbe (10.3) su:

$$\begin{aligned} \alpha_1 &= f_1 + f_2 + f_3, & \alpha_2 &= f_1 - f_2 - f_3, \\ \alpha_3 &= -f_1 + f_2 - f_3, & \alpha_4 &= -f_1 - f_2 + f_3. \end{aligned} \tag{10.6}$$

Želimo znati kada su te četiri vrijednosti u (10.6) racionalne. Dakako, ako su svi f_i racionalni, tada su i α_i. Obratno, pretpostavimo da su α_i racionalni. Onda su racionalni i $f_1 = \frac{\alpha_1+\alpha_2}{2}$, $f_2 = \frac{\alpha_1+\alpha_3}{2}$ i $f_3 = \frac{\alpha_1+\alpha_4}{2}$. Zaključak je: Koordinate (x, y) točke Q za koju je $2Q = P$ racionalne su ako i samo ako su $f_i = \sqrt{-e_i}$ racionalni. ■

Napokon, uočimo da Propozicija 19 vrijedi i kada se $\mathbb{Q}$ zamijeni bilo kojim poljem karakteristike različite od 2. Dokaz je u suštini isti. (Jedino trebamo paziti da koristimo algebarske umjesto geometrijskih argumenata, na primjer kada smo svodili na slučaj $P = (0, y_0)$.)

Propozicija 20. *Postoji bijekcija između pravokutnih trokuta s racionalnim stranicama $a < b < c$ površine n i parova točaka $(x, \pm y) \in 2E_n(\mathbb{Q}) - \mathcal{O}$. Veza je:*

$$(x, \pm y) \mapsto a = \sqrt{x+n} - \sqrt{x-n}, \quad b = \sqrt{x+n} + \sqrt{x-n}, \quad c = 2\sqrt{x};$$
$$a, b, c \mapsto \left(\frac{c^2}{4}, \pm \frac{(b^2 - a^2)c}{8} \right).$$

Dokaz: To je direktna posljedica Propozicije 1 i karakterizacije dvostrukih točaka na eliptičkoj krivulji iz Propozicije 19. ■

11. Literatura

- A. Dujella: Eliptičke krivulje i njihova primjena u kriptografiji, http://www.math.hr/~duje/ecc/eccseminar.html
- N. Koblitz: Introduction to Elliptic Curves and Modular Forms, Second Edition, Springer, New York, 1993.
- K. Rubin: Elliptic curves and right triangles, http://math.stanford.edu/~rubin/lectures/sumo/
- P. Serf: Congruent Numbers, Computational Number Theory, de Gruyter, 1991, 227-238