Od kongruencijskih brojeva do eliptičkih krivulja

Cicvarić, Borna

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Borna Cicvarić

OD KONGRUENCIJSKIH BROJEVA DO ELIPTIČKIH KRIVULJA

Diplomski rad

Voditelj rada:
prof.dr.sc. Marcela Hanzer

Zagreb, Srpanj, 2015.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Sadržaj **iii**

Uvod **2**

1 Kongruentni brojevi **3**
1.1 Definicija i ekvivalentne karakterizacije 3
1.2 Jednadžba vezana uz kongruentne brojeve 6

2 Eliptičke krivulje **7**
2.1 Definicija i točka u beskonačnosti 7
2.2 Dvostruko periodične funkcije 9
2.3 Polje eliptičkih funkcija 14
2.4 Eliptičke krivulje u Weierstrassovoj formi 16
2.5 Pravilo zbrajanja 20
2.6 Točke konačnog reda 26
2.7 Točke nad konačnim poljima i kongruentni brojevi 30

Bibliografija **37**

Uvod

Teorija eliptičkih krivulja zahvaća različite grane matematike: kompleksnu analizu, teoriju brojeva, algebarsku geometriju i teoriju reprezentacija. Neke osnovne rezultate iz sva četiri područja ćemo koristiti u ovom radu.

Kao motivaciju za ovu temu navodimo problem koji je nastao već u antičkoj Grčkoj. Kako su se tada često bavili geometrijom, nametnulo se pitanje: Postoji li, za zadani $n \in \mathbb{N}$, pravokutni trokut s racionalnim stranicama površine n? Za n koji zadovoljava to svojstvo kažemo da je kongruentan.

Iako se problem spominje već u to doba, prvi put su ga sistematično razmatrali arapski naučnici u desetom stoljeću. Oni su problem preferirali formulirati ovako (u prvom poglavlju pokazati ćemo da su ovi problemi uistinu ekvivalentni): Postoji li, za dani $n \in \mathbb{N}$, racionalni broj x takav da su $x^2 - n$ i $x^2 + n$ kvadrati racionalnih brojeva? Ispostavlja se da odgovor na to pitanje nije tako jednostavan. Neki veliki matematičari su se bavili tim problemom. Tako je Euler dokazao da je 7 kongruentan, dok je Fermat dokazao da 1 nije (to je posljedica Velikog Fermatovog Teorema, što ćemo pokazati na kraju prvog poglavlja). Nakog nekog vremena postalo je jasno da 1, 2, 3 i 4 nisu kongruentni, dok 5, 6, 7 i 8 jesu, no izgledalo je beznadno da se nađe kriterij kojim će biti moguće direktno provjeriti je li dani n kongruentan. Veliki iskorak napravljen je u dvadesetom stoljeću kada je problem postavljen u kontekstu aritmetičkih svojstva eliptičkih krivulja.

U ovom radu navest ćemo definiciju i neka općenita svojstva takvih krivulja, među koje spada i krivulja $y^2 = x^3 - n^2 x$, koju ćemo povezati s problemom kongruentnih brojeva. Naime, pokazati ćemo da na toj krivulji postoji točka racionalnih koordinata i beskonačnog reda ako i samo ako je n kongruentan. Takve točke je lakše naći nego što se možda čini. Naime, ispostaviti će se da su to sve racionalne točke osim određene 4 koje su reda 2. Tako ćemo dobiti neke ekvivalentne uvjete s problemom kongruentnih brojeva, od kojih će glavni rezultat biti ovaj teorem:

Teorem. *Pravokutan trokut s racionalnim stranicama površine n postoji ako i samo ako na krivulji $y^2 = x^3 - n^2 x$ postoje tri točke A, B i C takve da je $A = B + C$ i A ima racionalne koordinate.*

Ovo svojstvo je puno pojednostavilo početni problem, budući da bi bez njega problem

mogli riješiti samo tako da pokušamo naći takav pravokutni trokut, a to je skoro pa nemoguće za neke veće brojeve (npr. hipotenuza "najjednostavnijeg" pravokutnog trokuta racionalnih stranica i površine 157, kada do kraja skratimo brojnik i nazivnik, ima 48 znamenka u brojniku i 46 u nazivniku). Primjetimo da točke na krivulji $y^2 = x^3 - n^2x$ ne možemo zbrajati po koordinatama, pa ćemo zbrajanje definirati pomoću periodičnih kompleksnih funkcija. "Naše" zbrajanje će se bazirati na tvrdnji sljedećeg teorema:

Teorem. *Pravac koji sječe krivulju $y^2 = x^3 + n^2x$ u više od jedne točke, nužno ju siječe u točno tri točke A, B i C. Tada vrijedi:*

$$A + B + C = 0.$$

Poglavlje 1

Kongruentni brojevi

1.1 Definicija i ekvivalentne karakterizacije

Prvo navodimo definiciju:

Definicija 1. *Kažemo da je pozitivan racionalan broj $q \in \mathbb{Q}$ kongruentan ako postoji pravokutni trokut kojemu su duljine sve tri stranice racionalni brojevi i površina mu je q.*

Drugim riječima, pitamo se postoje li $X, Y, Z \in \mathbb{Q}$ (bez smanjenja općenitosti pretpostavimo $X < Y < Z$) koji zadovoljavaju sustav:

$$\begin{cases} X^2 + Y^2 = Z^2 \\ \dfrac{XY}{2} = q. \end{cases} \tag{1.1}$$

Pretpostavimo sada da je q kongruentan, te da $X, Y, Z \in \mathbb{Q}$ zadovoljavaju sustav (1.1). Postoji jedinstveni $s \in \mathbb{Q}$ takav da je s^2q kvadratno slobodan broj (tj. nije djeljiv s k^2, $\forall k \in \mathbb{N} \setminus \{1\}$). Tada je s^2q površina pravokutnog trokuta sa stranicama $sX, sY, sZ \in \mathbb{Q}$, pa je i s^2q kongruentan. Dakle, umjesto kongruentnog broja q možemo promatrati njegovog kvadratno slobodnog reprezentanta s^2q u $\mathbb{Q}^+/(\mathbb{Q}^+)^2$, gdje je $(\mathbb{Q}^+)^2$ skup kvadrata racionalnih brojeva. Stoga odsad nadalje pretpostavljamo da je kongruentan broj $q = n$ kvadratno slobodnan. Pitamo se postoji li neki jednostavniji kriterij za odrediti je li dani kvadratno slobodan n kongruetan. Ako se vratimo na sustav (1.1), iz njega dobijemo:

$$(X \pm Y)^2 = Z^2 \pm 4n. \tag{1.2}$$

Ovaj izraz nam daje naslutiti da vrijedi sljedeća propozicija:

Propozicija 1. *Neka je n pozitivan kvadratno slobodan broj i neka su $X, Y, Z, x \in \mathbb{Q}$ uz uvjet $X < Y < Z$. Tada postoji bijekcija između pravokutnih trokuta sa stranicama X, Y, Z i brojeva x za koje su $x, x+n, x-n \in (\mathbb{Q}^+)^2$. Korespondencija je:*

$$\begin{aligned} X, Y, Z \to x &= \left(\frac{Z}{2}\right)^2 \\ x \to X &= \sqrt{x+n} - \sqrt{x-n}, Y = \sqrt{x+n} + \sqrt{x-n}, Z = 2\sqrt{x}. \end{aligned} \tag{1.3}$$

Dokaz. Prvo pretpostavimo da $X, Y, Z \in \mathbb{Q}$ zadovoljavaju (1.1). Iz (1.2) dijeljenjem obje strane s 4 zaključujemo da $x = \left(\frac{Z}{2}\right)^2$ zadovoljava $x, x+n, x-n \in (\mathbb{Q}^+)^2$. Obratno, pretpostavimo da x ima gore navedena svojstva, te da su X, Y, Z definirani s (1.3). Tada je $X < Y < Z$ (zbog $x > n$), te imamo:

$$\begin{aligned} X^2 + Y^2 &= (\sqrt{x+n} - \sqrt{x-n})^2 + (\sqrt{x+n} + \sqrt{x-n})^2 = \\ &= 2(x+n) + 2(x-n) = 4x = Z^2 \\ \frac{XY}{2} &= \frac{(\sqrt{x+n} - \sqrt{x-n})(\sqrt{x+n} + \sqrt{x-n})}{2} = \frac{x+n-(x-n)}{2} = n, \end{aligned} \tag{1.4}$$

pa vrijedi i obrat. Preostaje pokazati da je $X, Y, Z \to x$ injekcija. Pretpostavimo da su trokuti sa stranicama $X < Y < Z$ i $X_0 < Y_0 < Z_0$ oba površine n i $x = \left(\frac{Z}{2}\right)^2 = \left(\frac{Z_0}{2}\right)^2$. Iz (1.2) sada zaključujemo $X = X_0$, $Y = Y_0$. □

Ova Propozicija nam daje ekvivalentnu karakterizaciju kongruentnih brojeva. Za kraj još navodimo zadatak čiju ćemo tvrdnju koristiti kasnije.

Zadatak 1. *Pitagorina trojka je uređena trojka (X, Y, Z) pozitivnih cijelih brojeva za koje vrijedi $X^2 + Y^2 = Z^2$. Kažemo da je Pitagorina trojka primitivna ako je $NZD(X, Y, Z) = 1$. Neka su $a > b$ relativno prosti prirodni brojevi različite parnosti. Dokaži da $X = a^2 - b^2$, $Y = 2ab$ i $Z = a^2 + b^2$ čine primitivni Pitagorinu trojku, te da se svaka primitivna Pitagorina trojka može dobiti na ovaj način.*

Rješenje:

$X = a^2 - b^2$, $Y = 2ab$ i $Z = a^2 + b^2$ zadovoljavaju $X^2 + Y^2 = Z^2$. Također vrijedi $NZD(X, Z) = NZD(a^2 - b^2, a^2 + b^2) = NZD(-2b^2, a^2 + b^2) = NZD(2b^2, a^2 + b^2) = NZD(b^2, a^2 + b^2) = NZD(b^2, a^2) = 1$, gdje smo u drugoj i petoj jednakosti koristili $NZD(n, m) = NZD(n + m, m)$,u trećoj $NZD(n, m) = NZD(-n, m)$, u četvrtoj činjenicu da su a i b različite parnosti, te u šestoj da su a^2 i b^2 relativno prosti.

Obratno, pretpostavimo da je (X, Y, Z) primitivna Pitagorina trojka. Kako za cijeli broj n vrijedi $n \equiv 0, 1 \pmod 4$, mora vrijediti da je Z neparan, te X i Y različite parnosti (bez smanjenja općenitosti neka je Y paran i X neparan). Vrijedi $Y^2 = (Z - X)(Z + X)$,

uvedimo oznaku $Z - X = 2u$, $Z + X = 2v$. Iz $\frac{Y^2}{4} = uv$ i $NZD(u, v) = 1$ (jer je $NZD(Z - X, Z + X) = NZD(2X, Z + X) =$ {jer su oba parna, i X nije djeljiv s 2} $= 2NZD(X, Z + X) = 2NZD(X, Z) = 2$), zaključujemo da su u i v kvadrati cijelih brojeva, pa postoje relativno prosti cijeli brojevi $a > b$ takvi da je $2a^2 = 2v = Z + X$ i $2b^2 = 2u = Z - X$. Vrijedi $X = \frac{1}{2}(Z + X - (Z - X)) = a^2 - b^2$, $Y = 2ab$, $Z = \frac{1}{2}(Z + X + (Z - X)) = a^2 + b^2$.

Zadatak 2. *a) Dokaži: Ako je* 1 *kongruentan broj, tada jednadžba* $x^4 - y^4 = u^2$ *ima cijelobrojno rješenje i u je neparan.*

b)Dokaži da 1 *nije kongruentan broj.*

Rješenje:

a) Ako je 1 kongruentan broj, tada vrijedi:

$$X^2 + Y^2 = Z^2$$
$$XY = 2$$

Postoji $s \in \mathbb{Z}$ takav da su sX, sY, sZ pozitivni cijeli brojevi, te $NZD(sX, sY, sZ) = 1$. Uvedimo oznake $X' = sX$, $Y' = sY$, $Z' = sZ$ (primjetimo da X' i Y' moraju biti različite parnosti). Tada vrijedi:

$$(X' \pm Y')^2 = Z'^2 \pm 4s^2 \Rightarrow (X'^2 - Y'^2)^2 = Z'^4 - (2s)^4,$$

a kako je $X'^2 - Y'^2$ neparan jer su X' i Y' različite parnosti, tvrdnja a) je dokazana.

b)Dokazujemo da jednandžba $x^4 + u^2 = y^4$, gdje je u neparan, nema netrivijalnih cijelobrojnih rješenja. Pretpostavimo da rješenje postoji. Uzmimo rješenje takvo da je y najmanji mogući. Tada je (x^2, u, y^2) primitivna Pitagorina trojka (jer bi inače mogli podijeliti sve s $NZD(x^2, u)$ i dobiti manji y), pa postoje cijeli brojevi a i b iz Zadatka 1 takvi da je

$$x^2 = 2ab, \quad u = a^2 - b^2, \quad y^2 = a^2 + b^2.$$

Iz $x^2 = 2ab$ zaključujemo da je točno jedan od brojeva a i b paran (jer su relativno prosti). Preciznije, vrijedi da postoje relativno prosti cijeli brojevi c i d takvi da vrijedi $\{a, b\} = \{2c^2, d^2\}$, i d je neparan. Sada imamo $y^2 = (2c^2)^2 + d^4$, pa je i $(2c^2, d^2, y)$ primitivna Pitagorina trojka (zbog $NZD(2c^2, d^2) = 1$). Opet možemo naći a_1 i b_1 iz Zadatka 1. Vrijedi:

$2c^2 = 2a_1b_1 (\Rightarrow a_1 = e^2, b_1 = f^2$ jer su a_1 i b_1 relativno prosti), $\quad d^2 = a_1^2 - b_1^2, \quad y = a_1^2 + b_1^2$.

Konačno, sada imamo $f^4 + d^2 = e^4$, gdje je d neparan i $e \leq e^4 = a_1^2 < a_1^2 + b_1^2 = y$, što je kontradikcija s minimalnošću y.

1.2 Jednadžba vezana uz kongruentne brojeve

Vratimo se ponovo na (1.2). Ako te dvije jednadžbe međusobno pomnožimo dobijemo $\left(\frac{X^2-Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2$. Stoga jednadžba $u^4 - n^2 = v^2$ ima barem jedno racionalno rješenje. Kada je pomnožimo s u^2 dobijemo $u^6 - (nu)^2 = (vu)^2$. Uz supstituciju $x = u^2 = \left(\frac{Z}{2}\right)^2$, $y = uv = \frac{(X^2-Y^2)Z}{8}$ vidimo da x i y zadovoljavaju kubnu jednadžbu:

$$y^2 = x^3 - n^2 x \tag{1.5}$$

Dakle, za svaki pravokutni trokut sa stranicama $X, Y, Z \in \mathbb{Q}$ površine n dobijemo pripadnu točku (x, y) na krivulji (1.5). S druge strane, očito iz svake točke na krivulji (1.5) ne možemo dobiti pripadni pravokutni trokut (npr. mora vrijediti $x \in (\mathbb{Q}^+)^2$). Isto tako, nazivnik od x mora biti djeljiv s 2. Da to pokažemo, primjetimo da postoji primitivna Pitagorina trojka X_0, Y_0, Z_0 takva da je $\frac{X_0}{X} = \frac{Y_0}{Y} = \frac{Z_0}{Z} = s \in \mathbb{N}$. Kako u primitivnoj Pitagorinoj trojci cijeli broj koji odgovara hipotenuzi mora biti neparan zaključujemo da je Z_0 neparan, pa $x = \left(\frac{Z}{2}\right)^2 = \left(\frac{Z_0}{2s}\right)^2$ ima nazivnik djeljiv sa 2. Dobili smo 2 nužna uvjeta da za točku (x, y) na krivulji (1.5) postoji pripadni pravokutni trokut. Ispostavlja se da su oni ujedno i dovoljni.

Propozicija 2. *Neka je* (x, y) *točka na krivulji* (1.5). *Pretpostavimo da je* $x \in (\mathbb{Q}^+)^2$, *te da mu je nazivnik djeljiv s 2. Tada postoji pravokutni trokut s racionalnim stranicama i površinom n koji je u korespondenciji s x u smislu Propozicije* 1.

Dokaz. Stavimo $u = \sqrt{x} \in \mathbb{Q}^+$. Provodimo unatrag korake s početka poglavlja. Prvo, neka je $v = \frac{y}{u}$, tada imamo $v^2 = \frac{y^2}{x} = (1.5) = x^2 - n^2$. Označimo sa t nazivnik od u. Tada je nazivnik od v^2 i x^2 jednak t^4. Iz toga slijedi da je (t^2v, t^2n, t^2x) primitivna Pitagorina trojka, gdje je t^2n paran, jer je prema pretpostavci nazivnik od x, tj. t^2 paran. Prema Zadatku 1, postoje cijeli brojevi a i b takvi da je $t^2v = a^2 - b^2$, $t^2n = 2ab$, $t^2x = a^2 + b^2$. Promotrimo sada trokut sa stranicama $\frac{2a}{t}, \frac{2b}{t}, 2u$. Vrijedi $\left(\frac{2a}{t}\right)^2 + \left(\frac{2b}{t}\right)^2 = \frac{4(a^2+b^2)}{t^2} = \frac{4t^2x}{t^2} = 4x = (2u)^2$, pa je taj trokut pravokutan i površina mu je $\frac{2ab}{t^2} = n$. Tom trokutu je, u smislu Propozicije 1, korespondan $x = \left(\frac{2u}{2}\right)^2 = u^2$. □

Poglavlje 2

Eliptičke krivulje

2.1 Definicija i točka u beskonačnosti

Započnimo s definicijom eliptičke krivulje.

Definicija 2. *Neka je K proizvoljno polje i $f \in K[x]$ polinom trećeg stupnja s različitim nultočkama (nultočke mogu biti i u nekom proširenju od K). Pretpostavimo da K nema karakteristiku 2. Tada kažemo da je*

$$y^2 = f(x) \tag{2.1}$$

eliptička krivulja, a skup njezinih rješenja koja su iz proširenja K' od K zovemo K' - točke eliptičke krivulje definirane s (2.1).

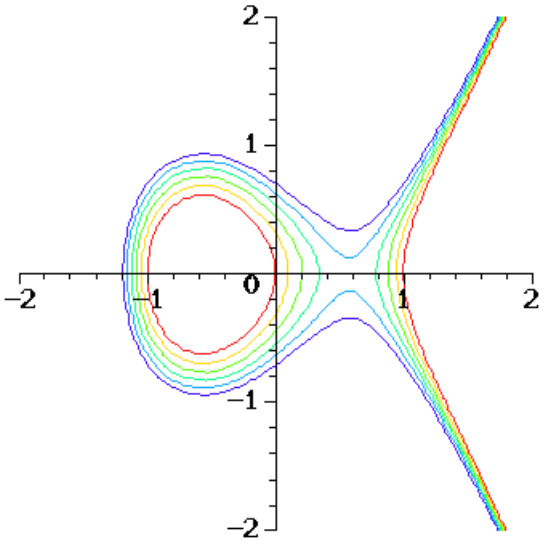
U primjeru iz prethodnog poglavlja, $K' = K = \mathbb{Q}$, $f(x) = x^3 - n^2x$. Napomenimo da $y^2 = x^3 - n^2x$ zadovoljava svojstva eliptičke krivulje u svakom polju karakteristike p ukoliko p ne dijeli $2n$, kako nultočke od $f(x)$ 0, $\pm n$ moraju biti različite.

Definicija 3. *Neka su $x_0, y_0 \in K'$ koordinate točke na krivulji C zadane jednadžbom $F(x, y) = 0$, kažemo da je C glatka u točki (x_0, y_0) ako parcijalne derivacije $\frac{\partial F}{\partial x}$ i $\frac{\partial F}{\partial y}$ nisu obje 0 u (x_0, y_0).*

Ovo je definicija neovisno o polju u kojem radimo. U slučaju $K' = \mathbb{R}$ ova definicija odgovara uvjetu da C ima tangentu. Za $F(x, y) = y^2 - f(x)$, u (x_0, y_0) dobijemo parcijalne derivacije $2y_0$ i $-f'(x_0)$. Kako K nije karakteristike 2, sustav

$$\begin{cases} 2y_0 = 0 \\ -f'(x_0) = 0 \end{cases}, \quad (x_0, y_0) \in K' \times K' \tag{2.2}$$

ima rješenje samo ako je $y_0 = 0$ i x_0 višestruka nultočka od $f(x)$. Kako zbog naše pretpostavke to nije moguće, vrijedi da je eliptička krivulja glatka u svim točkama. Uz točke



Slika 2.1: $y^2 = x^3 - x + b$, za $b = 0$(crvena), $0.1, 0.2, 0.3, 0.4, 0.5$(tamnoplava)

na krivulji (2.1), postoji važna "točka u beskonačnosti" koju bi željeli smatrati točkom krivulje. Da to definiramo, uvest ćemo projektivne koordinate.

Definicija 4. *Kažemo da monom $x^i y^j$ ima stupanj $i + j$. Stupanj polinoma $F(x, y)$ je maksimalni stupanj monoma koji se u njemu pojavljuju s koeficijentom različitim od* 0.

Definicija 5. *Neka je $F(x, y)$ polinom stupnja n. Definiramo pripadni homogeni polinom $\widetilde{F}(x, y, z)$ kao*

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

Primjetimo da $\widetilde{F}(x, y, z)$ dobijemo tako da svaki monom $x^i y^j$ u F pomnožimo sa z^{n-i-j}. Također vrijedi $F(x, y) = \widetilde{F}(x, y, 1)$. U našem primjeru, $F(x, y) = y^2 - x^3 + n^2 x$, pa dobijemo $\widetilde{F}(x, y, z) = zy^2 - x^3 + n^2 z^2 x$.

Neka je $\widetilde{F}$ homogeni polinom s koeficijentima iz polja K. Želimo rješiti jednadžbu $\widetilde{F}(x, y, z) = 0$, $x, y, z \in K$. Vrijedi:

- $\widetilde{F}(\lambda x, \lambda y, \lambda z) = \lambda^n \widetilde{F}(x, y, z)$, $\forall \lambda \in K$
- $\widetilde{F}(\lambda x, \lambda y, \lambda z) = 0 \Leftrightarrow \widetilde{F}(x, y, z) = 0$, $\forall \lambda \in K \setminus \{0\}$
- $\widetilde{F}(x, y, z) = 0 \Leftrightarrow F(\frac{x}{z}, \frac{y}{z}) = 0$, $\forall z \in K \setminus \{0\}$,

gdje su F i $\widetilde{F}$ u gore opisanom odnosu.

Dakle, dovoljno nam je gledati klase ekvivalencije trojki $(x, y, z) \in K^3$, gdje su (x, y, z) i (x', y', z') ekvivalentni ako postoji $\lambda \in K \setminus \{0\}$ tako da je $(x, y, z) = \lambda(x', y', z')$. Ako definiramo trivijalnu trojku kao $(0, 0, 0)$, neka je projektivna ravnina $\mathbb{P}^2_K$ skup svih klasa ekvivalencije netrivijalnih trojki. Pretpostavimo da je $K = \mathbb{R}$. $\mathbb{P}^2_{\mathbb{R}}$ geometrijski možemo zamisliti kao skup pravaca koji prolaze kroz ishodište u trodimenzionalnom prostoru. Drugi način kako možemo predočiti $\mathbb{P}^2_{\mathbb{R}}$ je tako da u $\mathbb{R}^3$ smjestimo ravninu $z = 1$. Svaki pravac kroz ishodište, osim onih u xy- ravnini, imaju jedinstven presjek s ravninom $z = 1$. Ako za te klase uzmemo reprezentante $(x, y, 1)$, možemo ih shvatiti kao običnu xy-ravninu. Ostale klase, u kojima je koordinata $z = 0$ čine "pravac u beskonačnosti". Pravac u beskonačnosti na sličan način zamišljamo kao pravac $y = 1$ u xy-ravnini, koji se sastoji d osvih klasa ekvivalencije s y koordinatom različitom od 0 i sadrži tocke $(x, 1, 0)$. Uz njih preostaje "točka u beskonačnosti" $(1, 0, 0)$. Neka je projektivni pravac $\mathbb{P}^1_K$ nad poljem K skup klasa ekvivalencije $(x, y) \sim (\lambda x, \lambda y)$. $\mathbb{P}^2_K$ možemo shvatiti kao ravninu $z = 1$ i $\mathbb{P}^1_K$, koji se sastoji od pravca $z = 0$, $y = 1$ i točke $(1, 0, 0)$. Rješenja sustava $\widetilde{F}(x, y, z) = 0$ tražimo među trojkama (x, y, z) u $\mathbb{P}^2_K$. Trojke s koordinatom $z \neq 0$ odgovaraju skupu točaka $\widetilde{F}(x, y, 1) = F(x, y) = 0$. Ostale točke su na pravcu u beskonačnosti. Skup rješenja $\widetilde{F}(x, y, z) = 0$ zovemo projektivni završetak krivulje $F(x, y) = 0$. Ubuduće svaki put kada spomenemo pravac, eliptičku krivulju i slično, mislimo na njihove projektivne završetke u $\mathbb{P}^2_K$ umjesto na obične krivulje u xy-ravnini. Vratimo se na naš standardni primjer, $\widetilde{F}(x, y, z) = zy^2 - x^3 + n^2z^2x$. Na pravcu u beskonačnosti promatramo klase ekvivalencije točaka $(x, y, 0)$ takve da je $0 = \widetilde{F}(x, y, 0) = -x^3$. Jedina takva klasa je $(0, 1, 0)$. Za $K = \mathbb{R}$ intuitivno možemo objasniti ovako: pravac $y = kx$, $k \in \mathbb{R}$ sječe $F(x, y)$ u točno jednoj točki. Za velike x, za točke na krivulji $\frac{y}{x} \to \infty$, a $\frac{y}{x} = \infty$ odgovara točki $(0, 1, 0)$. Tu točku sadrži svaka eliptička krivulja $y^2 = f(x)$. Svi koncepti analize na krivulji $F(x, y) = 0$ u xy-ravnini prenose se na pripadnu projektivnu krivulju $\widetilde{F}(x, y, z) = 0$. Obično takva svojstva u nekoj točki ovise o njenoj okolini. Svaka točka u $\mathbb{P}^2_K$ ima veliku okolinu koja izgleda kao obična ravnina. Preciznije, ako nas zanima točka u kojoj je $z \neq 0$ možemo ju promatrati u xy-ravnini gdje krivulja ima jednadžbu $F(x, y) = \widetilde{F}(x, y, 1) = 0$. Za $z = 0$, promatrat ćemo trojke oblika $(x, 1, 0)$ ili $(1, y, 0)$. U prvom slučaju zamišljamo ih kao točke oblika $\widetilde{F}(x, 1, z) = 0$ u xz-ravnini, a u drugom kao $\widetilde{F}(1, y, z) = 0$ u yz-ravnini.

2.2 Dvostruko periodične funkcije

Uzmimo $w_1, w_2 \in \mathbb{C}$ takve da je $w_1 \neq \lambda w_2$, $\forall \lambda \in \mathbb{R}$ (tj. $\{w_1, w_2\}$ je baza za $\mathbb{C}$ nad $\mathbb{R}$). Započinjemo s nekoliko definicija:

Definicija 6. *Kažemo da je $L \in \mathbb{C}$ rešetka u kompleksnoj ravnini ako postoji $\{w_1, w_2\}$ baza za $\mathbb{C}$ nad $\mathbb{R}$ takva da vrijedi $L = \{nw_1 + mw_2, n, m \in \mathbb{Z}\}$.*

Definicija 7. *Neka je* $\{w_1, w_2\}$ *baza za* $\mathbb{C}$ *nad* $\mathbb{R}$. *Fundamentalni paralelogram za* w_1 *i* w_2 *je* $\Pi = \{aw_1 + bw_2, a, b \in [0, 1]\}$.

Kako je $\{w_1, w_2\}$ baza za $\mathbb{C}$ nad $\mathbb{R}$, svaki $x \in \mathbb{C}$ možemo napisati kao $x = uw_1 + vw_2$, $u, v \in \mathbb{R}$. Slijedi da x možemo prikazati kao sumu elementa rešetke L i fundamentalnog paralelograma Π, te je taj prikaz jedinstven ukoliko $u, v \notin \mathbb{Z}$. Bez smanjenja općenitosti pretpostavljati ćemo da $\frac{w_1}{w_2}$ ima pozitivan imaginarni dio. Napomenimo još da izbor w_1, w_2 za danu rešetku L nije jedinstven (npr. umjesto w_1, w_2 mogli smo uzeti $w_1 + w_2, w_2$).

Definicija 8. *Kažemo da je funkcija* $f : D \to \bar{\mathbb{C}}$, $D \subset \mathbb{C}$ *meromorfna akko su zadovoljeni sljedeći uvjeti:*

- $S(f) = f^{-1}(\infty)$ *je diskretan skup u* D
- $f|_{(D\setminus S(f))} : D \setminus S(f) \to \mathbb{C}$ *je analitička*
- $S(f)$ *je skup polova od* f.

Definicija 9. *Neka je dana rešetka* L, *kažemo da je meromorfna funkcija* $f : \mathbb{C} \to \mathbb{C}$ *eliptička funkcija u odnosu na* L *ako vrijedi* $f(z) = f(z + l)$, $\forall z \in \mathbb{C}, \forall l \in L$.

Svojstvo u gornjoj definiciji dovoljno je provjeriti za $l = w_1$ i $l = w_2$. Dakle, eliptička funkcija je periodična s periodima w_1 i w_2. Takva funkcija je u potpunosti određena svojim vrijednostima na Π, s tim da joj se vrijednosti na nasuprotnim rubovima od Π podudaraju (tj. $f(bw_2) = f(w_1 + bw_2)$, $f(aw_1) = f(aw_1 + w_2)$, $a, b \in [0, 1]\}$).Stoga možemo f zadati na Π, s tim da nasuprotne stranice od Π "zalijepimo jednu na drugu" (takav skup nazivamo *torus*). Označimo sa $\mathcal{E}_L$ skup svih eliptičkih funkcija na rešetki L. Lako vidimo da je $\mathcal{E}_L$ potpolje polja svih meromorfnih funkcija jer je suma, razlika, umnožak i kvocijent dvije eliptičke funkcije opet eliptička. Dodatno, $\mathcal{E}_L$ je zatvoren na diferenciranje. Slijedi nekoliko propozicija o svojstavima eliptičkih funkcija. Ispostavlja se da je svojstvo dvostruke periodičosti meromorfnih funkcija puno jače nego isti uvjet u slučaju realne funkcije.

Propozicija 3. *Funkcija* $f(z) \in \mathcal{E}_L$, $L = \{nw_1 + mw_2\}$, *koja nema pola na fundamentalnom paralelogramu* Π *je konstanta.*

Dokaz. Pretpostavimo da f nema pola na Π. Kako je Π kompaktan, f mora biti ograničena na Π, pa postoji $M > 0$ takav da je $|f(z)| < M$, $\forall z \in \Pi$. No, tada je f ograničena s M na cijelom $\mathbb{C}$, pa je po Liouvilleovom teoremu konstanta. □

Propozicija 4. *Uz istu notaciju kao u prethodnoj propoziciji, označimo s* $\alpha + \Pi = \{\alpha + z, z \in \Pi\}$. *Pretpostavimo da* $f \in \mathcal{E}_L$ *nema pola na* $\partial(\alpha + \Pi)$. *Tada je suma reziduuma u unutrašnjosti skupa* $\alpha + \Pi$ *jednaka* 0.

Dokaz. Po teoremu o reziduumima, suma je jednaka

$$\frac{1}{2\pi i}\int_{\partial(\alpha+\Pi)} f(z)\,dz \tag{2.3}$$

Kako su vrijednosti od f na nasuprotnim rubovima jednake, a dz na nasuprotnim rubovima različitog predznaka, zaključujemo da je integral (2.3) jednak 0. □

Kako meromorfna funkcija može imati najviše konačno mnogo polova na kompaktnom skupu, moguće je izabrati α takav da na $\partial(\alpha + \Pi)$ nema polova od f. Primjetimo da Propozicija 4 povlači da nekonstantna funkcija f mora imati barem 2 različita pola (ili složen pol) u unutrašnjosti skupa $\alpha + \Pi$, jer bi u suprotnom suma u Propoziciji 4 bila različita od 0.

Propozicija 5. *Uz uvjete kao u Propoziciji 4, pretpostavimo da f nema polova na $\partial(\alpha+\Pi)$. Neka je $\{m_i\}$ skup redova različitih nultočaka u $\alpha+\Pi$, te $\{n_j\}$ skup različitih polova u $\alpha+\Pi$. Tada je $\sum m_i = \sum n_j$.*

Dokaz. Tvrdnja slijedi direktno iz korolara 41.2.(vidi [4], str. 81) i činjenice da je $\frac{1}{2\pi i}\int_{\partial(\alpha+\Pi)} f(z)\,dz = 0$. □

Sada definiramo funkciju za koju će se ispostaviti da je ključan primjer eliptičke funkcije za danu rešetu $L = \{nw_1 + mw_2\}$. Označavati ćemo ju s $\wp(z; L)$ ili samo $\wp(z)$ ukoliko je jasno o kojoj se rešetki radi.

Definicija 10. *Za danu rešetku L definiramo Weierstrrasovu $\wp$-funkciju $\wp : \mathbb{C} \to \mathbb{C}$ sa*

$$\wp(z) = \wp(z; L) = \frac{1}{z^2} + \sum_{l\in L\setminus\{0\}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2}\right) \tag{2.4}$$

Propozicija 6. *Suma u* (2.4) *konvergira apsolutno i uniformno na bilo kojem kompaktnom podskupu od $\mathbb{C} \setminus L$.*

Dokaz. Prvo napišemo sumande sa zajedničkim nazivnikom:

$$\sum_{l\in L\setminus\{0\}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2}\right) = \sum_{l\in L\setminus\{0\}} \frac{2z - z^2/l}{(z-l)^2 l} \tag{2.5}$$

Tvrdnja će biti dokazana korištenjem usporednog kriterija s $\sum_{l\in L\setminus\{0\}} \frac{1}{|l|^3}$. Preciznije, koristimo ove leme:

Lema 2.2.1. *Neka je dana rešetka L i konvergentan red pozitivnih brojeva $\sum_{l\in L\setminus\{0\}} b_l$. Pretpostavimo da niz $(f_l(z), l \in L)$ ima svojstvo da $|\frac{f_l(z)}{b_l}|$ ima konačan limes za $|l| \to \infty$, uniformno po z u nekom podskupu od $\mathbb{C}$. Tada $\sum_{l\in L\setminus\{0\}} f_l(z)$ konvergira apsolutno i uniformno po z u tom skupu.*

Dokaz. Tvrdnja je poopćenje Weierstrassovog M-testa (vidi [4], str. 48), slijedi iz činjenice da možemo pronaći $r, c > 0$ takve da je $|\frac{f_l(z)}{b_l}| \leq c$, za $|l| > r$, te primjenimo Weierstrassov M-test na redove $\sum_{|l|>r} cb_l$ i $\sum_{|l|>r} f_l(z)$. □

Lema 2.2.2. *Red*

$$\sum_{(m,n)\in\mathbb{Z}\setminus\{(0,0)\}} \frac{1}{(m^2+n^2)^\alpha}$$

konvergira akko je $\alpha > 1$.

Dokaz. Koristeći integralni kriterij dobijemo ekvivalentnu tvrdnju da $\int_{x^2+y^2\geq 1} \frac{dx\,dy}{(x^2+y^2)^\alpha}$ postoji akko je $\alpha > 1$. Prelaskom na polarne koordinate dobijemo da je integral jednak

$$I = \int_0^{2\pi}\int_1^\infty \frac{r\,dr\,d\phi}{r^{2\alpha}} = \int_1^\infty \frac{dr}{r^{2\alpha-1}}$$

Zadnji integral postoji akko je $2\alpha - 1 > 1 \Leftrightarrow \alpha > 1$. □

Lema 2.2.3. *Red* $\sum_{l\in L\setminus\{0\}} \frac{1}{|l|^s}$ *konvergira za* $s > 2$.

Dokaz. Iz Leme 2 slijedi da je dovoljno dokazati da postoji $\delta = \delta(w_1, w_2) > 0$ takav da je

$$|mw_1 + nw_2|^2 \geq \delta(m^2+n^2)$$

Ekvivalentno, možemo pokazati da $f(x,y) = \frac{|mw_1+nw_2|^2}{m^2+n^2}$ ima strogo pozitivan minimum na $\mathbb{R}^2 \setminus \{(0,0)\}$. Kako je $f(x,y)$ homogena, dovoljno je da ima strogo pozativan minimum na

$$S^1 = \{(x,y) \in \mathbb{R}^2, x^2+y^2 = 1\}$$

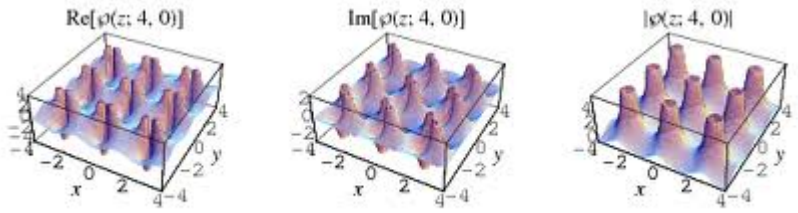
No, to je jasno pošto je S^1 kompaktan. □

□

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

Dokaz. Isto kao u prošloj propoziciji možemo pokazati da je za svaki fiksni $l \in L$ funkcija $\wp(z) - \frac{1}{(z-l)^2}$ neprekidna u točki $z = l$. Dakle, $\wp(z)$ je meromorfna funkcija s dvostrukim polovima u svim $l \in L$. Očito u drugim točkama nema polove. Primjetimo da je $\wp(z)$ parna funkcija zbog $\wp(z) = \frac{1}{z^2} + \sum_{l\in L\setminus\{0\}}(\frac{1}{(z-l)^2} - \frac{1}{l^2}) = \frac{1}{(-z)^2} + \sum_{-l\in L\setminus\{0\}}(\frac{1}{(-z+l)^2} - \frac{1}{(-l)^2}) = \frac{1}{(-z)^2} + \sum_{l\in L\setminus\{0\}}(\frac{1}{(-z-l)^2} - \frac{1}{(l)^2}) = \wp(-z)$.

Preostaje dokazati dvostruku periodičnost. Da bi to pokazali, promotrimo prvo $\wp'(z) = -2\sum_{l\in L} \frac{1}{(z-l)^3}$. Ona je dvostruko periodična jer zamjenom z sa $z + l_0$ za fiksni $l_0 \in L$ samo promjenimo poredak članova u sumi. Dakle, $\wp'(z) \in \mathcal{E}_L$. $\wp(z)$ je dvostruko periodična ako



Slika 2.2: Grafovi funkcije $\wp(z)$

vrijedi $\wp(z+w_i)-\wp(z)=0, i=1,2$. Uzmimo $i=1$. Derivacija funkcije $\wp(z+w_i)-\wp(z)$ je $\wp'(z+w_i)-\wp'(z)=0 \Rightarrow \wp(z+w_i)-\wp(z)=C$, gdje je C neka konstanta. Uvrštavanjem $z=-\frac{1}{2}w_1$ dobijemo $\wp(\frac{1}{2}w_i)-\wp(-\frac{1}{2}w_1)=C$, pa je $C=0$. Analogno dobijemo da je i w_2 period od $\wp(z)$ tj. $\wp(z)$ je dvostruko periodična. □

Primjetimo da dvostruka periodičnost od $\wp(z)$ nije očita iz definicije (2.4). Na domeni $\alpha+\Pi$, koja odgovara uvjetima Propozicije 5, $\wp(z)$ ima točno jedan dvostruki pol, pa po istoj propoziciji mora imati i dvije nultočke (brojeći kratnost). Isto vrijedi za funkciju oblika $\wp(z)-u$, za proizvoljnu konstantu u. Ova propozicija govori nešto više o tom svojstvu.

Propozicija 8. *Za svaki fiksni u eliptička funkcija $\wp(z)-u$ ima točno dvije nultočke na Π (brojeći kratnost). Također, za nultočke $\frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}$ od $\wp'(z)$ vrijedi da su $e_1=\wp\left(\frac{w_1}{2}\right), e_2=\wp\left(\frac{w_2}{2}\right), e_3=\wp\left(\frac{w_1+w_2}{2}\right)$ različite vrijednosti od u za koje $\wp(z)-u$ ima dvostruku nultočku.*

Dokaz. Da $\wp(z)-u$ ima barem dvije nultočke na Π je jasno iz komentara prije propozicije. Da ima više od dvije, mogli bi izabrati α takav da je zadovoljena Propozicija 5 i $\alpha+\Pi$ ima više od dvije nultočke, što nije moguće također zbog komentara prije propozicije. Kako je $\wp(z)$ parna, $\wp'(z)$ je neparna, imamo:

$$\wp'(\frac{w_1}{2})=-\wp'(-\frac{w_1}{2})=-\wp'(\frac{w_1}{2}) \tag{2.6}$$

gdje druga jednakost vrijedi jer $\wp'(z)$ ima period w_1. Slijedi da je $\frac{w_1}{2}$ nultočka od $\wp'(z)$, pa funkcija $\wp(z)-e_1$ ima dvostruku nultočku u $z=\frac{w_1}{2}$. Na isti način se dokaže za $\frac{w_2}{2}$ i $\frac{w_1+w_2}{2}$. Preostaje pokazati da su e_1, e_2 i e_3 međusobno različiti, to vrijedi zbog prvog dijela propozicije. □

Zadatak 3. *Dokaži da su rešetke $L=\{mw_1+nw_2\}$ i $L'=\{mw_1'+nw_2'\}$ jednake ako i samo ako postoji 2×2 matrica A s cjelobrojnim elementima i determinantom ± 1 takva da je $Aw=w'$ (gdje je w vektor stupac s elementima w_1, w_2). Ako su oba para w_1, w_2 i w_1', w_2' u smjeru kazaljke na sat, tada je* $\det A=1$.

Rješenje:
Pretpostavimo $L = L'$. Tada je $w_1', w_2' \in L$, tj. postoje cijeli brojevi a, b, c i d takvi da je

$$aw_1 + bw_2 = w_1'$$
$$cw_1 + dw_2 = w_2'$$

pa je traženi $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Analogno postoji matrica B s cijelobrojnim elementima takva da je $Bw' = w$. Vrijedi $AB = I$, slijedi $\det A \det B = 1$, a kako su $\det A$ i $\det B$ cijeli brojevi zaključujemo $\det A, \det B \in \{\pm 1\}$.

Pretpostavimo sada $\Im \frac{w_1}{w_2} > 0$. Tada je:

$$\frac{w_1'}{w_2'} = \frac{aw_1 + bw_2}{cw_1 + dw_2} = \frac{a\frac{w_1}{w_2} + b}{c\frac{w_1}{w_2} + d} = \frac{az + b}{cz + d},$$

gdje je $z = \frac{w_1}{w_2}$. Uvrstimo u gornju jednadžbu $z = x + iy, y > 0$. Slijedi:

$$\Im \frac{w_1'}{w_2'} = \Im \frac{ax + b + iay}{cx + d + icy} \cdot \frac{cx + d - icy}{cx + d - icy} = \frac{ay(cx + d) - cy(ax + b)}{(cx + d)^2 + (cy)^2} = \frac{y(ad - bc)}{(cx + d)^2 + (cy)^2} > 0 \Leftrightarrow$$

$$\Leftrightarrow ad - bc > 0,$$

zbog $y, (cx + d)^2 + (cy)^2 > 0$. Sada zbog prvog dijela zadatka zaključujemo $\det A = 1$.

2.3 Polje eliptičkih funkcija

U prošlom poglavlju imali smo prvi konkretan primjer eliptičke funkcije. Kao što $\sin x$ i $\cos x$ imaju važnu ulogu kod periodičnih funkcija u $\mathbb{R}$, tako $\wp(z)$ i $\wp'(z)$ imaju fundamentalnu ulogu u proučavanju eliptičkih funkcija. Za razliku od realnog slučaja, nije nam potreban red da izrazimo proizvolju eliptičku funkciju preko $\wp(z)$ i $\wp'(z)$.

Propozicija 9. *Za svaki $f(z) \in \mathcal{E}_L$ postoje racionalne funkcije $g(x)$ i $h(x)$ takve da vrijedi $f(z) = g(\wp(z)) + \wp'(z)h(\wp(z))$.*

Dokaz. $f(z) \in \mathcal{E}_L$ možemo napisati kao

$$f(z) = f_1(z) + \wp'(z)f_2(z) \tag{2.7}$$

gdje su $f_1(z) = \frac{f(z)+f(-z)}{2}$, $f_2(z) = \frac{f(z)-f(-z)}{2\wp'(z)}$ parne eliptičke funkcije. Dakle, dovoljno nam je dokazati:

Propozicija 10. *Za svaki $f(z) \in \mathcal{E}_L^+ \subset \mathcal{E}_L$ ($\mathcal{E}_L^+$ je potpolje svih parnih eliptičnih funkcija) postoji racionalna funkcija $g(x)$ takva da je $f(z) = g(\wp(z))$.*

Dokaz. Neka je $f(z) \in \mathcal{E}^+$. Probati ćemo konstruirati funkciju koja ima iste nultočke i polove kao $f(z)$ koristeći samo funkcije oblika $\wp(z) - u$, gdje je u neka konstanta. Omjer te funkcije i $f(z)$ će biti funkcija bez polova, dakle konstantna funkcija (prema Propoziciji 3). Ispostaviti će se da je dovoljno odabrati samo neke nultčke i polove.

Prvo ćemo objasniti kako biramo nultočke. Promatramo $f(z)$ na skupu $\Pi' = \{aw_1 + bw_2, a, b \in [0, 1\rangle\}$. Neka je $a \in \Pi'$ nultočka od $f(z)$, takva da $a \notin \{0, \frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}\}$. Odaberimo $a' \in \Pi'$ "simetričan" točki a, to jest, $a' = w_1 + w_2 - a$ ako je a u unutrašnjosti od Π', odnosno $a' = w_1 - a$ ili $a' = w_2 - a$ ukoliko je na nekoj od stranica Π'.

Tvrdnja 1. *a je nultočka reda $m \Rightarrow a'$ je nultočka reda m.*

Dokaz.

$$f(a' - z) = f(-a - z) = f(a + z)$$

gdje prva jednakosti vrijedi jer je f dvostruko periodična, a druga jer je parna. Dakle, ako je $f(a + z) = \sum_{i=m}^{\infty} a_i z^i \Rightarrow f(a' + z) = \sum_{i=m}^{\infty} a_i(-z)^i$, pa je i a' nultovcka reda m. □

Neka je za $f(z)$ $\{a_i^m\}$ multiskup nultočaka koje nisu u skupu $\{0, \frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}\}$, s tim da je u multiskupu po jedna nultočka iz svakog para a, a' onoliko puta koliki je njezin red.. Nećemo promatrati 0 ukoliko je ona nultočka, preostaju nam numtočke $a \in \{\frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}\}$.

Tvrdnja 2. *$a \in \{\frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}\}$ je nultočka reda $m \Rightarrow m$ je paran.*

Dokaz. Neka je $a = \frac{w_1}{2}$, tada je $f(\frac{w_1}{2} + z) = \sum_{i=m}^{\infty} a_i z^i$. Kao u Tvrdnji 1 dobijemo $f(\frac{w_1}{2} + z) = f(\frac{w_1}{2} - z) = \sum_{i=m}^{\infty} a_i(-z)^i$, pa zaključujemo da je m paran. □

Za takav a uzmemo još multiskup nultočaka $\{a_j^m\}$, s tim da svaku nultočku uzmemo m puta ako joj je red $2m$. Označimo sa $N = \{a_i^m\} \cup \{a_j^m\}$. Analogno napravimo multiskup polova P. Definiramo funkciju

$$g(z) = \frac{\prod_{a \in N}(\wp(z) - \wp(a))}{\prod_{p \in P}(\wp(z) - \wp(p))}$$

Pokazati ćemo da je $f(z) = c \cdot g(z)$. Pogledajmo prvo točke iz $\Pi' \setminus \{0\}$. Nultočke od $g(z)$ dolaze od nultočaka funkcija $\wp(z) - \wp(a)$, dok polovi dolaze od nultočaka funkcija $\wp(z) - \wp(p)$. No, iz Zadatka 2 znamo da $\wp(z) - u$ ima točno jednu dvostruku nultočku u $z = u$ ako je $u \in \{\frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}\}$, inače ima točno dvije jednosruke nultočke u u i njoj simetričnoj točki u'. Zbog konstrukcije funkcije $g(z)$ odmah vidimo da ima $g(z)$ i $f(z)$ imaju isti red nultočaka i polova na $\Pi' \setminus \{0\}$. Još moramo pokazati da imaju isti red nultočke ili pola u 0 (ukoliko 0 nije ni pol ni nultočka smo gotovi). To slijedi iz Propozicije 5. Naime, izaberemo α takav da $f(z)$ i $g(z)$ nemaju nultočke i polove na rubu, te da sadrži točno jednu točku $l \in L$. Označimo sa m_f red nultočke l od $f(z)$ (m_f je negativan ako je l pol). analogno definiramo m_g. Tada vrijedi:

m_f + (suma redova nultočaka od $f(z)$) - (suma redova polova od $f(z)$)= $=m_g$ + (suma redova nultočaka od $g(z)$) - (suma redova polova od $g(z)$) = =0

Kako su izrazi u pripadnim zagradama jednaki, zaključujemo $m_f = m_g$. Time je dokaz Propozicije 10, pa tako i Propozicije 9, završen. □

□

Iz ove Propozicije izravno slijedi npr. : (1) Parna funkcija $(\wp'(z))^2$ je kubni polinom od $\wp(z)$, jer $\wp'(z)$ ima trostruki pol u 0 i tri jednostruke nultočke, pa je $|N| = 3$, $|P| = 0$. (2) Parna funkcija $\wp(nz)$, za bilo koji fiksni $n \in \mathbb{N}$ je racionalna funkcija od $\wp(z)$. Ove dvije tvrdnje biti će važne za razmatranja koja slijede.

2.4 Eliptičke krivulje u Weierstrassovoj formi

Iznesimo precizinije prvu tvrdnju s kraja prošlog poglavlja. Iz Propozicije 8 znamo da $(\wp'(z))^2$ ima dvostruke nultočke u $\frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}$, dakle $N = \{\frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}\}$, iz čega slijedi:

$$\begin{aligned}(\wp'(z))^2 &= C(\wp(z) - \wp(\frac{w_1}{2}))(\wp(z) - \wp(\frac{w_2}{2}))(\wp(z) - \wp(\frac{w_1 + w_2}{2})) \\ &= C(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)\end{aligned} \tag{2.8}$$

C ćemo odrediti tako da promatramo Laurentov red obje strane oko 0. Prisjetimo se da je $\wp(z) - z^{-2}$ neprekidna u ishodištu, pa isto vrijedi i za $\wp'(z) + 2z^{-3}$. Stoga je vodeći koeficijent na lijevoj strani u (2.8) $(2z^{-3})^2$, a na desnoj $C(z^{-2})^3$. Izjednačavanjem ta dva izraza dobijemo $C = 4$. Dakle, $\wp(z)$ zadovoljava diferencijalnu jednadžbu

$$(\wp'(z))^2 = f(\wp(z)), \quad f(x) = C(x - e_1)(x - e_2)(x - e_3) \in \mathbb{C}[x]$$

Koristeći Propoziciju 3 dobiti ćemo još jednu diferencijalnu jednadžbu koju zadovoljava $\wp(z)$. Pretpostavimo da nađemo polinom $f(x) = ax^3 + bx^2 + cx + d$ takav da se Laurentov razvoj oko 0 funkcija $f(\wp(z))$ i $(\wp'(z))^2$ podudara u negativnim potencijama od z. Tada njihova razlika $(\wp'(z))^2 - f(\wp(z))$ nema pol u 0, a ni nigdje drugdje (pošto je 0 jedini pol funkcija $\wp(z)$ i $\wp'(z)$), dakle razlika im je konstanta (po Propoziciji 3). Ako pogodno odaberemo slobodni član od $f(x)$, dobijemo $(\wp'(z))^2 = f(\wp(z))$.

Da nađemo $f(x)$ moramo prvo razviti $\wp(z)$ i $(\wp'(z))^2$ u red oko 0. Neka je c po apsolutnoj vrijednosti najmanji element rešetke L različit od 0. Uzmimo $r < 1$ i $z \in K(0, rc)$. Za svaki $l \in L$ razvijemo u red izraz koji sadrži l u (2.4). Počnemo od geometrijskog niza

$$\frac{1}{1 - x} = 1 + x + x^2 + \dots$$

Diferenciranjem reda član po član i zamjenom x sa $\frac{z}{l}$ dobijemo

$$\frac{1}{\left(1-\frac{z}{l}\right)^2} = 1 + 2\frac{z}{l} + 3\left(\frac{z}{l}\right)^2 + \dots.$$

Oduzmimo 1 s obje strane i podijelimo jednadžbu s l^2, te to uvrstimo u (2.4):

$$\wp(z) = \frac{1}{z^2} + \sum_{l\in L\setminus\{0\}} \sum_{k=1}^{\infty} (k+1)\frac{z^k}{l^{k+2}} \tag{2.9}$$

Tvrdimo da ovaj dvostruki red konvergira za svaki $z \in K(0, rc)$. Da to dokažemo, napišimo sumu apsolutnih vrijednosti članova unutarnje sume kao (koristimo $|z| < rc < r|l|, \forall l \in L \setminus \{0\}$):

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

Sada tvrdnja slijedi iz Leme 2 u dokazu Propozicije 6. Zato u (2.9) možemo zamijeniti poredak sumacije i zapisati $\wp(z)$ na sljedeći način:

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

gdje za $k > 2$ uvodimo:

Definicija 11. *Za $k \in \mathbb{N}$ definiramo Eisensteinov red*

$$G_k = G_k(L) = G_k(w_1, w_2) = \sum_{l\in L\setminus\{0\}} l^{-k}$$

Primjetimo da je $G_k = 0$ za neparan k jer se tada član za l pokrati s članom za $-l$, što je očekivano jer se u razvoju od $\wp(z)$ pojavljuju samo parne potencije od z. Da bi našli polinom koji nam je potreban, izrazimo jos $\wp'(z)$, $\wp'(z)^2$, $\wp(z)^2$ i $\wp(z)^3$ u terminima $G_k, k > 2$.

$$\begin{aligned}
\wp'(z) &= -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \dots \\
\wp'(z)^2 &= \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + (36G_4 - 168G_8)z^2 + \dots \\
\wp(z)^2 &= \frac{1}{z^4} + 4G_4 + 10G_6 z^2 + \dots \\
\wp(z)^3 &= \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + (27G_4^2 + 21G_8)z^2 + \dots
\end{aligned}$$

Da bi našli koeficijente od $f(x)$ tako da je zadovoljena jednadžba

$$\wp'(z) = a\wp(z)^3 + b\wp(z)^2 + c\wp(z) + d$$

dovoljno je da se na lijevoj i desnoj strani podudaraju koeficijenti uz negativne potencije od z i konstantni član. Uvrstimo li samo te članove dobijemo:

$$\frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 = a\frac{1}{z^6} + b\frac{1}{z^4} + (9aG_4 + c)\frac{1}{z^2} + 15aG_6 + 4bG_4 + d$$

Lagano slijedi da je $a = 4$, $b = 0$, $c = -60G_4$, $d = -140G_6$. Običaj je koristiti oznake

$$g_2 = g_2(L) = 60G_4, g_3 = g_3(L) = 140G_6$$

Došli smo do još jedne diferencijalne jednadžbe koju $\wp(z)$ zadovoljava:

$$\wp'(z)^2 = f(\wp(z)), \quad f(x) = 4x^3 - g_2x - g_3 \in \mathbb{C}[x] \tag{2.10}$$

Uspoređujući koeficijente uz pozitivne potencije od z možemo doći do raznih identiteta koje G_k zadovoljavaju.

Jednadžba (2.10) ima jednostavnu geometrijsku interpretaciju. Pretpostavimo da uzmemo funkciju s fundamentalnog torusa $\mathbb{C}/L$ (tj. fundamentalnog paralelograma sa zaljepljenim nasuprotnim stranicama) u $\mathbb{P}^2_{\mathbb{C}}$ definiranu s

$$\begin{aligned} z &\mapsto (\wp(z), \wp'(z), 1), \quad z \neq 0 \\ z &\mapsto (0, 1, 0), \quad z = 0 \end{aligned} \tag{2.11}$$

Slika za svaki $z \neq 0$ iz $\mathbb{C}/L$ je točka u xy-ravnini (s kompleksnim koordinatama) čije x- i y- koordinate zadovoljavaju $y^2 = f(x)$ zbog (2.12). Kako je $f(x) \in \mathbb{C}[x]$ polinom trećeg stupnja s različitim nultočkama, svaka točka $z \in \mathbb{C}/L$ se preslikava u točku na eliptičkoj krivulji $y^2 = f(x)$ u $\mathbb{P}^2_{\mathbb{C}}$.

Za svaku vrijednost od x osim nultočaka od $f(x)$ (i ∞) postoje točno dvije vrijednosti od z takve da je $\wp(z) = x$ (slijedi iz Propozicije 8). Y-koordinate od $y = \wp'(z)$ koji dolaze od tih z su dva druga korijena od $f(x) = f(\wp(z))$. Ako je x nultočka od $f(x)$, tada postoji jedinstven z takav da je $\wp(z) = x$, dok je odgovarajuća y-koordinata $y = \wp'(z) = 0$, pa opet dobivamo rješenja jednadžbe $y^2 = f(x)$ za zadani x.

Također, preslikavanje iz $\mathbb{C}/L$ na eliptičku krivulju je analitičko, tj. u okolini svake točke u $\mathbb{C}/L$ možemo ga prikazati kao trojku analitičkih funkcija. U okolini točaka iz $\mathbb{C}$ koje nisu elementi rešetke preslikavanje je dano s $z \to (\wp(z), \wp'(z), 1)$; dok je u okolini elemenata rešetke preslikavanje dano s $z \to (\wp(z)/\wp'(z), 11/\wp'(z))$, što je analitička trojka u okolini od L. Dakle, vrijedi sljedeća propozicija:

Propozicija 11. *Preslikavanje definirano sa* (2.12) *je analitičko* $1-1$ *preslikavanje između* $\mathbb{C}/L$ *i eliptičke krivulje* $y^2 = 4x^3 - g_2x - g_3$ *u* $\mathbb{P}^2_{\mathbb{C}}$.

Pitamo se kako izgleda inverzno preslikavanje. Možemo ga konstruirati tako da uzimamo integrale od $dx/y = (4x^3 - g_2x - g_3)^{-\frac{1}{2}}\,dx$ od fiksnog početka do različitih krajeva. Taj integral će ovisiti o putu, ali će se mijenjati samo za "period", tj. element rešetke L. Tako dobijemo dobro definirano preslikavanje u $\mathbb{C}/L$.

Da zaključimo ovo poglavlje, par riječi o algebarskoj pozadini naše eliptičke krivulje. Iz Propozicije 8 znamo da se svaka eliptička funkcija može zapisati kao racionalna funkcija od $\wp(z)$ i $\wp'(z)$. Sada po bijekciji iz Propozicije 11 eliptičku funkciju preslikamo u racionalan izraz od x i y na eliptičkoj krivulji u $\mathbb{P}^2_{\mathbb{C}}$. Dakle, ako polje $\mathbb{C}(x, y)$ racionalnih funkcija u xy- ravnini restringiramo na krivulju $y^2 = f(x)$ i preslikamo ih nazad na $\mathbb{C}/L$ zamjenom $x = \wp(z)$, $y = \wp'(z)$, dobijemo upravo $\mathcal{E}_L$. Kako je restrikcija od y^2 ista kao restrikcija od $f(x)$, spomenutu restrikciju od $\mathbb{C}(x, y)$ dobijemo kao kvadratno proširenje od $\mathbb{C}(x) : \mathbb{C}(x)[y]/(y^2 - f(x))$.

U algebarskoj geometriji, polje $\mathbb{C}(x)$ odgovara kompleksnom pravcu $\mathbb{P}^1_{\mathbb{C}}$, dok $\mathbb{C}(x, y)/(y^2 - f(x))$ odgovara eliptičkoj krivulji u $\mathbb{P}^2_{\mathbb{C}}$. Prsteni $A = \mathbb{C}[x]$ i $B = \mathbb{C}[x, y]/(y^2 - f(x))$ su "prsteni cijelih" u ta dva polja. Maksimalni ideali u A su oblika $(x - a)A$, pa su u $1 - 1$ korespondenciji s $a \in \mathbb{C}$. Maksimalni ideali u B su oblika $(x - a)B + (y - b)B$ (gdje je $b = \sqrt{f(a)}$), to odgovara točki (a, b) na eliptičkoj krivulji.

Maksimalni ideal A, kad je "podignut" u prsten B, nije više prost, tj. ideal $(x - a)B$ je produkt dva ideala:

$$(x - a)B = ((x - a)B + (y - b)B)((x - a)B + (y + b)B).$$

Maksimalni ideal korespondan točki a na x-osi razdvaja se u dva maksimalna ideala korespondna s dvije točke na eliptičkoj krivulji. Ako je $b = 0$, tj. ako je a nultočka od $f(x)$, tada su oba ideala jednaka. U tom slučaju kažemo da se ideal $(x - a)A$ "grana" u B. Ovo se dogodi u točkama a koje su x-koordinate samo jedne točke $(a, 0)$ na eliptičkoj krivulji.

Zadatak 4. *Neka je $L = \mathbb{Z}[i]$ prsten Gaussovih cijelih brojeva. Dokaži da je tada $g_3 = 0$ i $g_2 \in \mathbb{R} \setminus \{0\}$.*

Rješenje:
Vrijedi $\mathbb{Z}[i] \setminus \{0\} = \{z, iz, -z, -iz;\ \ z \in S\}$, za $S = \{z;\ \ z = n + im, n, m \in \mathbb{N}\}$. Tada je

$$g_3 = \sum_{z\in S}(z^{-6} + (iz)^{-6} + (-z)^{-6} + (-iz)^{-6}) = \sum_{z\in S}(z^{-6} - z^{-6} + z^{-6} - z^{-6}) = \sum_{z\in S} 0 = 0$$

$$g_2 = \sum_{z\in S}(z^{-4} + (iz)^{-4} + (-z)^{-4} + (-iz)^{-4}) = 4\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\frac{1}{(m + in)^4}\cdot\frac{(m - in)^4}{(m - in)^4} =$$

$$= 4\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\left(\frac{m^4 - 6m^2n^2 + n^4}{(m^2 + n^2)^4} + i\frac{4n^3m - 4m^3n}{(m^2 + n^2)^4}\right).$$

Sada se imaginarni dio za par (m, n) pokrati s imaginarnim dijelom za par (n, m) ako su m i n različiti, dok je imaginarni dio 0 za $m = n$. Realni dio nije 0 zbog :

$$\frac{m^4 - 6m^2n^2 + n^4}{(m^2+n^2)^4} = 1 - \frac{8m^2n^2}{(m^2+n^2)^4} \geq 1 - \frac{8m^2n^2}{(2mn)^4} = 1 - \frac{1}{2m^2n^2} > 0,$$

gdje prva nejednakost vrijedi zbog $m^2 + n^2 \geq 2mn \Leftrightarrow (m-n)^2 \geq 0$.

2.5 Pravilo zbrajanja

Pokazali smo kako $\wp(z)$ daje $1-1$ korespondenciju između $\mathbb{C}/L$ i točaka na eliptičkoj krivulji $y^2 = f(x) = 4x^3 - g_2(L)x - g_3(L)$ u $\mathbb{P}^2_{\mathbb{C}}$. Jasno je kako zbrajamo elemente u $\mathbb{C}/L$, to je obično zbrajane "modulo L". Iskoristimo to i korespondenciju između $\mathbb{C}/L$ i eliptičke krivulje da uvedemo zbrajanje točaka na eliptičkoj krivulji. Za točke $P_1 = (x_1, y_1)$ i $P_2 = (x_2, y_2)$ nađemo $z_1, z_2 \in \mathbb{C}/L$ takve da je $P_1 = (\wp(z_1), \wp'(z_1))$ i $P_2 = (\wp(z_2), \wp'(z_2))$. Onda vrijedi $P_1 + P_2 = (\wp(z_1 + z_2), \wp'(z_1 + z_2))$.

Zanimljivo je da ovakvo zbrajanje ima jednostavnu geometrijsku interpretaciju i koordinate točke $P_1 + P_2$ možemo jednostavno izraziti preko x_1,x_2,y_1 i y_2. Time ćemo se baviti u ovom poglavlju. Za početak navodimo lemu:

Lema 2.5.1. *Neka je $f(x) \in \mathcal{E}_L$. Neka je Π fundamentalan paralelogram rešetke L i $\alpha \in \mathbb{C}$ takav da $f(z)$ nema nultočaka ni polova na rubu od $\alpha + \Pi$. Neka je $\{a_i\}$ multiskup nultočaka od $f(z)$ u unutrašnjosti skupa $\alpha + \Pi$ (svaka nultočka se ponavlja onoliko puta koliki joj je red), te $\{p_j\}$ multiskup polova od $f(z)$ u unutrašnjosti skupa $\alpha + \Pi$ (svaki pol se ponavlja onoliko puta koliki mu je red). Tada je $\sum a_i - \sum p_j \in L$.*

Dokaz. Prisjetimo se da funkcija $\frac{f'(z)}{f(z)}$ ima pol u a ako je a nultočka ili pol od $f(z)$, te je razvoj od $\frac{f'(z)}{f(z)}$ blizu a jednak $\frac{m}{z-a} + \ldots$ (m je red od a, $m < 0$ ako je a pol). Tada funkcija $\frac{zf'(z)}{f(z)}$ ima iste polove, ali ako uvrstimo $z = a + (z-a)$ vidimo da razvoj započinje s $\frac{am}{z-a}$. Zbog Propozicije 5, zaključujemo da je $\sum a_i - \sum p_j$ jednaka sumi reziduuma funkcije $\frac{zf'(z)}{f(z)}$ u unutrašnjosti skupa $\alpha + \Pi$. Koristeći teorem o reziduumima dobijemo

$$\begin{aligned}
\sum a_i - \sum p_j &= \frac{1}{2\pi i} \int_{\partial(\alpha+\Pi)} \frac{zf'(z)}{f(z)}\, dz = \\
&= \frac{1}{2\pi i} \left(\int_{\alpha}^{\alpha+w_2} \frac{zf'(z)}{f(z)}\, dz - \int_{\alpha+w_1}^{\alpha+w_1+w_2} \frac{zf'(z)}{f(z)}\, dz \right) = \\
&= \frac{1}{2\pi i} \left(\int_{\alpha}^{\alpha+w_2} \frac{zf'(z)}{f(z)}\, dz - \int_{\alpha}^{\alpha+w_2} \frac{(z+w_1)f'(z)}{f(z)}\, dz \right) = \\
&= -\frac{w_1}{2\pi i} \int_{\alpha}^{\alpha+w_2} \frac{f'(z)}{f(z)}\, dz
\end{aligned}$$

Uvedimo sada zamjenu varijabli $u = f(z)$. Tada je $\frac{f'(z)\,dz}{f(z)} = \frac{du}{u}$. Neka je C_1 zatvoren put od $f(\alpha)$ do $f(\alpha + w_2) = f(\alpha)$ gdje put ide po $u = f(z)$ kad z ide od α do $\alpha + w_2$. Tada vrijedi

$$\frac{1}{2\pi i}\int_{\alpha}^{\alpha+w_2} \frac{f'(z)}{f(z)}\,dz = \frac{1}{2\pi i}\int_{C_1} \frac{du}{u},$$

gdje postoji neki $n \in \mathbb{Z}$ koji je broj koliko se puta C_1 namota oko ishodišta u pozitivnom smjeru. Dakle, dio originalnog integrala koji računamo je $-w_1 n$. Na sličan način dobijemo da je drugi dio integrala $w_2 m$, za neki $m \in \mathbb{Z}$. Dakle, $\sum a_i - \sum p_j = -w_1 n + w_2 m \in L$, što je trebalo i dokazati. □

Sada smo spremni pokazati kako dvije točke na eliptičkoj krivulji možemo zbrojiti direktno, bez korištenja bijekcije iz Propozicije 11. Za $z \in \mathbb{C}_L$ uvedimo oznaku $P_z = (\wp(z), \wp'(z), 1)$ za $z \neq 0$, te $P_0 = (0, 1, 0)$. Prvo promatramo neke specijalne slučajeve. Očito je kako ćemo zbrajati P_{z_1} i P_{z_2} ukoliko je z_1 ili z_2 jednak 0, dakle, P_0 je neutralni element za zbrajanje, pa ćemo ga označavati s 0. Pretpostavimo sada P_{z_1} i P_{z_2} imaju istu x-koordinatu, ali različite y-koordinate. Tada mora vrijediti $y_1 = -y_2$. U ovom slučaju $z_2 = -z_1 \pmod{L}$, jer samo točke "simetrične" u odnosu na L daju istu $\wp$-vrijednost. Stoga je $P_{z_1} + P_{z_2} = P_0 = 0$, tj. te dvije točke su međusobno aditivni inverzi. Geometrijski, ukoliko vertikalni pravac siječe eliptičku krivulju u dvije točke, tada je njihova suma 0. Lako vidimo da ovo vrijedi i ukoliko je $y_1 = y_2 = 0$. Pokazali smo:

Propozicija 12. *Aditivni inverz točke* (x, y) *je* $(x, -y)$.

Uzmimo sad dvije točke na krivulji $P_1 = (x_1, y_1)$ i $P_2 = (x_2, y_2)$ (obje različite od 0) i označimo sa l pravac koji prolazi kroz te dvije točke. Ukoliko je l vertikalan, tada je $P_1 + P_2 = 0$. Pretpostavimo sada da l nije vertikalan. Tvrdimo da tada l sječe eliptičku krivulju u još točno jednoj točki $\widetilde{P}_3 = (\widetilde{x}_3, \widetilde{y}_3)$, te da je $P_1 + P_2 = P_3 = -\widetilde{P}_3 = (\widetilde{x}_3, -\widetilde{y}_3)$.

Napišimo l u obliku $y = mx + b$. Točka na tom pravcu je i na eliptičkoj krivulji ako i samo ako je $(mx + b)^2 = f(x) = 4x^3 - g_2 x - g_3$, odnosno ako i samo ako je x korijen od $f(x) - (mx + b)^2$. Taj polinom ima tri nultočke i svaka od njih nam daje točku presjeka. Ukoliko je x dvostruka ili trostruka nultočka, tada l presjeca krivulju s kratnošću dva ili tri (m je kratnost tangente u točki (x_0, y_0) ako je $f(x) - y_0 - f'(x - x_0) = \sum_{n=m}^{\infty} a_n (x - x_0)^n$, $a_m \neq 0$). U svakom slučaju, postoji ukupno tri točke presjeka (brojeći kratnost). Primjetimo da i vertikalni pravac sječe krivulju u tri točke, uključujući i točku u beskonačnosti 0. Također vrijedi :

Propozicija 13. *Pravac u beskonačnosti, čija je jednadžba* $z = 0$*, je tangenta na eliptičku krivulju* $y^2 = f(x)$ *u* $(0, 1, 0)$*, te je kratnost tangente tri.*

Dokaz. Imamo $\widetilde{F}(x, y, z) = 4x^3 - g_2 x z^2 - g_3 z^3 - y^2 z$, dakle $\nabla \widetilde{F}(x, y, z) = (12x^2 - g_2 z^2, -2yz, -g_2 x - 3g_3 z^2, -y^2)$, pa tangencijalna ravnina u $(0, 1, 0)$ ima jednadžbu

$$t \ldots \frac{\partial \widetilde{F}}{\partial x}(0,1,0)(x-0) + \frac{\partial \widetilde{F}}{\partial y}(0,1,0)(y-1) + \frac{\partial \widetilde{F}}{\partial z}(0,1,0)(z-0) = 0 \Leftrightarrow z = 0$$

Da je m točka infleksije (tj. da je kratnost od m je strogo veća od 2) dovoljno je da vrijedi $F''(x_0) = 0$, gdje je $(x_0, y_0, z_0) = (0,1,0)$. To vrijedi zbog $F''(x) = 24x$. Kratnost je točno 3 zbog $F'''(x_0) = 24 \neq 0$. □

Dakle, svaki pravac u $\mathbb{P}^2_{\mathbb{C}}$ sječe krivulju u tri točke. Ovo je specijalan slučaj Bezoutovog teorema, kojeg navodimo bez dokaza:

Bezoutov teorem. *Neka su $\widetilde{F}(x,y,z)$ i $\widetilde{G}(x,y,z)$ homogeni polinomi stupnjeva m i n redom, na algebarski zatvorenom polju K. Pretpostavimo da $\widetilde{F}$ i $\widetilde{G}$ nemaju zajedničkih faktora. Tada krivulje u $\mathbb{P}^2_{\mathbb{C}}$ definirane s $\widetilde{F}$ i $\widetilde{G}$ imaju mn točaka presjeka, brojeći kratnost.*

U našem slučaju $\widetilde{F}(x,y,z) = y^2z - 4x^3 + g_2xz^2 + g_3z^3$ i $\widetilde{G}(x,y,z) = y - mx - bz$. Sada smo spremni dokazati:

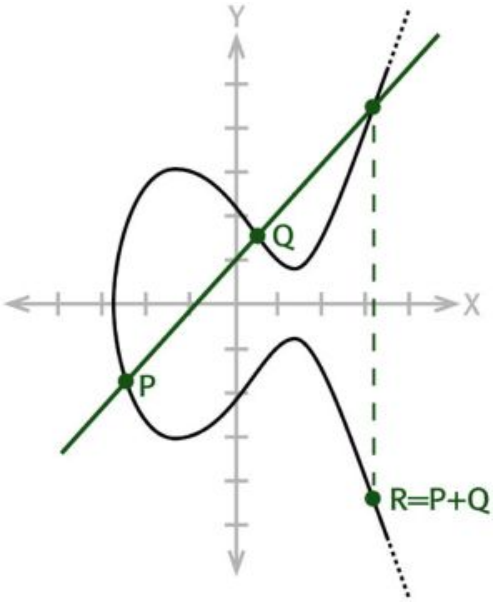
Propozicija 14. *Neka je $P_1 + P_2 = P_3$. Tada je $-P_3$ treća točka presjeka pravca l (koji prolazi kroz P_1 i P_2) i eliptičke krivulje. Ako je $P_1 = P_2$ tada je l tangenta u P_1.*

Dokaz. Već smo pokazali slučaje kada je P_1 ili P_2 jednak 0, te slučaj $P_1 = -P_2$. Neka je $P_1 = P_{z_1}$, $P_2 = P_{z_2}$. Pretpostavimo prvo da je l oblika $y = mx + b$. $P_z = (\wp'(z), \wp(z)) \in l$ akko vrijedi $\wp'(z) = m\wp(z) + b$. Eliptička funkcija $\wp'(z) - m\wp(z) - b$ ima tri pola, pa stoga i tri nultočke na $\mathbb{C}/L$. Dvije od njih su z_1 i z_2. Prema Lemi 4, zbroj polova i nultočaka je 0 modulo L. No, sva tri pola su u 0 ($\wp'(z)$ ima trostruki pol u 0), pa treća nultočka mora biti $-(z_1 + z_2)$ modulo L. Dakle, treća točka presjeka je $P_{-(z_1+z_2)} = -P_{z_3}$, što smo i željeli.
Ovaj argument vrijedi samo ako su sve tri točke različite. Općenito moramo pokazati da se dvostruka ili trostruka kratnost nultočke podudara s dvostukom ili trostrukom kratnošću presjeka. Neka su z_1, z_2 i z_3 nultočke od $\wp'(z) - m\wp(z) - b$, svaka nultočka se pojavljuje onoliko puta kolika joj je kratnost. Kako l nije vertikalan, nijedne dvije od ove tri točke nisu jedna drugoj inverz. Tada su $-z_1$, $-z_2$ i z_3 nultočke polinoma $\wp'(z) + m\wp(z) + b$, pa su $\pm z_1$, $\pm z_2$ i $\pm z_3$ nultočke od $\wp'(z)^2 - (m\wp(z) + b)^2 = f(\wp(z)) - (m\wp(z) + b)^2 = 4(\wp(z) - x_1)(\wp(z) - x_2)(\wp(z) - x_3)$, gdje su x_1, x_2 i x_3 nultočke od $f(x) - (mx + b)^2$. Bez smanjenja općenitosti neka je $\wp(z_1) = x_1$, tada kratnost od x_1 ovisi o tome koliko brojeva $\pm z_2$, $\pm z_3$ je jednako $\pm z_1$. To je isto kao i koliko je brojeva od z_2, $-z_3$ jednako z_1. Dakle, obje "kratnosti" su jednake. □

Jedan od nedostataka ovog pristupa je da ga a priori možemo primjeniti samo na eliptičke krivulje oblika $y^2 = 4x^3 - g_2(L)x - g_3(L)$ i krivulje koje možemo dobiti linearnom

zamjenom varijable (zbrajanje koje smo definirali i dalje daje Abelovu grupu ako napravimo ovakvu transformaciju). Kasnije ćemo dokazati da svaku eliptičku krivulju na $\mathbb{C}$ možemo transformirati u Weierstrassovu formu za neku rešetku L.

Pokušajmo sada koordinate $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ izraziti preko x_1, x_2, y_1, y_2, i koeficijenata jednadžbe eliptičke krivulje. Iako smo se mi bavili samo slučajem $y^2 = 4x^3 - g_2(L)x - g_3(L)$ ispostavlja se da zbrajanje iz Propozicije 14 daje Abelovu grupu za bilo koju eliptičku krivulju $y^2 = f(x)$. Zato ćemo pretpostaviti da je $f(x) = ax^3 + bx^2 + cx + d \in K[x]$ bilo koji kubni polinom s različitim nultočkama.



Slika 2.3: Zbrajanje točaka na eliptičkoj krivulji

U nastavku pretpostavljamo da su P_1 i P_2 različiti od 0, te da je $P_1 \neq P_2$. Tada pravac kroz P_1 i P_2 (ili tangenta kroz P_1 ako je $P_1 = P_2$) ima oblik $y = mx + b$, gdje je $m = \frac{y_2 - y_1}{x_2 - x_1}$ ako je $P_1 \neq P_2$, odnosno $m = \frac{dy}{dx}\Big|_{(x_1, y_1)}$ za $P_1 = P_2$. U drugom slučaju možemo dobiti m implicitnim deriviranjem $y^2 = f(x)$, dobijemo $m = \frac{f'(x_1)}{2y_1}$. U oba slučaja je odsječak na y-osi $\beta = y_1 - mx_1$.

Tada je x_3, x-koordinata sume, treći korijen polinoma $f(x) - (mx + \beta)^2$ (osim x_1 i x_2).

Iz Vieteovih formula imamo $x_1 + x_2 + x_3 = -\frac{b-m^2}{a}$, pa vrijedi:

$$\begin{aligned} x_3 &= -x_1 - x_2 - \frac{b}{a} + \frac{1}{a}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2, \quad P_1 \neq P_2 \\ x_3 &= -2x_1 - \frac{b}{a} + \frac{1}{a}\left(\frac{f'(x_1)}{2y_1}\right)^2, \quad P_1 = P_2 \end{aligned} \tag{2.12}$$

Za y koordinatu imamo:

$$y_3 = -y_1 + m(x_1 - x_3)$$

gdje je x_3 dan s (2.12), a m s

$$\begin{aligned} m &= \frac{y_2 - y_1}{x_2 - x_1}, \quad P_1 \neq P_2 \\ m &= \frac{f'(x_1)}{2y_1}, \quad P_1 = P_2 \end{aligned} \tag{2.13}$$

Bilo je moguće pomoću gore navedenih formula definirati zbrajanje na krivulji, te onda algebarskim putem pokazati da vrijede aksiomi komutativne grupe. Neki od dokaza bi bili problematični, na primjer provjeriti asocijativnost, no velika prednost ovog načina u odnosu na geometrijski i kompleksno-analitički dokaz je u tome da ne moramo pretpostavljati da je polje na kojem je definirana eliptička krivulja $\mathbb{C}$, čak nije bitno niti da ima karakteristiku 0. Drugim riječima, vidjeli bi da gore navedene formule daju Abelovu grupu za svako polje K čija je karakteristika različita od 2. Iako taj dokaz nećemo provoditi, ubuduće ćemo koristiti činjenicu da za danu eliptičku krivulju $y^2 = ax^3 + bx^2 + cx + d \in K[x]$, bilo koje dvije točke u nekom proširenju od K možemo zbrojiti pomoću formula (2.12) i (2.13).

Zadatak 5. *Neka je x točka infleksije na eliptičkoj krivulji $y^2 = x^3 - n^2x$. Nađi eksplicitnu formulu za x.*

Rješenje:

Vrijedi $y'' = 0$. Označimo s $f(x) = x^3 - n^2x$. Imamo redom:

$$\begin{aligned}
y^2 = f(x) = x^3 - n^2x \quad & \Big| \frac{d}{dx} \\
2y'y = f'(x) = 3x^2 - n^2 \quad & \Big| \frac{d}{dx} \\
2y''y + 2y'^2 = f''(x) = 6x \quad & \Big| 2y^2, y'' = 0 \\
(2y'y)^2 &= 12xy^2 \\
f'(x)^2 &= 12xf(x) \\
(3x^2 - n^2)^2 &= 12x(x^3 - n^2x) \\
9x^4 - 6x^2n^2 + n^4 &= 12x^4 - 12x^2n^2 \\
0 &= -3x^4 + 6x^2n^2 + n^4
\end{aligned}$$

Iz ove kvadratne jednadžbe dobijemo rješenje $x = \pm n\sqrt{1 \pm 2\frac{\sqrt{3}}{3}}$.

Zadatak 6. *Pojednostavi izraz za x-koordinatu točke $2P$ za eliptičku krivulju $y^2 = x^3 - n^2x$. Pokaži da ako P nije reda 2, onda je x-koordinata točke $2P$ kvadrat racionalnog broja s parnim nazivnikom.*

Rješenje: Iz formule (2.12) imamo:

$$\begin{aligned}
x_3 &= -2x_1 + \left(\frac{3x_1^2 - n^2}{2y_1}\right)^2 = \\
&= \frac{-8x_1(x_1^3 - n^2x_1) + 9x_1^4 - 6x_1^2n^2 + n^4}{4y_1^2} = \\
&= \frac{x_1^4 + 2x_1^2n^2 + n^4}{4y_1^2} = \\
&= \left(\frac{x_1^2 + n^2}{2y_1}\right)^2
\end{aligned}$$

Preostaje pokazati da je nazivnik paran. Uvedimo $ord_2a = k$, gdje je $a \in \mathbb{N}, a = 2^k l, l \in \mathbb{N}$ neparan, te za $a \in \mathbb{Q}, a = \frac{b}{c}$ vrijedi $ord_2a = ord_2b - ord_2c$.

Ako je y_1 neparan, tada iz $y_1^2 = (x_1^2 - n^2)x$ zaključujemo da je $x_1^2 + n^2$ neparan, pa je nazivnik od $2P$ paran.

Ako je y_1 paran, tada zbog $ord_2(x_1^2 + n^2) \leq 2$ (slijedi iz $ord_2n \leq 1$ jer je n kvadratno slobodan) imamo da tvrdnja trivijalno slijedi za $ord_2(x_1^2 + n^2) \leq 1$, pa preostaje pokazati tvrdnju za $ord_2(x_1^2 + n^2) = 2$. Tada nužno slijedi $ord_2x_1 \geq 1, ord_2n = 1$, no tada je $ord_2y^2 = ord_2(x_1^2 - n^2) + ord_2x \geq 3 \Rightarrow ord_2y \geq 2$, pa je opet nazivnik od $2P$ paran.

2.6 Točke konačnog reda

Sada kad smo definirali grupu, u njoj nas zanimaju točke konačnog reda. Pošto je grupa Abelova, svi elementi konačnog reda tvore podgrupu. U našem slučaju, vidimo da je P_z točka konačnog reda ako i samo ako je $Nz \in L$, za neki $N \in \mathbb{N}$, tj. ako je z racionalna linearna kombinacija od w_1 i w_2. Tada ćemo za najmanji takav N reći da je točan red od P_z. Općenito, svaki višekratnik od N je ujedno i red od P_z. Ukoliko promatramo izomorfizam iz $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ na eliptičku krivulju dan s $(a, b) \mapsto P_{aw_1+bw_2}$, tada je skup svih elemenata konačnog reda slika od $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$.

Uzmimo sada fiksni N. Neka je K polje karakteristike $\neq 2$ i $f(x) = ax^3 + bx^2 + cx + d = a(x - e_1)(x - e_2)(x - e_3) \in K[x]$, polinom s različitim nultočkama (moguće i iz nekog proširenja od K). Želimo promatrati točke reda N na krivulji $y^2 = f(x)$, koje također mogu biti iz proširenja od K. Znamo da su točke reda 2 točka u beskonačnosti, te $(e_i, 0)$, $i = 1, 2, 3$. Pretpostavimo sada da je $N > 2$.

Definicija 12. *Neka je N neparan. Kažemo da je P netrivijalan element reda N ako je $P \neq 0$ i $NP = 0$. Ako je N paran, kažemo da je P netrivijalan element reda N ako je $2P \neq 0$ i $NP = 0$.*

Propozicija 15. *Neka je K' bilo koje proširenje od K (ne nužno algebarsko) i neka je $\sigma : K' \mapsto \sigma K'$ bilo koji izomorfizam kojemu su fiksne točke svi elementi od K. Ako je $P \in \mathbb{P}^2_K$ točka točnog reda N na eliptičkoj krivulji $y^2 = f(x)$ ($f(x) \in K[x]$), tada σP ima egzaktan red N (gdje je $P = (x, y, z) \in \mathbb{P}'^2_K$, $\sigma P = (\sigma x, \sigma y, \sigma z) \in \mathbb{P}^2_{\sigma K'}$).*

Dokaz. Iz adicijske formule $\sigma P_1 + \sigma P_2 = \sigma(P_1 + P_2)$ slijedi $N(\sigma P) = \sigma(NP) = \sigma(0) = 0$, dakle N je red od σP. Da je egzaktan vidimo jer iz $N'(\sigma P) = 0$ zbog iste formule dobijemo $\sigma(N'P) = 0$, pa je $N'P = 0 \Rightarrow N' \geq N$. □

Propozicija 16. *Uz uvjete iz Propozicije 15, neka je $K \subset \mathbb{C}$. Označimo s $K_N \subset \mathbb{C}$ polje dobiveno dodavanjem x- i y-koordinata svih točaka reda N u skup K, a s K_{N^+} skup dobiven dodavanjem samo x-koordinata. Tada su i K_N i K_{N^+} Galoisova proširenja od K.*

Dokaz. Grupa točaka reda N u $\mathbb{P}^2_{\mathbb{C}}$ je konačna, štoviše, izomorfna s $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$. Tvrdnju dokazujemo samo za K_N, dokaz za K_{N^+} slijedi analogno. Da bi K_N bio Galoisovo proširenje od K dovoljno je da je separabilno i normalno. Očito je da je serparabilan jer je podskup od $\mathbb{C}$. Da dokažemo normalnost, uzmimo proizvoljnu σ koja zadovoljava Propoziciju 15 za $K' = K_N$. Po istoj propoziciji σ preslikava elemente reda N u elemente reda N (to jest, permutira ih), a na K je identiteta, pa je po definiciji normalno. □

Neka je $Gal(K_N/K) = \{\sigma | \sigma : K_N \mapsto K_N \text{ izomorfizam}, \sigma(K) = K\}$. Kako svaki $\sigma \in Gal(K_N/K)$ poštuje zbrajanje točaka, slijedi da σ daje invertibilno linearno preslikavanje iz $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ u $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$. Uzmimo sada proizvoljan komutativni prsten R.

Označimo sa $GL_n(R)$ skup svih invertibilnih matrica s elementima iz R. Znamo da za takvu matricu A vrijedi $\det A \in R^*$ (ovdje s R^* označavamo skup svih invertibilnih elemenata prstena R). Na primjer,

$$GL_2(\mathbb{Z}/N\mathbb{Z}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), a, b, c, d \in \mathbb{Z}/N\mathbb{Z}, ad - bc \in (\mathbb{Z}/N\mathbb{Z})^*\}$$

U našem slučaju vidjeli smo da je $Gal(K_N/K)$ izomorfan podgrupi grupe svih linearnih preslikavanja $(\mathbb{Z}/N\mathbb{Z})^2 \to (\mathbb{Z}/N\mathbb{Z})^2$. Stoga svaki $\sigma \in Gal(K_N/K)$ možemo poistovjetiti s matricom $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z}/N\mathbb{Z})$. Elemente matrice možemo naći iz jednadžbi

$$\sigma P_{w_1/N} = P_{aw_1/N+cw_2/N}, \qquad \sigma P_{w_2/N} = P_{bw_1/N+dw_2/N}.$$

Ovo je direktna generalizacija situacije s poljima $\mathbb{Q}_N = \mathbb{Q}(\sqrt[N]{1})$. Sjetimo se da je $Gal(\mathbb{Q}_N/\mathbb{Q}) \approx (\mathbb{Z}/N\mathbb{Z})^* = GL_1(\mathbb{Z}/N\mathbb{Z})$, gdje element a koji odgovara σ određujemo pomoću

$$\sigma(e^{2\pi i/N}) = e^{2a\pi i/N}.$$

No, za razliku od ovog, u dvodimenzionalnom slučaju je, generalno, $Gal(K_N/K) \to GL_2(\mathbb{Z}/N\mathbb{Z})$ samo injekcija, a ne izomorfizam.

U slučaju $K \subset \mathbb{C}$, npr. $K = \mathbb{Q}(g_2, g_3)$, gdje je $y^2 = f(x) = x^3 - g_2x - g_3$ krivulja u Weierstrassovoj formi, koristiti ćemo $\wp$-funkciju da odredimo polinom čije su nultočke x-koordinate od točaka reda N (tj. K_{N^+} će biti polje nultočaka takvog polinoma). Prvo želimo konstruirati funkciju $f_n(z)$ čije su nultočke svi $z \neq 0$ za koje je P_z reda N. Konstrukcija je slična onoj u Propoziciji 9. Ukoliko je $u \in \mathbb{C}/L$ točka reda N, onda je to i njoj simetrična točka $-u$ (ili u^*, kako smo ju označavali u Propozicji 9). Promatramo 2 slučaja:

(1) N je neparan. Onda su u i $-u$ uvijek različite modulo L (tj. $u \notin \{\frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}\}$). Definiramo

$$f_N(z) = N \prod_{\substack{u \in \mathbb{C}/L \\ Nu \in L}} (\wp(z) - \wp(u)), \tag{2.14}$$

s tim da uzmemo samo jedan element iz 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 pol u 0 reda $N^2 - 1$. Njezin vodeći koeficijent u razvoju oko $z = 0$ je $\frac{N}{z^{N^2-1}}$.

(2)N je paran. Prvo promatramo netrivijalne $u \in \mathbb{C}/L$ reda N. Definiramo $\widetilde{f_N}(z)$ kao produkt u (2.14). 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 pol u 0 reda $N^2 - 4$. Njezin vodeći koeficijent u razvoju oko $z = 0$ je $\frac{N}{z^{N^2-4}}$.

Za neparne N funkcija $f_N(z)$ ima svojstvo da je

$$f_N(z)^2 = N^2 \prod_{\substack{u\in\mathbb{C}/L\\ u\neq 0\\ Nu\in L}} (\wp(z)-\wp(u)).$$

Za parne N funkcija $f_N(z) = \frac{1}{2}\wp'(z)\widetilde{f_N}(z)$ također ima to svojstvo. Imamo:

$$\begin{aligned} f_N(z)^2 &= \frac{1}{4}\wp'(z)^2\widetilde{f_N}(z)^2 \\ &= N^2(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)\prod_{\substack{u\in\mathbb{C}/L\\ 2u\notin L\\ Nu\in L}}(\wp(z)-\wp(u)) \\ &= N^2\prod_{\substack{u\in\mathbb{C}/L\\ u\neq 0\\ Nu\in L}}(\wp(z)-\wp(u)). \end{aligned}$$

Vidimo da točka $(x,y) = (\wp(z),\wp'(z))$ ima neparan red N ako i samo ako je $F_N(x) = 0$, i ima paran red N ako i samo ako je $y = 0$(tj. točka je reda 2) ili je $F_N(x) = 0$. Iz Propozicija 15 i 16 znamo da svaki automorfizam od $\mathbb{C}$ kojemu su fiksni elementi $K = \mathbb{Q}(g_2,g_3)$ permutira nultočke od F_N. Dakle, koeficijenti od F_N su u $K = \mathbb{Q}(g_2,g_3)$.

Ako krenemo od proizvoljne eliptičke krivulje $f(x) = ax^3 + bx^2 + cx + d$, možemo pomoću formula (2.12) i (2.13) izračunati racionalnu funkciju od x i y, koja je x-koordinata od NP, gdje je $P = (x,y)$. Nakon što pojednostavimo izraz, dobili bi da je nazivnik 0 ako i samo ako je NP točka u beskonačnosti (tj. 0). Kako izgleda taj izraz? Pretpostavimo prvo da je N neparan. Tada je nazivnik izraz iz $K[x,y]$ (s tim da se y pojavljuje samo na prvu potenciju), a kako je $K = \mathbb{Q}(a,b,c,d)$, izraz nestaje akko je x jedna od $\frac{N^2-1}{2}$ vrijednosti x koordinate netrivijalnih točaka reda N. Dakle, izraz mora biti polinom samo u x s $\frac{N^2-1}{2}$ nultočaka. Slično, za parne N nazivnik je oblika $y*$ (polinom samo u x), gdje polinom iz $K[x]$ ima $\frac{N^2-4}{2}$ nultočaka. Ovaj postupak se može primjeniti za bilo koju eliptičku krivulju $y^2 = f(x)$ i bilo koje polje K čija karakteristika nije 2.

Moguće je da za općenito polje K ne moramo nužno dobiti točno N^2-1 netrivijalnih točaka reda N. Ukoliko K nije algebarski zatvoreno, te točke mogu biti u nekom proširenju od K, no postoji još jedan razlog. Ako je K karakteristike p, može se dogoditi da se vodeći koeficijent poništi modulo p, pa se stupanj polinoma smanji. Kasnije ćemo navesti primjere u kojima je manje od N^2 točaka reda N čak i kad je K algebarski zatvoreno. Ova diskusija vodi do sljedeće propozicije.

Propozicija 17. *Neka je $y^2 = f(x)$ eliptička krivulja nad poljem K, čija je karakteristika različita od 2. Tada postoji najviše N^2 točaka reda N u bilo kojem proširenju K' od K.*

Promotrimo sada slučaj kad je K konačno polje, kako bi iskoristili rezultat u Propoziciji 17. Uzmimo $K = \mathbb{F}_q$. Kako je $|\mathbb{P}^2_{\mathbb{F}_q}| = q^2 + q + 1$ (netrivijalnih trojki ima ukupno $q^3 - 1$, a klasa ekvivalencije za trojku (x, y, z) je $\{\lambda(x, y, z) | \lambda = 2, 3, \ldots, q\}$, tj. svaka klasa ima $q - 1$ elemenata, pa je $|\mathbb{P}^2_{\mathbb{F}_q}| = \frac{q^3-1}{q-1}$) , slijedi da ima konačno $\mathbb{F}_q$ točaka na eliptičkoj krivulji $y^2 = f(x)$ za $f(x) \in \mathbb{F}_q[x]$, pa je grupa $\mathbb{F}_q$-točaka konačna Abelova grupa. Želimo odrediti njezin tip, tj. zapis kao produkt cikličkih grupa reda koji je potencija prostog broja. Izlistat ćemo sve redove cikličkih grupa koje se pojavljuju redom: 2^{α_2}, 2^{β_2}, 2^{γ_2},..., 3^{α_3}, 3^{β_3}, 3^{γ_3},..., 5^{α_5}, 5^{β_5}, 5^{γ_5},... Iz Propozicije 17 slijedi da za svaki prosti l u proguktu mogu biti najviše dvije komponente potencija od l , jer bi inavce bilo više od l^2 točaka reda l.

Kao primjer, uzmimo $y^2 = x^3 - nx$ nad $K = \mathbb{F}_q$, gdje je $q = p^f$. Pretpostavimo da p ne dijeli $2n$. Za $q \equiv 3 \pmod 4$ lagano je izbrojati $\mathbb{F}_q$-točke.

Propozicija 18. *Neka je $q = p^f \equiv 3 \pmod 4$, $p \nmid 2n$. Tada ima $q + 1$ $\mathbb{F}_q$-točaka na eliptičkoj krivulji $y^2 = x^3 - n^2x$.*

Dokaz. Prvo, postoje 4 točke reda 2: točka u beskonačnosti, $(0, 0)$ i $(\pm n, 0)$. Sada izbrojimo parove gdje je $x \neq 0, \pm n$. Tih $q - 3$ točaka poredajmo u parove $\{x, -x\}$. Kako je $f(x) = x^3 - n^2x$ neparna funkcija i -1 nije kvadrat u $\mathbb{F}_q$ (slijedi iz $q \equiv 3 \pmod 4$), vrijedi da je točno jedan element iz $\{f(x), f(-x)\}$ kvadrat u $\mathbb{F}_q$. Ovisno koji od brojeva $\{f(x), f(-x)\}$ je kvadrat, dobijemo točno dvije točke $(x, \pm\sqrt{f(x)}$ ili $(-x, \pm\sqrt{f(-x)}$. Dakle, $\frac{q-3}{2}$ parova nam daju $q - 3$ točke. Uz 4 točke reda dva, imamo ih ukupno $q + 1$, što je trebalo i dokazati. □

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

Na primjer, za $q = 7^3$ ima $344 = 2^3 \cdot 43$ točaka. Pošto su 4 točke reda dva, zaključujemo da je tip grupe od $\mathbb{F}_{343}$-točaka na $y^2 = x^3 - n^2x$ oblika $(2, 2^2, 43)$.

Zanimljiviji je primjer $q = p = 107$. Tada je na krivulji $108 = 2^2 \cdot 3^3$ točaka. Grupa je tipa $(2, 2, 3^3)$ ili $(2, 2, 3, 3^2)$. Da to odredimo, moramo dokučiti ima li 3 ili 9 točaka reda 3 (kako 3 dijeli red grupe, moraju postojati netrivijalne točke reda 3). Iz Zadatka 2 znamo da su x-koordinate točaka reda 3 nultočke polinoma $-3x^4 + 6n^2x^2 + n^4 = 0$, tj. $x = \pm n\sqrt{1 \pm 2\sqrt{3}/3}$. Tada su y-koordinate $\pm\sqrt{f(x)}$. Bez direktnog računanja vidimo da ne mogu sve točke biti u $\mathbb{F}_{107}$ jer ako je $((x, y) \in \mathbb{F}_{107}) \Rightarrow \left((x, \sqrt{-1}y) \notin \mathbb{F}_{107}\right)$. Dakle, postoje 3 točke reda 3, pa je tip grupe $(2, 2, 3^3)$.

Primjetimo da kada bi K bilo polje karakteristike 3, tada grupa K-točaka na eliptičkoj krivulji ne bi imala netrivijalnih točaka reda 3 zbog $-3x^4 + 6n^2x^2 + n^4 = n^4 \neq 0$. Ovo je primjer poništavanja vodećeg koeficijenta spomenutog ranije u ovom poglavlju.

Zadatak 7. *Za eliptičku krivulju $y^2 = 4x^3 - g_2x - g_3$ izrazi $\wp(2z)$ kao racionalnu funkciju od $\wp(Z)$.*

Rješenje:

Uvedimo supstituciju $\wp(z) = x$, $\wp'(z) = y$ (ovi x i y su na eliptičkoj krivulji iz zadatka). Koristimo formule (2.12), gdje za ovaj f vrijedi $a = 4$, $b = 0$, $f'(x) = 12x - g_2$. Dalje računamo:

$$\wp(2z) = x_3 = (2.12) = -2x + \frac{1}{4} \cdot \left(\frac{12x^2 - g_2}{2y} \right)^2 = -2x + \frac{144x^4 - 24x^2 g_2 + g_2^2}{16y^2} =$$
$$= \frac{144x^4 - 24x^2 g_2 + g_2^2 - 128x^4 + 32x^2 g_2 + 32x g_3}{16y^2} = \frac{16x^4 + 8x^2 g_2 + 32x g_3 + g_2^2}{16(4x^3 - g_2 x - g_3)}.$$

2.7 Točke nad konačnim poljima i problem kongruentnih brojeva

Uglavnom nas zanimaju eliptičke krivulje E nad $\mathbb{Q}$, osobito eliptička krivulja $y^2 = x^3 - n^2 x$, koju ćemo označavati s E_n. Ukoliko je K bilo koje polje čija karakteristika p ne dijeli $2n$ ista jednadžba (gdje stavimo n modulo p) je eliptička krivulja nad K. S $E_n(K)$ označavati ćemo skup točaka krivulje s koordinatama u K. Npr., Propozicija 18 iz prošlog poglavlja kaže $|E_n(\mathbb{F}_q)| = q + 1$.

Definicija 13. *E_n definiranu nad $\mathbb{F}_p$ zovemo redukcija modulo p. Kažemo da je redukcija dobra ako p ne dijeli $2n$, tj. ako $y^2 = x^3 - n^2 x$ daje eliptičku krivulju nad $\mathbb{F}_p$.*

Ispostaviti će se da ovakva redukcija polja $\mathbb{Q}$ za različite p daje korisne informacije o $\mathbb{Q}$-točkama. Ovo je često komplicirana procedura, no postoji rezultat tog tipa koji je dovoljno jednostavan da ga odmah iznesemo. Koristiti ćemo redukciju modulo p da odredimo torzionu podgrupu grupe $E_n(\mathbb{Q})$, grupe $\mathbb{Q}$-točaka na eliptičkoj krivulji $y^2 = x^3 - n^2 x$.

U Abelovoj grupi, elementi konačnog reda tvore podgupu koju zovemo torzijska podgrupa. Na primjer, $E(\mathbb{C})$ grupa kompleksnih točaka na eliptičkoj krivulji je izomorfna s $\mathbb{C}/L$, koja je za bilo koju rešetku L izomorfna s $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ (izomorfizam je dan s $h : \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z} \to \mathbb{C}/L$, $h(x, y) = xw_1 + yw_2$). Torzijskoj podgrupi od $\mathbb{C}/L$ odgovara $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$, dakle u $\mathbb{C}/L$ se sastoji od svih racionalnih linearnih kombinacija od w_1 i w_2.

Osnovni Mordellov teorem kaže da je $E(\mathbb{Q})$ konačno generirana Abelova grupa. Iz toga slijede dvije tvrdnje

(1) torzijska podgrupa $E(\mathbb{Q})_{tors}$ je konačna

(2) $E(\mathbb{Q})$ je izomorfna direktnoj sumi torzione podgrupe $E(\mathbb{Q})_{tors}$ i konačno mnogo $\mathbb{Z}$-ova, tj. $E(\mathbb{Q}) \approx E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$. r iz ove formule zovemo rang grupe $E(\mathbb{Q})$. $r > 0$ ako i samo ako $E(\mathbb{Q})$ ima beskonačno mnogo $\mathbb{Q}$-točaka. Mordellova teorem vrijedi i ukoliko $\mathbb{Q}$

zamijenimo bilo kojim poljem algebarskih brojeva. Ova generalizacija zove se Mordell-Weilov teorem. Ovaj teorem nećemo dokazivati jer nam neće biti potreban niti samo u Mordellovom obliku. Sada dokazujemo tvrdnju da su jedine racionalne točke konačnog reda na E_n četiri točke reda 2 (točka u beskonačnosti, $(0,0)$, $(\pm n, 0)$.

Propozicija 19. $\#E_n(\mathbb{Q})_{tors} = 4$.

Dokaz. Ideja dokaza je da konstruiramo homomorfizam iz $E_n(\mathbb{Q})_{tors}$ u $E_n(\mathbb{F}_p)$ koji je injekcija za većinu p. To implicira da red od $E_n(\mathbb{Q})_{tors}$ dijeli red od $E_n(\mathbb{F}_p)$ za takve p. Ali kako nijedan broj veći od 4 ne može dijeliti sve takve brojeve $\#E_n(\mathbb{F}_p)$, barem znamo da $\#E_n(\mathbb{F}_p)$ ide po svim brojevim oblika $p+1$ gdje je p prost broj kongruentan 3 modulo 4 (slijedi iz Propozicije 18).

Počinjemo konstrukcijom homomorfizma iz $E_n(\mathbb{Q})$ u $E_n(\mathbb{F}_p)$, tj. preslikavanje iz $\mathbb{P}^2_{\mathbb{Q}}$ u $\mathbb{P}^2_{\mathbb{F}_p}$. U nastavku ćemo uvijek birati trojke (x,y,z) iz $\mathbb{P}^2_{\mathbb{Q}}$ na način da su x,y i z cijeli brojevikojima je najveći zajednički djelitelj jednak 1. Do na multiplikaciju s ± 1 postoji jedinstvena takva trojka u svakoj klasi ekvivalencije. Za fiksni prost broj p definiramo sliku točke $P = (x,y,z) \in \mathbb{P}^2_{\mathbb{Q}}$ sa $\bar{P} = (\bar{x}, \bar{y}, \bar{z}) \in \mathbb{P}^2_{\mathbb{F}_p}$, gdje $\bar{\cdot}$ označava redukciju modulo p. Kako $p \nmid NZD(x,y,z)$, $\bar{P} \neq (0,0,0)$. Također, primjetimo da smo (x,y,z) mogli pomnožiti s bilo kojim cijelim brojem koji nije djeljiv s p bez za promijenimo $\bar{P}$.

Lako se vidi da iz $P \in E_n(\mathbb{Q}) \Rightarrow \bar{P} \in E_n(\mathbb{F}_p)$ i da se $P_1 + P_2$ preslikava u $\bar{P}_1 + \bar{P}_2$, jer nije bitno ako prvo koristimo adicijske formule (2.12) i (2.13) da nađemo zbroj pa ga onda reduciramo modulo p ili obrnuto. Dakle, naše preslikavanje je homomorfizam iz $E_n(\mathbb{Q})$ u $E_n(\mathbb{F}_p)$ za svaki prosti p koji ne dijeli $2n$.

Promotrimo sada koje točke iz $\mathbb{P}^2_{\mathbb{Q}}$ imaju istu sliku u $\mathbb{P}^2_{\mathbb{F}_p}$.

Lema 2.7.1. *$\bar{P}_1 = \bar{P}_2$ ako i samo ako je vektorski produkt od P_1 i P_2 (ako ih shvatimo kao vektore u $\mathbb{R}^3$) djeliv s p, tj. ako i samo ako p dijeli brojeve $y_1z_2 - y_2z_1$, $x_2z_1 - x_1z_2$ i $x_1y_2 - x_2y_1$.*

Dokaz. Pretpostavimo prvo da p dijeli vektorski produkt. Imamo dva slučaja:

(1) p dijeli x_1. Tada p dijeli x_2z_1 i x_2y_1, pa kako ne može dijeliti i y i z mora dijeliti x_2. Pretpostavimo $y \nmid p$ (isto dobijemo i za slučaj $z \nmid p$). Tada $\bar{P}_2 = (0, \bar{y}_1\bar{y}_2, \bar{y}_1\bar{z}_2) = (0, \bar{y}_1\bar{y}_2, \bar{y}_2\bar{z}_1) = (0, \bar{y}_1, \bar{z}_1) = \bar{P}_1$

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

Obratno, pretpostavimo $\bar{P}_1 = \bar{P}_2$. Bez smanjenja općenitosti pretpostavimo da $p \nmid x_1$ (isti argument vrijedi i za $p \nmid y_1$ ili $p \nmid z_1$). Zbog $\bar{P}_1 = \bar{P}_2$ slijedi $p \nmid x_2$. Dakle, $(\bar{x}_1\bar{x}_2, \bar{x}_1\bar{y}_2, \bar{x}_1\bar{z}_2) = \bar{P}_2 = \bar{P}_1 = (\bar{x}_2\bar{x}_1, \bar{x}_2\bar{y}_1, \bar{x}_2\bar{z}_1)$. Pošto su prve koordinate jednake, slijedi da i druga i treća koordinata moraju biti jednake, tj. p dijeli $x_1y_2 - x_2y_1$ i$x_1z_2 - x_2z_1$. Preostaje pokazati da p dijeli $y_1z_2 - y_2z_1$. Ukoliko su y_1 i z_1 djeljiva s p, tvrdnja slijedi trivijalno. U suprotnom, tvrdnja slijedi ako u gornjem argumentu x_1, x_2 zamijenimo s y_1, y_2 ili z_1, z_2. Time je dokaz leme završen. □

Sada dokazujemo Propoziciju 19. Pretpostavimo suprotno, tj. da $E_n(\mathbb{Q})_tors$ sadrži element 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 $S = \{P_1, P_2, \ldots, P_m\}$ gdje je $m = |S|$ ili 8 ili neparan broj.

Stavimo $P_i = \{x_i, y_i, z_i\}$, $i = 1, 2, \ldots, m$. Za svaki par točaka P_i, P_j promatramo vektorski produkt $(y_iz_j - y_jz_i, x_jz_i - x_iz_j, x_iy_j - x_jy_i) \in \mathbb{R}^3$. Kako su P_i i P_j različiti, oni nisu proporcionalni kao vektori u $\mathbb{R}^3$ pa njihov vektorski produkt nije nul vektor. Neka je $n_{ij} = GCD\{y_iz_j - y_jz_i, x_jz_i - x_iz_j, x_iy_j - x_jy_i\}$. Po lemi 5, P_i i P_j imaju istu sliku $\bar{P}_i = \bar{P}_j$ u $E_n(\mathbb{F}_p)$ akko $p \mid n_{ij}$. Dakle, ako uzmemo p prost broj dobre redukcije koji je veći od $\max n_{ij}$, tada su sve slike međusobno različite, tj. preslikavanje modulo p je injekcija od S u $E_n(\mathbb{F}_p)$.

To pak znači da za sve osim konačno mnogo p-ova broj m mora dijeliti $|E_n(\mathbb{F}_p)|$, jer je slika od S podgrupa reda m. Zato za sve osim konačno mnogo prostih brojeva p kongruentnih 3 modulo 4 mora vrijediti $p \equiv -1 \pmod{m}$. To je u kontradikciji s Dirichletovim teoremom o prostim brojevima u aritmetičkim nizovima. To jest, ako je $m = 8$, to bi značilo da postoji samo konačno mnogo prostih brojeva oblika $8k + 3$. Ako je m neparan, to bi značilo da ima samo konačno mnogo prostih brojeva oblika $4m + 3$ (ako $3 \nmid m$), odnosno $12k + 7$ (ako $3 \mid m$). Dirichletov teorem daje nam kontradikciju u sva 3 slučaja. Time je dokaz završen. □

Ova Propozicija daje nam važan rezultat: Ne postoje postoje "netrivijalne" racionalne točke konačnog reda u E_n. Zanimljivije (i teže) pitanje je postoje li točke beskonačnog reda, tj. je li rang od $E_n(\mathbb{Q})$ strogo veći od 0. Pokazati ćemo da je ovo pitanje ekvivalentno problemu je li n kongruentan.

Propozicija 20. *n je kongruentan ako i samo ako $E_n(\mathbb{Q})$ ima rang strogo veći od* 0.

Dokaz. Pretpostavimo prvo da je n kongruentan. U početku drugog poglavlja, vidjeli smo da je to ekvivalentno s postojanjem racionalne točke u E_n čija je x-koordinata u $(\mathbb{Q}^+)^2$. Kako su x-koordinate od netrivijalnih točaka reda dva 0 i $\pm n$, mora postojati racionalna točka reda većeg od 2. Zbog Propozicije 19, takva točka ima beskonačan red, dakle $r \geq 1$.

Obratno, neka je P točka beskonačnog reda. Po Zadatku 6 x-koordinata točke $2P$ je kvadrat racionalnog broja s parnim nazivnikom. Sada iz Propozicije 2 točka $2P$ korespondira s pravokutnim trokutom racionalnih stranica i površine n (u smislu Propozicije 1). Time je dokaz završen. □

Primjetimo da nam u ovom dokazu Propozicija 19 kaže da netrivijalne racionalne točke oblika $2P$ možemo dobiti samo iz točaka beskonačnog reda. Neka je $2E_n(\mathbb{Q}) = \{2x : x \in E_n(\mathbb{Q})\}$. Tada je Propozicija 19 ekvivalentna tome da je $2E_n(\mathbb{Q})$ izomorfna s $\mathbb{Z}^r$. Skup $2E_n(\mathbb{Q}) - 0$ (0 označava točku u beskonačnosti) je prazan ako i samo ako je $r = 0$. Vidjeli smo da elementi skupa $2E_n(\mathbb{Q}) - 0$ vode do pravokutnih trokuta racionanih stranica

i površine n na način opisan u Propoziciji 1. Nameće se pitanje jesu li sve točke koje zadovoljavaju uvjete Propozicije 2 elementi skupa $2E_n(\mathbb{Q})$. O tome nam govori sljedeća propozicija:

Propozicija 21. *Postoji* $1-1$ *korespondencija između pravokutnih trokuta racionalnih stranica* $X < Y < Z$ *i površine* n*, i parova točaka* $(x, \pm y) \in 2E_n(\mathbb{Q}) - 0$*. Korespondencija je dana s:*

$$(x, \pm y) \mapsto \sqrt{x+n} - \sqrt{x-n},\ \sqrt{x+n} + \sqrt{x-n}, 2\sqrt{x}$$
$$X, Y, Z \mapsto \left(\frac{Z^2}{4}, \pm\frac{(Y^2 - X^2)Z}{8}\right).$$

Dokaz. Koristeći Propoziciju 1, ova tvrdnja je neposredna posljedica sljedeće karakterizacije elemenata skupa $2E_n(\mathbb{Q}) - 0$:

Propozicija 22. *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* $P = (x_0, y_0) \in E_n(\mathbb{Q}) - 0$*. Tada je* $P \in 2E_n(\mathbb{Q}) - 0$ *ako i samo ako su* $x - e_1, x - e_2, x - e_3 \in (\mathbb{Q}^+)^2$.

Dokaz. Napravimo zamjenu varijabli $x' = x - x_0$. Ako jednostavno translatiramo geometrijsku sliku za zbrajanje točaka, vidimo da je $P' = (0, y_0)$ na krivulji E' s jednadžbom $y^2 = (x - e_1')(x - e_2')(x - e_3')$, gdje je $e_i' = e_i - x_0$, ujedno i na $2E'(\mathbb{Q}) - 0$ ako i samo ako je originalni $P \in 2E_n(\mathbb{Q}) - 0$. I trivijalno, $x_0 - e_i$ su svi kvadrati ako i samo ako su $(0 - e_i')$ kvadrati. Dakle, dovoljno je dokazati tvrdnju za $x_0 = 0$.

Nadalje, primjetimo da ako postoji $Q \in E(\mathbb{Q})$ takav da je $2Q = P$, tada postoje još točno 3 točke $Q_i = Q + (e_i, 0)$, $i = 1, 2, 3$, takve da je $2Q_i = P$. Izaberimo Q tako da je $2Q = P = (0, y_0)$. Želimo odrediti uvjete za koje bi koordinate od Q bile racionalne. Vrijedi $2Q = P$ ako i samo ako tangenta na krivulju u Q prolazi kroz $-P = (0, -y_0)$. Te 4 točke možemo geometrijski dobiti crtanjem tangenta na krivulju koje prolaze kroz $-P$.

Pokažimo da su koordinate od Q racionalne ako i samo ako je pravac koji prolazi kroz $-P$ i Q ima racionalni koeficijent smjera. "Samo ako" smjer je očit. Obratno, ako je koeficijent smjera m racionalan, tada x-koordinata od Q, koja je dvostruka nultočka jednadžbe $(mx - y_0)^2 = (x - e_1)(x - e_2)(x - e_3)$, mora isto biti racionalna (eksplicitno, $x = \frac{e_1+e_2+e_3+m^2}{2}$). U tom slučaju je i y koordinata od Q racionalna. Dakle, želimo saznati kada su koeficijenti smjera od sve 4 tangente koje prolaze kroz $-P$ racionalni.

Broj $m \in \mathbb{C}$ je koeficijent smjera tangente koja prolazi kroz $-P$ ako i samo ako sljedeća jednadžba ima dvostruku nultočku:

$$(mx - y_0)^2 = (x - e_1)(x - e_2)(x - e_3) = x^3 + ax^2 + bx + c, \tag{2.15}$$

gdje je

$$a = -e_1 - e_2 - e_3, \quad b = e_1e_2 + e_2e_3 + e_3e_1, \quad c = -e_1e_2e_3 = y_0^2.$$

Zadnja jednakost vrijedi zbog činjenice da je točka $(0, y_0)$ na krivulji $y^2 = x^3 + ax^2 + bx + c$. Iz (2.15) dobijemo da sljedeća jednadžba mora imati dvostruku nultočku:

$$x^2 + (a - m^2)x + (b + 2my_0) = 0.$$

To će vrijediti ako je diskriminanta 0, tj.

$$(a - m^2)^2 - 4(b + 2my_0) = 0. \tag{2.16}$$

Želimo saznati kada je jedna (pa tako i sve četiri) nultočka ovog polinoma u m racionalna.

Taj uvjet tražimo u terminima e_i-eva (točnije da je ekvivalentna tvrdnja $-e_i \in \mathbb{Q}^2$). U (2.16) a i b su simetrični polinomi u e_i, dok je y_0 simetričan polinom u $\sqrt{e_i}$. Točnije, uvodimo f_i za koje vrijedi $f_i^2 = -e_i$, $i = 1, 2, 3$. Postoje dvije moguće vrijednosti za f_i ako je $e_i \neq 0$. Odaberimo f_i-ove na bilo koji način tako da je zadovoljeno $y_0 = f_1f_2f_3$. Ako je $e_i \neq 0$ za svaki i, tada predznak od f_1 i f_2 možemo izabrati proizvoljno, a predznak od f_3 će biti jednoznačno određen. Ako je npr. $f_3 = 0$, tada predznake od f_1 i f_2 možemo izabrati proizvoljno. U oba slučaja postoje četiri načina odabira f_1, f_2, f_3 na željeni način. Ako fiksiramo jedan takav odabir f_1, f_2, f_3 tada sva 4 slučaja možemo izlistati ovako (pretpostavimo da su e_1 i e_2 različiti od 0):

$$f_1, f_2, f_3; \quad -f_1, f_2, -f_3; \quad f_1, -f_2, -f_3; \quad -f_1, -f_2, f_3.$$

Sada su koeficijenti u (2.16) simetrične funkcije od f_1, f_2, f_3. Preciznije, ako stavimo $s_1 = f_1 + f_2 + f_3$, $s_2 = f_1f_2 + f_2f_3 + f_3f_1$, $s_3 = f_1f_2f_3$, tada vrijedi:

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

Dakle, jednadžba (2.16) postaje

$$(m^2 - s_1^2)^2 + 4s_2(m^2 - s_1^2) - 8s_3(m - s_1) = 0.$$

Odmah vidimo da je ovaj polinom djeljiv s $m - s_1$, tj. $m = s_1 = f_1 + f_2 + f_3$ mu je nultočka. Ostale tri nultočke dolaze od ostala tri izbora f_i-ova, pa su sva rješenja jednadžbe (2.16):

$$\begin{aligned} m_1 &= f_1 + f_2 + f_3; & m_2 &= f_1 - f_2 - f_3; \\ m_3 &= -f_1 + f_2 - f_3; & m_4 &= -f_1 - f_2 + f_3. \end{aligned} \tag{2.17}$$

Promotrimo kada su svi m_i u (2.17) racionalni. Jasno je da tvrdnja vrijedi ako su svi f_i racionalni. Obrnuto, pretpostavimo da su svi m_i racionalni. Tada vrijedi $f_i = \frac{m_1+m_{i+1}}{2}$. Zaključujemo da su koordinate (x, y) točke Q (za koju vrijedi $2Q = P$) racionalne ako i samo ako su $f_i = \sqrt{e_i}$ racionalne za $i = 1, 2, 3$. Time je dokaz Propozicije 22, pa tako i Propozicije 21, završen.

□

□

Za kraj, primjetimo da smo gornju propoziciju mogli dokazati i da $\mathbb{Q}$ zamijenimo bilo kojim poljem K karakteristike različite od 2. Dokaz je sličan, samo u nekim slučajevima trebamo upotrijebiti algebarske argumente umjesto geometrijskih (kao npr. kod ograničavanja na slučaj $P = (0, y_0)$).

Bibliografija

[1] E. Freitag, R. Busam, Complex Analysis, Second Edition, Springer Verlag, Berlin, 2009.

[2] G. Hardy, E. Wright, An Introduction to the Theory of Numbers, Fourth Edition, Oxford University press, Oxford, 1960.

[3] N. Koblitz, Introduction to Eliptic Curves and Modular Forms, Second Edition, Springer Verlag, New York, 1984.

[4] Š. Ungar, Kompleksna analiza, dostupno na http://web.math.pmf.unizg.hr/ ungar/NASTAVA/nastava.html (travanj 2015.)

Sažetak

Ukratko, ovaj rad započeli smo problemom kongruentnih brojeva, te smo problem povezali s eliptičkom krivuljom $y^2 = x^3 - n^2x$. Potom smo definirali eliptičke krivulje i eliptičke funkcije. Pokazali smo da se svaka eliptička funkcija može prikazati kao racionalna funkcija Weierstrassove $\wp$ funkcije, te da preko nje možemo napraviti bijekciju između $\mathbb{C}/L$ i točaka na eliptičkoj krivulji u $\mathbb{P}^2_{\mathbb{C}}$.

Preko te bijekcije definirali smo zbrajanje na eliptičkoj krivulji i objasnili njegovu geometrijsku interpretaciju. Sada kad možemo zbrajati točke na eliptičkoj krivulji (tj. taj skup točaka ima svojstvo grupe) promatramo točke konačnog reda, koji tvore podgrupu. Na kraju promotrimo eliptičke krivulje $y^2 = x^3 - n^2x$ (koje ćemo označavati E_n) nad $\mathbb{Q}$. Pomoću redukcije modulo p, gdje je $p \in \mathbb{N}$ prost, dokažemo da se torzijska podgrupa od $E_n(\mathbb{Q})$ sastoji od samo 4 elementa, te da svaki drugi element iz $E_n(\mathbb{Q})$ ima beskonačan red. Na kraju naše rezultate povežemo s problemom kongruentnih brojeva i dobijemo krajnji teorem:

Teorem. *$n \in \mathbb{N}$ je kongruentan broj ako i samo ako u $E_n(\mathbb{Q})$ postoji točka beskonačnog reda (tj. ako postoje $P, Q \in E_n(\mathbb{Q})$ i $P \neq 0$ takvi da je $P = 2Q$).*

Summary

To sumarize, we began with the congruent number problem and related it to the eliptic curve $y^2 = x^3 - n^2x$. Next, we defined eliptic curves and eliptic functions. We showed that every eliptic function can be written as a rational function of the Weierstrass $\wp$ function, and used it to construct a bijection between $\mathbb{C}/L$ and points of an eliptic curve in $\mathbb{P}^2_{\mathbb{C}}$.

Using that bijection, we defined addition of points of an eliptic curve and explained its geometrical interpretation. Now the points of an eliptic curve have the properties of a group, so we examined the points of finite order, which form a subgroup. In the end we focus on the curve $y^2 = x^3 - n^2x$, (which we will denote E_n) over $\mathbb{Q}$. Using reduction modulo p, where $p \in \mathbb{N}$ is a prime, we prove that the torsion subgroup of $E_n(\mathbb{Q})$ consists of only 4 elementa, and all the other elements of $E_n(\mathbb{Q})$ have infinite order. At the end we use our results and go back to the congruent number problem to prove the following theorem:

Teorem. *$n \in \mathbb{N}$ is a congruent number if and only if $E_n(\mathbb{Q})$ contains a point of infinite order (in other words, if there exist $P, Q \in E_n(\mathbb{Q})$, with $P \neq 0$ such that $P = 2Q$) .*

Životopis

Rođen sam u Rijeci 11.05.1991. godine. Tokom svog osnovnoškolskog i srednjoškolskog obrazovanja sudjelovao sam na mnogo natjecanja iz područja sporta (atletike i tenisa), informatike, logike i matematike. Najzapaženije rezultate imao sam iz matematike, gdje sam od 6 sudjelovanja na državnim natjecanjima osvojio dvije prve, dvije druge i dvije treće nagrade. Nastupao sam i u sklopu hrvatske ekipe na Srenjeeuropskoj matematičkoj olimpijadi 2008. i osvojio pohvalu, te na Međunarodnoj matematičkoj olimpijadi 2009. i 2010., gdje sam redom osvojio pohvalu i brončanu medalju.

Svoje obrazovanje sam nastavio na Prirodoslovno-matematičkom fakultetu u Zagrebu. Nakon tri godine na preddiplomskom studiju upisao sam diplomski smjer Matematička statistika. U tom periodu također sam u tri navrata sudjelovao na međunarodnim natjecanjima iz matematike kao dio ekipe fakulteta, dva puta na Međunarodnom matematičkom natjecanju Vojtech Jarnik u Češkoj i jednom na Međunarodnom matematičkom natjecanju u Bugarskoj, gdje sam osvojio srebrnu medalju. Uz to, bio sam demonstrator iz kolegija Elementarne matematike 1 i 2, te Vektorskih prostora, te svake godine držao predavanja iz dodatnog gradiva matematike nadarenim učenicima srednjih škola u Zagrebu i Rijeci.