Универзитет у Београду
Математички факултет

Мастер рад

Тангентно-тетивни закон сабирања на елиптичким кривама. Морделова теорама

Бранислав Милошевић

Ментор:
Проф. др Зоран Ракић
редовни професор
Математичког факултета
Универзитета у Београду

Београд, 2020. године

University of Belgrade
Faculty of Mathematics

Master thesis

Chord-Tangent Group Law on a Cubic Curves. Mordell's Finite Generation Theorem

Branislav Milošević

Advisor:
Prof. Zoran Rakić
full professor at
Belgrade University
Faculty of Mathematics

Београд, 2020. године

Подаци о мастер раду

Назив и седиште самосталне високошколске установе
Универзитет у Београду
Студентски трг 1, Београд
проф. др Иванка Поповић, ректор
редовни професор Технолошко-металуршког факултета Универзитета у Београду

Назив и седиште високошколске установе
Математички факултет
Студентски трг 16, Београд
проф. др Зоран Ракић, декан
редовни професор Математичког факултета Универзитета у Београду

Врста и степен студија
Мастер академске студије, II степен

Судијски програм и смер
Математика, Професор математике и рачунарства

Назив катедре
Катедра за методику наставе
др Небојша Икодиновић, шеф катедре
ванредни професор Математичког факултета Универзитета у Београду

Назив мастер рада
Тангентно-тетивни закон сабирања на елиптичким кривама.
Морделова теорама

Комисија
проф. др Зоран Ракић, ментор
редовни професор Математичког факултета Универзитета у Београду

проф. др Зоран Петровић, члан
редовни професор Математичког факултета Универзитета у Београду

др Ђорђе Баралић, члан
виши научни сарадник Математичког института САНУ

Студент
Бранислав Милошевић

„О елиптичким кривама је могуће бесконачно писати.
[Ово није претња.]"[1)]

Серж Ланг[2)]

[1)]Из увода књиге S. Lang, *Elliptic curves. Diophantine Analysis*, Springer-Verlag, Berlin, 1978.

[2)]Serge Lang (1927–2005), америчко-француски математичар

Захвалност и посвета

Неизмерно се захваљујем свом ментору проф. др Зорану Ракићу на предложеној теми, подршци, поверењу да ћу успети у писању о овој теми, као и стручној помоћи и саветима приликом израде самог рада. Мотивисао ме је да што више научим и несебично ми је, са пуно стрпљења, преносио знање како о овој теми, тако и са њеном техничком припремом.

Захвалност дугујем и члановима комисије, проф. др Зорану Петровићу и др Ђорђу Баралићу. Њихови стручни коментари, сугестије и примедбе значајно су допринели квалитету овог рада.

Захваљујем се и свима онима који су ме на разне начине подстицали да напишем овај рад. Ту посебно мислим на пријатеље и драге колеге Љубишу Младеновића и Илију Мировића. Њима дугујем и захвалност пре свега на искреној и пријатељској подршци, саветима и разговорима.

Имао сам срећу да ми у основној и средњој школи, као и на факултету, математику предају професори који су били заљубљеници у свој предмет, и који су ми пренели ту своју љубав према математици. Њима се такође захваљујем.

• • •

Овај рад посвећујем супрузи Ивани која је својим бескрајним стрпљењем, разумевањем и подршком помогла да истрајем у писању овог рада. Иако није математичар по струци, пажљиво је прочитала цео рад, и тако дала велики допринос да у њему има што мање штампарских и језичких грешака. Без ње не бих успео у писању овог рада.

Предговор

Циљ овог рада је да упознамо један од веома важних и значајних математичких објеката – елиптичку криву, затим да покажемо како се помоћу тангентно-тетивног закона уводи операција сабирања тачака на њој, и да на крају формулишемо и докажемо Морделову теорему.

Цео рад је подељен на девет нумерисаних поглавља. Свако поглавље је подељено на више нумерисаних параграфа, а сваки параграф се састоји од неколико тачака или секција.

У првом поглављу подсетићемо се пројективних простора, јер су нам нека знања из пројективне геометрије потребна да бисмо добили потпунију слику о елиптичким кривама.

Друго поглавље представља кратак увод у криве. Дефинисаћемо криву, навешћемо проблем који се може јавити приликом њеног дефинисања, и показаћемо на које начине можемо задати криве.

Треће поглавље је посвећено алгебарским кривама. У оквиру њега прецизираћемо неке појмове и садржаје који су нам неопходни за упознавање са елиптичким кривама. Дефинисаћемо алгебарску криву, показаћемо њене особине над пољем $\mathbb{C}$ комплексних бројева, затим ћемо извршити и класификацију алгебарских кривих према реду и роду. Управо род алгебарске криве ће нам омогућити да дамо геометријску дефиницију елиптичке криве, која је позната и као њена шира дефиниција. Ово, и претходна два поглавља, можемо схватити и као припрему за увођење елиптичких кривих.

У четвртом поглављу, са више детаља упознаћемо елиптичке криве. Помоћу Вајерштрасове кубне криве даћемо алгебарску дефиницију елиптичке криве, затим ћемо показати својства елиптичких кривих над пољем $\mathbb{C}$, и указаћемо на њену везу са елиптичким интегралима.

Пето поглавље посвећено је тангентно-тетивном закону. Помоћу њега увешћемо сабирање тачака на елиптичкој кривој, па самим тим и дефинисаћемо структуру на њој. Показаћемо да је та структура група, и у случају поља $\mathbb{R}$ реалних бројева даћемо и експлицитне формуле за сабирање тачака на елиптичкој кривој.

Шесто поглавље се бави елиптичким кривама над пољем $\mathbb{Q}$ рационалних бројева. У оквиру њега, упознаћемо се са скупом рационалних тачака елиптичке криве, формулисаћмо Морделову теорему у вези са тим скупом, и даћемо дефиниције торзије и ранга елиптичке криве.

У седмом поглављу упознаћемо елиптичке криве над коначним пољима. Истакнућемо проблем који се јавља приликом одређивања струкутре групе елиптичке криве над пољем $\mathbb{Q}$, и објаснићемо зашто је потребно елиптичке криве посматрати над коначним пољима. Дефинисаћемо L-функцију елиптичке криве и упознаћемо један од седам миленијумских проблема.

Осмо поглавље садржи доказ, прецизније идеју доказа Морделове теореме. То ћемо показати помоћу слабе Морделове теореме, функције висине и теореме о спусту.

Девето поглавље нам показује да, иако су један од најизучаванијих објеката, елиптичке криве имају и велику примену. Посебно ћемо се осврнути на примену коју су елиптичке криве имале при доказу последње Фермаове теорме, која је, не случајно, баш остављена за сам крај овог рада.

На крају, напоменимо да су поред главног циља овог рада обухваћене и неке додатне теме које заузимају значајно место у Теорији елиптичких кривих и које нам, на известан начин, пружају једну комплетнију слику о самим елиптичким кривама. То је и разлог због неуобичајеног обима који овај рад има.

Имена страних математичара су транскрибована на српски језик. Тако је, на пример, написано *Морделова теорема*, уместо *Mordell-ова теорема*. Сва наведена имена у самом раду, налазе се на његовом крају под називом *Индекс имена*. Коришћена литература је, такође, наведена на крају рада.

Текст рада је сложем у LaTeX-у – систему за обраду текста који је намењен писању лепих књига, поготову математичких, [46], [54]. Већина цртежа је урађна помоћу апликације *Геогебра* [9] а мањи број уз помоћ програма *Фотошоп* [56].

Садржај

Увод

• Појам линије

Математика[3] је наука која се развија од када и људски род. Она нам омогућава да спознамо свет око нас. Галилеј[5] је рекао да је велика књига природе написана језиком математике, а Ломоносов[6] сматра да математика доводи ум у хармонију. За математику се каже и да је уметност људског ума. Иако апстрактна[8] наука – чије су теорије сасвим далеко од опипљивог и стварног – она проучава и објекте који су познати већини људи који нису стручњаци за математику. Један од таквих објеката је и *линија*. Она је дело природе и вековима је присутна у људским животима. Појам линије у свести човека постао је јасан веома давно, још у праисторији. Путања баченог камена, зраци светла, облици лишћа и цвећа, ивице обала река и мора, само су неке од појава у природи које су привлачиле пажњу наших предака. Дуготрајним посматрањем тих појава они су поступно усвајали појам линије. Било је потребно доста времена пре него што су људи почели упоређивати и разликовати различите врсте и облике линија.

• Историјски осврт на развој науке о кривама

Уопштавањем и апстраховањем линије настаје математички објекат који називамо *крива*. Први документован интерес за криве јавио се код Менехма[9] око 350. године пре нове ере. Интересовање за криве почело је много пре него што су оне постале предмет математичких проучавања. То се види у многим примерима из праисторије где су линије коришћене као украс на зидовима

---

[3] на грчком *μαθηματικός* што у преводу значи *научни*, од *μάθημα – знање*. Назив *μάθημα* је био у етимолошкој[4] сродности са грчким називом *μαθηματικα – математички списи*, од које потиче модеран назив *Математика*.

[4] *Етимологија* је наука о пореклу речи

[5] Галилео Галилеј (Galileo Galilei, 1564–1642), италијански астроном, физичар, математичар и филозоф

[6] Михаил Васиљевич Ломоносов (Михаи́л Васи́льевич Ломоно́сов, 1711–1765), руски писац и ерудита[7]

[7] синоним за ученог, образованог, начитаног човека, склоног дубоком размишљању

[8] Реч *апстракција* потиче од латинске речи *abstractio* што у преводу значи *издвајање*, *извлачење*, *одвајање*, *одвлачење*. Математика је апстрактна јер нас, на пример, учи сабирању не питајући да ли се ради о крушкама, капиталу или нечем трећем.

[9] Менехмо (Μέναιχμος, око 375–300 пре нове ере), грчки математичар

пећина, или као украс на свакодневним предметима.

Основни принципи на којима је заснована *Теорија кривих* потиче из доба Еуклида[10]. Тада, у време развоја грчке геометрије, пре развоја рачунских операција – специјално диференцијалног рачуна – Теорија кривих је садржала разматрања везана само за елементарне криве: праву, изломљену линију, круг, кружни лук, елипсу, хиперболу и параболу. У средњем веку открића грчких математичара су заборављена. Захваљујући радовима Ојлера[11], Монжа[12] и Гауса[13], Теорија кривих је почела да се развија током 18. и 19. века.

Разни задаци из геометрије, механике, физике, природних наука и технике су основа на којој се развила *наука о кривама*. Геометријска и механичка својства кривих уочавају се, на пример, у грађевинским конструкцијама, оптици, сликарству, архитектури, цртању и геометријским конструкцијама. Неке криве су присутне у физичким појавама, природи и свакодневном животу.

• Алгебарске и елиптичке криве

Посебну улогу међу кривама имају оне које су одређене алгебарским једначинама – *алгебарске криве*. Проучаване су још у старој Грчкој, а данас су најпроучаванији објект *алгебарске геометрије*. *Теорија алгебарских кривих* је велика област са дугом историјом и многобројним применама.

Важна класа алгебарских кривих су *елиптичке криве* – криве задате алгебарским једначинама облика $y^2 = x^3 + ax + b$. Интензивно се проучавају преко сто година, а у последњих сто година су битан део бројних важних математичких резултата. *Теорија елиптичких кривих* спада у лепе и важне теме савремене математике, јер повезује низ важних математичких дисциплина као што су *алгебарска* и *пројективна геометрија*, *теорија бројева*, *алгебра*, *топологија* и друге.

• Диофант и елиптичке криве

Зачеци идеје о елиптичким кривама јављају се још код Диофанта[14]. Он је неодређене кубне једначине решавао помоћу геометријских техника. Једначине је посматрао као криве и за њихова *рационална решења* је тражио све *рационалне тачке* које припадају тој кривој. Методе које је, притом, користио су *метода тангенте* – ако рационална тачка припада кривој, тада тангента криве у тој тачки сече криву у још једној рационалној тачки – и *метода*

[10] Еуклид из Александрије (Εὐκλειδης, око 330–275 пре нове ере), грчки математичар, оснивач геометријске школе у Александрији

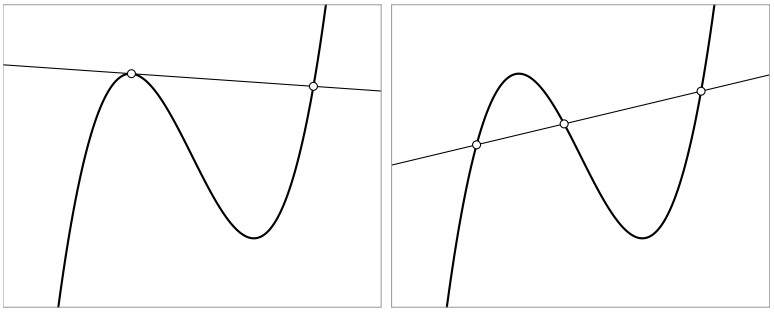
[11] Леонард Ојлер (Leonhard Euler, 1707–1783), швајцарски математичар и физичар

[12] Гаспар Монж (Gaspard Monge, 1746–1818), француски математичар и инжењер

[13] Јохан Карл Фридрих Гаус (Johann Carl Friedrich Gauß, 1777–1855), немачки математичар

[14] Диофант (Διόφαντος, 3. век), грчки математичар. Живео је у Александрији, па је познат и као Диофант Александријски.

тетиве – ако две рационалне тачке припадају кривој, права која је њима одређена сече криву у још једној рационалној тачки.



Те две методе су касније и назване по њему: *Диофантова метода тангенте*, односно *Диофантова метода тетиве*. На њима се заснива тангентно-тетивни закон сабирања на елиптичким кривама.

• Елиптичке криве над пољем $\mathbb{Q}$ рационалних бројева

Иако је за *формалну дефиницију* елиптичке криве потребно познавање алгебарске геометрије, могуће је описати нека њена својства над пољем $\mathbb{Q}$ рационалних бројева коришћењем само школске алгебре и геометрије.

Основни *проблем* у вези са датом елиптичком кривом E састоји се у томе да се одреди скуп $E(\mathbb{Q})$ свих њених рационалних тачака – уколико он постоји. Да би се решио тај проблем уочено је да се на елиптичкој кривој E може увести структура дефинисањем *тангентно-тетивног закона сабирања*. Показује се да је та структура Абелова[15)] група. Скуп $E(\mathbb{Q})$ је једна подгрупа Абелове групе E у односу на дефинисано сабирање. Штавише, према Морделовој[16)] теореми из 1922. године, скуп $E(\mathbb{Q})$ је *коначно генерисана Абелова група*, то јест постоји коначан скуп рационалних тачака такав да се свака друга рационална тачка на елиптичкој кривој E може добити помоћу тангентно-тетивног закона сабирања. Како је свака коначно генерисана Абелова група изоморфна производу цикличних група, можемо описати структуру групе $E(\mathbb{Q})$:

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus \mathcal{T}or(E),$$

где је $\mathbb{Z}^r$ слободна подгрупа, а $\mathcal{T}or(E)$ торзиона подгрупа од $E(\mathbb{Q})$. Број $r \in \mathbb{Z}_0^+$ је ранг од $E(\mathbb{Q})$ или *ранг елиптичке криве* E, и он мери величину групе $E(\mathbb{Q})$, то јест број њених независних рационалних тачака. Проблем је што не постоји алгоритам за одређивање ранга и не зна се који ненегативан цео број може бити ранг елиптичке криве E.

• Елиптичке криве и проблеми за миленијумску награду

Важност теорије елиптичких кривих показује и чињеница да је проблем одређивања *ранга* елиптичке криве предмет чувене Бирч[17)] и Свинертон-Даје-

[15)] Нилс Хенрик Абел (Niels Henrik Abel, 1802–1829), норвешки математичар
[16)] Луис Џоел Мордел (Louis Joel Mordell, 1888–1972), америчко-британски математичар
[17)] Брајан Џон Бирч (Bryan John Birch, 1931), британски математичар

рове[18] хипотезе[19]. Она је један од *седам миленијумских проблема* Клејовог[20] института[21], за чије решење је Институт понудио награду од милион долара.

Бирч и Свинертон-Дајер су 1965. године формулисали хипотезу која укључује такозвану L-функцију елиптичке криве E. То је функција $L(E;s)$ коју можемо доделити елиптичкој кривој E и она одговара броју решења одговарајуће једначине $y^2 = x^3 + ax + b$ по модулу p, где је p прост број. Та хипотеза доводи у везу понашање функције $L(E;s)$ са рангом елиптичке криве.

Доказ ове хипотезе омогућио би нам да одредимо слободну подгупу $\mathbb{Z}^r$ групе $E(\mathbb{Q})$, па самим тим и ранг r елиптичке криве E.

• Елиптичке криве и последња Фермаова теорема

Диофантове једначине и *проблеми* који се проучавају још од старе Грчке, почели су све више да се изучавају у двадесетом веку уз коришћење савременијег и моћнијег апарата у које спадају и елиптичке криве. У доказу најпознатијег таквог проблема – *последње Фермаове*[22] *теореме*, Вајлс[23] је користио теорију елиптичких кривих.

Решење последње Фермаове теореме, показује да елиптичке криве представљају једно од најкориснијих истраживачких оруђа у теорији бројева, па је њихово проучавање изузетно корисно и значајно.

• Елиптичке криве и криптографија

Иако се нећемо посебно бавити у овом раду, напоменимо да кључну улогу у данашњој *криптографији*[24] имају такође елиптичке криве. Иако спадају у «чисту» математику, елиптичке криве су се појавом криптографије показале као изузетно корисне и у примени.

Криптографија је део наше свакодневице, мада често тога нисмо ни свесни. Када обављамо електронске трансакције са банком – плаћамо, уплаћујемо или подижемо новац – преко компјутера (e-banking), мобилног уређаја (m-banking) или банкомата, те трансакције које садрже број нашег рачуна, број картице, и слично, се шифрују, и на другом крају дешифрују, помоћу алгоритма који користи елиптичке криве. Више о криптографији видети у [17], [14] и [15].

---

[18] Питер Свинертон-Дајер (Peter Swinnerton-Dyer, 1927), енглески математичар

[19] Реч *хипотеза* потиче од грчке речи *ὑπόθεσις* што у преводу значи *подлога*, *претпоставка*. У математичкој терминологији има значење исказа за који претпостављамо да је истинит, али који још увек није ни доказан ни оповргнут, односно исказа који се користи у неком расуђивању или доказивању а који се, том приликом, не доказује.

[20] Ландон Томас Клеј (Landon Thomas Clay, 1926–2017), амерички бизнисмен

[21] Clay Mathematics Institute of Cambridge, Massachusetts – CMI)

[22] Пјер Ферма (Pierre de Fermat, 1601–1665), француски математичар и правник

[23] Ендру Џон Вајлс (Andrew John Wiles, 1953), британски математичар

[24] *Криптографија* или *шифровање* је наука која се бави методама очувања тајности информација. Она проналази методе за чување информација у оној форми која ће бити читљива само онима којима је информација намењена док ће за остале бити неупотребљива.

1

Пројективни простори

Неке чињенице у вези са елиптичким кривама «природније» ће нам деловати кроз знања о пројективним просторима. Због тога, у овом поглављу, подсетићемо се, укратко, пројективног простора. Поновићемо векторске и афине просторе, али само у оној мери која нам је неопходна за излагање о пројективним просторима. За више детаља о њима погледати у [23], [24], [25] и [7].

1.1 Векторски простори

Од првих почетака античке геометрије, Еуклидових *Елемената* [1)], преко Њутнове[2)] механике, истраживања нееуклидских геометрија, па до Ајнштајнове[3)] теорије релативности, геометрија је највеће подстицаје имала у настојањима човека да опише свет у коме живи. Геометрија која се учи у основној и средњој школи заснована је на претпоставци да је простор у коме живимо добро апроксимиран *еуклидским простором*, или прецизније претпостављамо да је

[1)] *Елементи* ($\Sigma\tau o\iota\chi\varepsilon\tilde{\iota}\alpha$) су најчувенији и најутицајнији уџбеник геометрије грчког математичара Еуклида. Он је тим уџбеником поставио темеље геометрији која се по њему и назива *еуклидска геометрија*. *Елементи* систематски излажу грчка геометријска знања тог времена аксиоматском методом, и представљају прву аксиоматизацију математике. Због тога се еуклидска геометрија често користи као средство за учење аксиоматског метода. *Елементи* садрже тринаест књига од којих првих шест обухватају *планиметрију*, наредних четири *геометријску теорију бројева*, а последње три *стереометрију*. Они представљају изванредан образац изградње геометрије дедуктивном методом. Елементарна геометрија, која се изучава у школама многих земаља света, се у мало чему разликује од геометрије изложене у *Елементима*. Након *Библије*, *Елементи* су књига која је доживела највише издања – 1700 издања до 1900. године. Зато је називају и «геометријском Библијом».

[2)] Исак Њутн (Isaac Newton, 1643–1727), енглески математичар, физичар, теоријски механичар и астроном, један од највећих научника у историји

[3)] Алберт Ајнштајн (Albert Einstein, 1879–1955), теоријски физичар рођен у Немачкој у јеврејској породици, један од твораца савремене физике

простор у коме живимо описан *аксиомама* које је понудио Хилберт[4)], крајем 19. и почетком 20. века прилагођавајући *Еуклидову аксиоматику* дату у *Елементима* савременом математичком језику.

Вишевековна примена геометрије, а нарочито потреба да се објасне појмови силе и кретања у физици и механици, довели су до појаве вектора[5)]. Уопштавањем и апстраховањем вектора и операција са њима, долазимо до векторског или линеарног простора – основног објекта у линеарној алгебри.

• Дефиниција векторскг простора

Дефиниција 1.1. *Векторски* или *линеарни простор* над датим пољем $\mathbb{K}$ је уређена четворка $(\mathbb{V}, \mathbb{K}, +, \cdot)$ скупа $\mathbb{V}$, поља $\mathbb{K}$, једне бинарне операције

$$(u, v) \mapsto u + v \qquad \mathbb{V} \times \mathbb{V} \to \mathbb{V},$$

којом се сваком пару елемената u и v из $\mathbb{V}$ придружује неки елемент $u + v$ из $\mathbb{V}$, и једне спољне $\mathbb{K}$-операције

$$(\alpha, v) \mapsto \alpha \cdot v \qquad \mathbb{K} \times \mathbb{V} \to \mathbb{V},$$

којом се сваком елементу α из $\mathbb{K}$ и сваком елементу v из $\mathbb{V}$ придружује неки елемент $\alpha \cdot v$ из $\mathbb{V}$, таква да за свако u, v и w из $\mathbb{V}$ и свако α и β из $\mathbb{K}$ важе следећи услови или *аксиоме векторског простора*:

В1. $(\mathbb{V}, +)$ је Абелова група, то јест:

- 1° $u + (v + w) = (u + v) + w$,
- 2° постоји елемент 0 из $\mathbb{V}$ такав да је $v + 0 = v$,
- 3° за свако v из $\mathbb{V}$ постоји јединствени елемент $-v$ такав да је $v + (-v) = 0$,
- 4° $u + v = v + u$,

В2. $\alpha \cdot (\beta \cdot v) = (\alpha \cdot \beta) \cdot v$ (квазиасоцијативност),

В3. $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$ (квазидистрибутивност),

В4. $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$ (квазидистрибутивност),

В5. $1 \cdot v = v$ (нетривијалност),

при чему је $1 = 1_{\mathbb{K}}$ јединица, а $\alpha + \beta$ и $\alpha \cdot \beta$ су сума и производ елемената α и β у уоченом пољу $\mathbb{K}$.

Елементе скупа $\mathbb{V}$ зовемо *векторима*, а елементе из поља $\mathbb{K}$ *скаларима*[6)] у том

[4)] Давид Хилберт (David Hilbert, 1862–1943), немачки математичар

[5)] Реч *вектор* потиче од латинске речи *veho*, *vehere* што у преводу значи *вући*, *возити*, *теглити*, односно *vector* што у преводу значи *преносилац*, *ко нешто носи* [*на себи*].

[6)] Реч *скалар* потиче од латинских речи *scala lestve* што у преводу значи *објекат који има своје место на скали* [*бројева*].

векторском простору. Кажемо и да је сам скуп $\mathbb{V}$ један векторски простор над пољем $\mathbb{K}$, или само $\mathbb{K}$-векторски простор у односу на уочене операције.

Векторски простор је *реалан*, односно *комплексан*, ако је $\mathbb{K} = \mathbb{R}$, односно $\mathbb{K} = \mathbb{C}$.

Ако је јасно о ком пољу $\mathbb{K}$ је реч, и ако нема потребе истицати његове операције $+$ и $\cdot$, убудуће уместо векторски простор $(\mathbb{V}, \mathbb{K}, +, \cdot)$ рећи ћемо векторски простор $\mathbb{V}$ или само простор $\mathbb{V}$.

• Координатни векторски простор

Дефиниција 1.2. За свако поље $\mathbb{K}$ и било који природан број n, скуп

$$\mathbb{K}^n = \{(x_1, \ldots, x_n) \mid x_r \in \mathbb{K}\}$$

свих уређених n-торки $(x_1, \ldots, x_n)$, са x_r-овима из $\mathbb{K}$ јесте и један векторски простор над $\mathbb{K}$. Називамо га *координатним векторским простором* димензије n над уоченим пољем $\mathbb{K}$.

Ако је $\mathbb{K}$ поље $\mathbb{R}$ реалних бројева, координатни векторски простор $\mathbb{R}^n$ називамо *стандардним векторским простором* над пољем $\mathbb{R}$.

1.2 Афини простори

У простору тачака, где је тачка један од основних појмова, можемо увести нови објекат – вектор. Тако простору тачака придружујемо један векторски простор над пољем $\mathbb{K}$ у коме нема тачака већ је основни објекат вектор. Да бисмо, у том простору, увели тачке као нове објекте, то јест помоћу векторског простора увели простор тачака морамо посматрати нову врсту простора – афине[7)] просторе – у коме су основни објекти тачка и вектор. Тиме успостављамо једну фундаменталну везу између две основне области математике – геометрије и алгебре. Та веза нам омогућава да многе важне особине векторских простора пренесемо на простор тачака и тако неке геометријске проблеме потпуније разумемо и знатно једноставније докажемо.

• Дефиниција афиног простора

Дефиниција 1.3. *Афини простор* над датим пољем $\mathbb{K}$ је уређена тројка $(\mathcal{A}, \mathbb{V}, +)$ скупа $\mathcal{A}$ – чије елементе зовемо *тачкама*, векторског $\mathbb{V}$ над пољем $\mathbb{K}$ и једног пресликавања

$$(A, v) \mapsto A + v \qquad \mathcal{A} \times \mathbb{V} \to \mathcal{A}$$

[7)] Реч *афина* потиче од Ојлера, који у својој књизи *Introductio in analysin infinitorum* из 1748. године користи латинску реч *affinis*, што у преводу значи *сродно*, односно *повезано*.

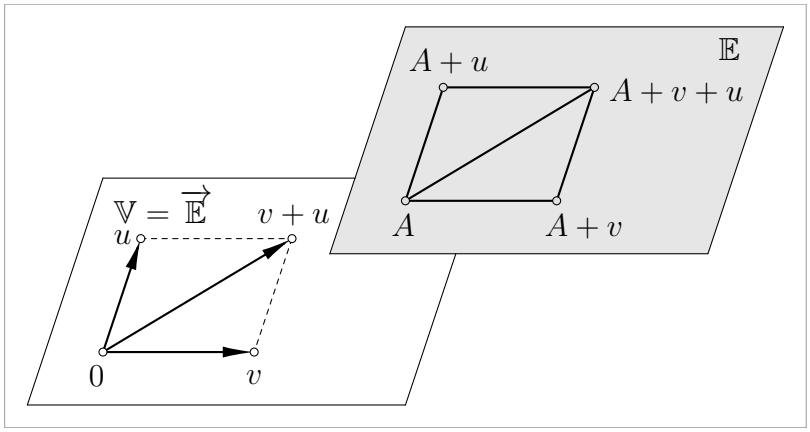
којим се сваком пару (A, v) елемената A из $\mathcal{A}$ и v из $\mathbb{V}$ придружује неки елемент $A + v$ из $\mathcal{A}$, које задовољава следеће услове или *аксиоме афиног простора*:

A1. $A + 0 = A$ за сваку тачку A из $\mathcal{A}$,

A2. $(A + v) + u = A + (v + u)$ за сваку тачку A из $\mathcal{A}$ и свако v и u из $\mathbb{V}$,

A3. За сваки пар тачака A и B из $\mathcal{A}$ постоји тачно један вектор v из $\mathbb{V}$, такав да је $B = A + v$.

Ова дефиниција илустрована је следећим цртежом.



Афини простор $(\mathcal{A}, \mathbb{V}, +)$ се састоји из *тачака* $A, B, \ldots$, *вектора* $v, u, \ldots$ и *скалара* $\alpha, \beta, \ldots$, и када говоримо о њима мислимо на тачке из скупа $\mathcal{A}$, односно на векторе и скаларе из векторског простора $\mathbb{V}$.

Уколико то не доводи до забуне, афини простор $(\mathcal{A}, \mathbb{V}, +)$ ћемо означавати истим симболом као и његов скуп тачака, то јест са $\mathcal{A}$.

Јединствени вектор v из аксиоме A3 означавамо са $B - A$ или $\overrightarrow{AB}$, па је

$$B = A + v \Leftrightarrow v = B - A \Leftrightarrow v = \overrightarrow{AB}.$$

Уз то, ако је и $C = B + u$, према аксиоми A2, тада је и $C = A + (v + u)$, чиме се и саме аксиоме A1, A2 и A3 своде на:

⟨1⟩ за произвољне три тачке A, B и C из $\mathbb{E}$ важи $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$ (аксиома троугла),

⟨2⟩ за сваку тачку A из $\mathbb{E}$ и сваки вектор v из $\mathbb{V}$ постоји и тачно једна тачка B из $\mathbb{E}$ за коју је $v = \overrightarrow{AB}$ (аксиома надовезивања).

• Директриса и димензија афиног простора

Дефиниција 1.4. За векторски простор $\mathbb{V}$ кажемо да је придружен афином простору $(\mathcal{A}, \mathbb{V}, +)$. Називамо га и *директрисом* или *простором транслација* афиног простора $\mathcal{A}$.

Дефиниција 1.5. *Димензија* афиног простора $\mathcal{A}$ је димензија његове директрисе $\mathbb{V}$, то јест $\dim \mathcal{A} = \dim \mathbb{V}$.

Афине просторе димензије један зовемо и *афиним правама*, а оне димензије два, *афиним равнима*. Ако је афини простор димензије нула, његова директриса садржи само нула вектор, па тада и сам афини простор садржи само једну тачку.

Уколико желимо да истакнемо димензију афиног простора, писаћемо $\mathcal{A}^n$, или, ако је потребно, $(\mathcal{A}^n, \mathbb{V}^n, +)$.

Потпростор димензије $n-1$ или кодимензије 1 називамо *хиперраван*[8] у афином простору димензије n.

Афини простор је *реалан*, односно *комплексан*, ако је одговарајући векторски простор реалан, односно комплексан.

• Афинизација векторског простора

Ако у афином простору $(\mathcal{A}, \mathbb{V}, +)$ ставимо да је $\mathcal{A} = \mathbb{V}$, тако добијени простор $(\mathbb{V}, \mathbb{V}, +)$ је такође један афини простор, и у њему се тачке и вектори подударају – ако је A било која тачка из $\mathcal{A}$, она је и вектор у $\mathbb{V}$.

Дефиниција 1.6. Афини простор $(\mathbb{V}, \mathbb{V}, +)$ називамо *стандардном афинизацијом* или само *афинизацијом* уоченог векторског простора $\mathbb{V}$ и означавамо га са

$$\mathbb{V}_{\text{af}} = \mathbb{V} = \mathcal{A} = (\mathbb{V}, \mathbb{V}, +).$$

Посебно, ако је директриса $\mathbb{V}$ скуп $\mathbb{K}^n$ свих n-торки са компонентама из поља $\mathbb{K}$, тада су тачке и вектори тог афиног простора $\mathbb{K}^n_{\text{af}}$ уређене n-торке са компонентама из $\mathbb{K}$. Означаваћемо га и са $\mathbb{A}^n(\mathbb{K})$[10]:

$$\mathbb{A}^n(\mathbb{K}) = \big\{(x_1, \ldots, x_n) \mid x_i \in \mathbb{K},\, i = 1, \ldots, n\big\} = \mathbb{K}^n. \tag{1.1}$$

За нас су од посебног интереса афини простори $\mathbb{A}^1(\mathbb{K})$ димензије један

$$\mathbb{A}^1(\mathbb{K}) = \big\{x \mid x \in \mathbb{K}\big\} = \mathbb{K}^1 = \mathbb{K} \quad - \quad \textit{афина права},$$

односно афини простори $\mathbb{A}^2(\mathbb{K})$ димензије два

$$\mathbb{A}^2(\mathbb{K}) = \big\{(x, y) \mid x, y \in \mathbb{K}\big\} = \mathbb{K}^2 = \mathbb{K} \times \mathbb{K} \quad - \quad \textit{афина раван}.$$

[8] Префикс *хипер-* потиче од грчке речи *νπερ* што у преводу значи *изнад, над, преко*. Као први део сложенице употребљава се да означи *нешто више, јаче, у већој мери, повећано*. У математичкој терминологији, назив хиперраван потиче од вишедимензионалне аналогије[9] дводимензионалне равни у тродимензионалном простору.

[9] Реч *аналоган* потиче од грчке речи *ανалογος* што у преводу значи *сличан, подобан, сагласан, одговарајући, сродан, истоврстан*; *који одговара неком закону, правилу, типу или обрасцу*.

[10] користићемо ову ознаку уобичајену у алгебарској геометрији

Ако је $\mathbb{K} = \mathbb{R}$ реалну афину праву $\mathbb{A}^1(\mathbb{R}) = \mathbb{R}^1 = \mathbb{R}$ називамо *реална права*, а реалну афину раван $\mathbb{A}^2(\mathbb{R}) = \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ *реална раван*.

За $\mathbb{K} = \mathbb{C}$ комплексну афину праву $\mathbb{A}^1(\mathbb{C}) = \mathbb{C}^1 = \mathbb{C}$ називамо *комплексна права*, а комплексну афину раван $\mathbb{A}^2(\mathbb{C}) = \mathbb{C}^2 = \mathbb{C} \times \mathbb{C}$ *комплексна раван*.

Реалну раван $\mathbb{R}^2$ у којој представљамо комплексне бројеве звaћемо и *Гаусова раван* и означаваћемо је, такође, са $\mathbb{C}$.

• Координате

Да бисмо у афином простору оперативно записивали геометријске објекте, уводимо координате избором координатног система. Тиме, такође, успостављамо везу геометрије и алгебре.

Дефиниција 1.7. Уређену n-торку $(x_1, \ldots, x_n)$ из једнакости (1.1) називамо *афиним координатама* или само *координатама* како тачке, тако и вектора тог афиног простора.

Поред афиних, тачке афиног простора могу имати и хомогене афине или кажемо само хомогене[11)] координате.

Дефиниција 1.8. Нека су $(x_1, \ldots, x_n)$ координате тачке из афиног простора. Кажемо да су $X_1, \ldots, X_n, X_{n+1}$ њене *хомогене координате* ако важи

$$\frac{X_1}{X_{n+1}} = x_1, \ldots, \frac{X_n}{X_{n+1}} = x_n, X_{n+1} \neq 0.$$

Ако хомогене координате помножимо једним истим бројем $\lambda \neq 0$ оне представљају исту тачку, то јест $(n+1)$-торке

$$(X_1, \ldots, X_{n+1}) \quad \text{и} \quad (\lambda X_1, \ldots, \lambda X_{n+1}), \lambda \neq 0$$

су координате исте тачке, па хомогене координате тачака афиног простора нису јединствене. Због тога, хомогене координате означавамо са двотачком уместо са запетом, то јест пишемо

$$(X_1 : \cdots : X_{n+1}).$$

Сама та ознака нам сугерише да је код хомогених координата битан однос бројева $X_1, \ldots, X_{n+1}$, а не вредност сваког од њих појединачно. Кажемо и да су хомогене координате дефинисане до на множење константом, односно одређене до на хомогеност.

• Бесконачно далека тачка и пројективизација

Увођење хомогених координата омогућава нам да афином простору додамо бесконачно далеке тачке.

[11)] Реч *хомоген* потиче од грчке речи *ὁμογενής* што у преводу значи *једнородност*, *онај који има иста својства у сваком делу и увек*.

Дефиниција 1.9. *Бесконачно далека тачка* је објекат који дефинишемо у хомогеним координатама $(X_1 : \cdots : X_n : X_{n+1})$ условом

$$X_{n+1} = 0,$$

а међу преосталим координатама је бар једна различита од нуле.

Ако је, на пример, тачка A бесконачно далека, писаћемо

$$A_\infty = (X_1 : \cdots : X_n : 0).$$

Предност хомогених координата је да оне «лепо» представљају бесконачно далеке тачке.

Дефиниција 1.10. Додавање бесконачно далеких тачака афином простору називамо *пројективазацијом* афиног простора.

Пројективизацијом добијамо потпунију слику о објектима у афином простору. Због тога бесконачно далеке тачке у извесном смислу издвајамо од преосталих тачака афиног простора.

Бесконачно далеке тачке формирају хипераван коју називамо *бесконачно далека хипераван*. У афиној равни хипераван је *бесконачно далека права*.

1.3 Пројективни простори

Постоји простор у коме ни на који начин не издвајамо бесконачно далеке тачке, то јест у коме су тачке и бесконачно далеке тачке равноправне. Називамо га пројективни простор. Геометрија тог простора – пројективна[12)] геометрија – је краљица свих геометрија. Она је синоним за модерну геометрију 19. века.

У почетку, пројективном геометријом су се бавили сликари, инжењери, архитекте и тек по неки математичар. Главни разлог за то били су управо проблеми са цртањем на које су они свакодневно наилазили, посебно проблем цртања илузије просторне дубине, онако како то ми реално видимо. Због тога, њихови радови су били доста непрецизни и непотпуни, али су успели много тога да открију. Најзначајнији међу њима био је Дезарг[13)].

Оснивач модерне пројективне геометрије био је Понселе[14)], који је преузео идеје свог учитеља Монжа и разрадио их на вишем апстрактном нивоу. Он је, за време заробљеништва у Русији 1813, аналитички доказао[15)] једну

[12)] Реч *пројективан* потиче од новолатинске речи *projectivus* што у преводу значи *избачен, који баца, бацачки*.

[13)] Жерар Дезарг (Girard Desargues, 1591–1661), француски математичар и инжењер

[14)] Жан Виктор Понселе (Jean Victor Poncelet, 1788–1867), француски математичар и инжењер

[15)] то јест доказао је методом координата које подразумева да геометријским објектима придружујемо уређене n-торке бројева

од најлепших, најважнијих и најдубљих теорема[16] класичне геометрије чији доказ[17] представља синтетички[18] начин увођења структуре групе на елиптичкој кривој.

• Хомогене координате

С обзиром на то да су све тачке пројективног простора равноправне, хомогене координате можемо дефинисати над било којим пољем $\mathbb{K}$, при том не користећи појам афиног простора.

Дефиниција 1.11. Две $(n+1)$-торке $(X_1, \ldots, X_{n+1})$ и $(X'_1, \ldots, X'_{n+1})$ скупа $\mathbb{K}^{n+1} \setminus \{(0, \ldots, 0)\}$ су у релацији $\sim$ ако је

$$(X'_1, \ldots, X'_{n+1}) = \lambda(X_1, \ldots, X_{n+1}),$$

што је еквивалентно са $X'_i = \lambda X_i$ за $i = 1, \ldots, n+1$ и $\lambda \neq 0$.

На основу [7, страна 11], важи

Лема 1.1. Релација $\sim$ дефинисана на скупу $\mathbb{K}^{n+1} \setminus \{(0, \ldots, 0)\}$ је релација еквиваленције. □

Уведена еквиваленција раставља скуп $\mathbb{K}^{n+1} \setminus \{(0, \ldots, 0)\}$ на класе еквиваленције. Класу еквиваленције $\big\{(X_1, \ldots, X_{n+1}) \mid (X_1, \ldots, X_{n+1}) \sim (X'_1, \ldots, X'_{n+1})\big\}$ у односу на ту релацију означавамо са $(X_1 : \cdots : X_{n+1})$. Скуп

$$\big\{(X_1 : \cdots : X_{n+1}) \mid X_i \in \mathbb{K},\, i = 1, \ldots, n\big\}$$

свих класа еквиваленције, то јест количнички скуп скупа $\mathbb{K}^{n+1} \setminus \{(0, \ldots, 0)\}$ означаваћемо са $\mathbb{P}^n(\mathbb{K})$[19]. Дакле,

$$\begin{aligned}\big(\mathbb{K}^{n+1} \setminus \{(0, \ldots, 0)\}\big) /_\sim &= \big\{(X_1, \ldots, X_{n+1}) \mid X_i \in \mathbb{K},\, i = 1, \ldots, n\big\} /_\sim \\ &= \big\{(X_1 : \cdots : X_{n+1}) \mid X_i \in \mathbb{K},\, i = 1, \ldots, n\big\} \\ &= \mathbb{P}^n(\mathbb{K}).\end{aligned}$$

• Дефиниција пројективног простора

Пројективни простори су сложени математички објекти, јер се они добијају као количнички простори. Поред пројективне геометрије, проучавају их и

[16] *Понселеова теорема*, [12, страна 23]: Нека су $\mathcal{C}$ и $\mathcal{D}$ две равне конике. Претпоставимо да постоји полигон уписан у $\mathcal{C}$ и описан око $\mathcal{D}$. Тада има бесконачно много таквих полигона и сви они имају исти број страница. Свака тачка конике $\mathcal{C}$ може бити теме таквог полигона.

[17] Тај нови доказ, чисто геометријски, објављен је у *Traité des propriétés projectives des figures*, 1822. године.

[18] то јест без коришћења метода алгебре и анализе, заснивајући се само на геометријским објектима

[19] користићемо ову ознаку уобичајену у алгебарској геометрији

диференцијална геометрија, алгебарска геометрија, топологија и друге дисциплине. Дефинишемо их као просторе тачака које су у бијекцији са хомогеним координатама. Прецизније,

Дефиниција 1.12. *Пројективни простор* димензије n над пољем $\mathbb{K}$ је уређени пар $(\mathcal{P}^n, \mathfrak{P})$ скупа $\mathcal{P}^n$ – чије елементе зовемо *тачкама* и једне бијекције

$$A \mapsto \mathfrak{P}(A) = (X_1 : \cdots : X_{n+1}) \qquad \mathcal{P}^n \to \mathbb{P}^n(\mathbb{K})$$

којом се сваком елементу A из $\mathcal{P}$ придружује неки елемент $(X_1 : \cdots : X_{n+1})$ из $\mathbb{P}^n(\mathbb{K})$.

У том случају, $(X_1 : \cdots : X_{n+1})$ називамо *хомогене* или *пројективне* координате тачке A из $\mathcal{P}^n$. Уочимо да у пројективном простору димензије n имамо $n+1$ координату.

Пошто се бијекција $\mathfrak{P}$ подразумева, у ознаци за пројективни простор ћемо је најчешће изостављати, то јест уместо $(\mathcal{P}^n, \mathfrak{P})$ писаћемо само $\mathcal{P}^n$.

Пројективне просторе $\mathcal{P}^1$ димензије један зовемо *пројективним правама*, а пројективне просторе $\mathcal{P}^2$ димензије два *пројективним равнима*.

• Комплексификација

Пројективни простор је *реалан*, односно *комплексан*, ако је $\mathbb{K} = \mathbb{R}$, односно $\mathbb{K} = \mathbb{C}$, то јест ако су координате $(X_1 : \cdots : X_{n+1})$ реалне, односно комплексне.

Због алгебарске незатворености поља $\mathbb{R}$, јављају се многи проблеми. Решавамо их комплексификацијом.

Дефиниција 1.13. Смештање реалног пројективног простора у одговарајући комплексни пројективни простор називамо *комплексификацијом*.

Пројективизација и комплексификација нам омогућавају потпуно схватање пројективних објеката.

• Пројективни простор хомогених координата

Ако у пројективном простору $(\mathcal{P}^n, \mathfrak{P})$ ставимо да је $\mathcal{P}^n = \mathbb{P}^n(\mathbb{K})$ и $\mathfrak{P} = Id$, тако добијени простор $(\mathbb{P}^n(\mathbb{K}), Id)$ је такође један пројективни простор.

Дефиниција 1.14. Пројективни простор $(\mathbb{P}^n(\mathbb{K}), Id)$ називамо *пројективни простор хомогених координата* и означавамо га са $\mathbb{P}^n(\mathbb{K})$.

За нас су од посебног интереса пројективни простори $\mathbb{P}^1(\mathbb{K})$ димензије један

$$\mathbb{P}^1(\mathbb{K}) = \big\{(X : Y) \mid X, Y \in \mathbb{K}\big\} \quad - \quad \textit{пројективна права},$$

односно пројективни простори $\mathbb{P}^2(\mathbb{K})$ димензије два

$$\mathbb{P}^2(\mathbb{K}) = \big\{(X : Y : Z) \mid X, Y, Z \in \mathbb{K}\big\} \quad - \quad \textit{пројективна раван}.$$

Ако је $\mathbb{K} = \mathbb{R}$ пројективну праву $\mathbb{P}^1(\mathbb{R})$ називамо *реална пројективна права*, а пројективну раван $\mathbb{P}^2(\mathbb{R})$ *реална пројективна раван*. За $\mathbb{K} = \mathbb{C}$ пројективну праву $\mathbb{P}^1(\mathbb{C})$ називамо *комплексна пројективна права*, а пројективну раван $\mathbb{P}^2(\mathbb{C})$ *комплексна пројективна раван*.

Пројективна права $\mathbb{P}^1(\mathbb{K})$ се састоји од афине праве $\mathbb{A}^1(\mathbb{K})$ коју можемо идентификовати са подскупом

$$\big\{(X:Y) \mid Y \neq 0\big\} = \left\{ \left(\frac{X}{Y} : 1\right) \;\middle|\; X \in \mathbb{K} \right\} \subset \mathbb{P}^1(\mathbb{K})$$

и још једне бесконачно делеке тачке $X_\infty(1:0)$, то јест

$$\mathbb{P}^1(\mathbb{K}) = \mathbb{A}^1(\mathbb{K}) \sqcup {}^{20)}\{X_\infty\}. \tag{1.2}$$

Слично је

$$\mathbb{P}^2(\mathbb{K}) = \mathbb{A}^2(\mathbb{K}) \sqcup p_\infty, \tag{1.3}$$

при чему је p_∞ бесконачно далека права.

И уопште, за сваки пројективни простор $\mathbb{P}^n(\mathbb{K})$ важи

$$\mathbb{P}^n(\mathbb{K}) = \mathbb{A}^n(\mathbb{K}) \sqcup \mathbb{P}^{n-1}(\mathbb{K}).$$

Због једнакости (1.2) кажемо да пројективна права локално изгледа као афина права. Слично, због једнакости (1.3) кажемо да пројективна раван локално изгледа као афина раван. Због ове повезаности између пројективне и афине праве, односно пројективне и афине равни, сва тврђења која важе у пројективном, важе и у афином случају.

• Пројективни простор и визуелизација. Равни $\mathcal{S}^2$ и $\overline{\mathbb{R}}^2$

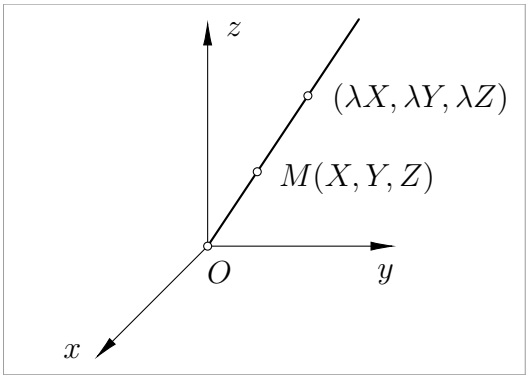
Визуелизација, као начин да се апстрактни појмови приближе људском уму, одувек је била повезана са геометријом. Наш визуелни свет, иако многи људи тога нису свесни, има геометрију ближу пројективном него еуклидском простору[21)]. Због тога су математичари почели све више да верују у бесконачно далеке тачке, доживљавајући основне концепте геометрије као пројективне.

С друге стране, пројективни простор није лако визуелизовати. Навешћемо две визуализације реалне пројективне равни $\mathbb{P}^2(\mathbb{R})$.

Нека је $\mathbb{A}^3(\mathbb{R}) = \mathbb{R}^3$ реалан афини тродимензионални простор. Посматрајмо скуп свих правих које пролазе кроз координатни почетак O. Тај скуп називамо *сноп* са центром O, и означавамо га истим словом O. Свака права снопа једнозначно је одређена задавањем неке своје тачке M која је различита од тачке O. Нека су (X, Y, Z) координате тачке M.

[20)] Овом угластом ознаком краће означавамо *дисјунктну унију*, то јест унију $\mathbb{A}^1(\mathbb{K}) \cup \{X_\infty\}$ где је $\mathbb{A}^1(\mathbb{K}) \cap \{X_\infty\} = \emptyset$

[21)] Илуструјмо то на следећем примеру: стојимо на прузи и посматрамо шине, уз претпоставку да је пруга права. Шине су паралелне, али нама изгледа као да се њихово растојање постепено смањује, тако да се оне завршавају једној [бесконачно далекој] тачки.

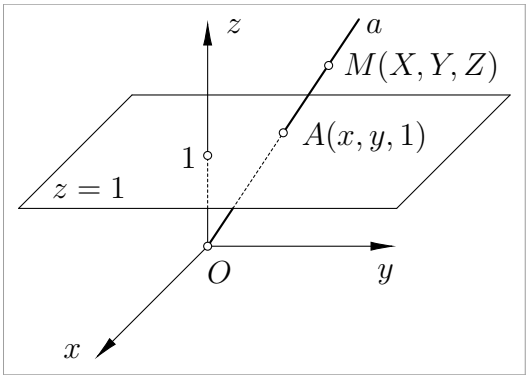


Тада тачка $(\lambda X, \lambda Y, \lambda Z)$ за свако $\lambda \neq 0$ одређује ту исту праву OM[22)]. Праву, разматрану као елемент снопа, називамо *тачка*, а тројку $(X : Y : Z)$ њеним *хомогеним координатама*. Скуп свих тачака, то јест правих у снопу O, задовољава услове дефиниције (1.12) пројективног простора за $n = 2$ и $\mathbb{K} = \mathbb{R}$. На тај начин добили смо један модел реалне пројективне равни $\mathbb{P}^2(\mathbb{R})$. Називамо га *сноп модел пројективне равни* и означавамо га са $\mathcal{S}^2$. Сви елементи ове пројективне равни, то јест праве снопа су геометријски равноправни.

Дакле, реалну пројективну раван $\mathbb{P}^2(\mathbb{R})$ можемо схватити као скуп правих у простору $\mathbb{R}^3$ које садрже координатни почетак O, то јест као сноп правих у простору $\mathbb{R}^3$ са центром у тачки O. Према томе,

$$\mathbb{P}^2(\mathbb{R}) = \big\{(X : Y : Z) \mid X, Y, Z \in \mathbb{R}\big\} = \mathcal{S}^2.$$

Реалну пројективну раван $\mathbb{P}^2(\mathbb{R})$ можемо визуелизовати и на други начин. Посматрајмо, опет, $\mathbb{A}^3(\mathbb{R}) = \mathbb{R}^3$ реалан афини тродимензионални простор и сноп правих у том простору са центром у координатном почетку O. Уочимо неку раван која не садржи координатни почетак O.



[22)] Слично и ми видимо објекте око нас, односно цртамо то што видимо. Људско око идентификује све тачке које се налазе на једном зраку – замишљеној полуправој[23)] у простору која полази из ока – односно види само једну тачку која представља тај зрак. Тако, на пример, када сликар постави платно, свака тачка коју видимо на слици представља пресек зрака и платна, то јест полуправе и равни.

[23)] Уместо полуправе можемо узети и праву. То неће ништа битно променити јер део праве «иза ока» нећемо видети нити ће он сећи платно, а с друге стране, може битно олакшати посао у заснивању пројективне геометрије.

Нека је то, на пример, раван која је параралелна са xOy равни и на растојању један од координатног почетка, то јест раван $z = 1$[24]. Свака права a снопа O, која је једнозначно одређена тачком $M(X, Y, Z)$, осим оних које припадају xOy равни, то јест равни $z = 0$, сече раван $z = 1$ у тачки $A(\frac{X}{Z}, \frac{Y}{Z}, 1)$. То значи да свакој правој a која не припада равни $z = 0$ одговара тачка $A(\frac{X}{Z}, \frac{Y}{Z}, 1)$. Ако означимо $\frac{X}{Z}$ са x, а $\frac{Y}{Z}$ са y, координате тачке A су $(x, y, 1)$. Зато сваку праву a снопа O која не припада равни $z = 0$ можемо поистоветити са поменутим пресечним тачкама $A(x, y, 1)$ које се налазе у равни $z = 1$. Преостале тачке $(x, y, 0)$ чине бесконачно далеку праву.

Дакле, реалну пројективну раван $\mathbb{P}^2(\mathbb{R})$ можемо схватити као афину раван $\mathbb{R}^2$ којој смо додали бесконачно далеку праву p_∞. Овај модел називамо *допуњена* или *проширена афина раван* и означавамо са $\overline{\mathbb{R}}^2$. Према томе,

$$\mathbb{P}^2(\mathbb{R}) = \big\{(X : Y : Z) \mid X, Y, Z \in \mathbb{R}\big\} = \mathbb{R}^2 \cup p_\infty = \overline{\mathbb{R}}^2.$$

Ова раван је природни амбијент за криве другог реда, перспективне цртеже и друге објекте.

[24] Раван $z = 1$ смо изабрали потпуно произвољно, то јест уместо ње смо могли да посматрамо било коју другу раван која не садржи тачку $(0, 0, 0)$.

2
Увод у криве

Елиптичке криве су, као што им и само име каже, криве, па ћемо се због тога, у овом поглављу, подсетити најосновнијих чињеница у вези са појмом криве. За више детаља погледати [41], [30], [58] и [11].

2.1 Дефинисање криве

• Појам криве

Крива је веома важан математички појам. Можемо је дефинисати и задати на разне начине.

Као што је уобичајено у математици али и у другим наукама[1)], према [41, 2.2, страна 43] полазимо од најједноставнијих објеката у афином простору $\mathbb{R}^n$ који су у неком смислу једнодимензионални и њих називамо *кривама*. За криву кажемо и да је *најједноставнији нелинеарни објекат*. Ми ћемо се ограничити на случај када је $n = 2$, то јест на криве у равни $\mathbb{R}^2$.

• Проблеми при дефинисању криве

Кроз историју било је много погрешних дефиниција криве. Чак је и Жордан[2)] у 19. веку дао једну дефиницију која је у почетку била прихваћена од математичара, а за коју се касније утврдило да није тачна. Наиме, он је сматрао да је крива непрекидна слика једног сегмента из поља $\mathbb{R}$ реалних бројева.

После извесног времена, Пеано[3)] је задивио математички свет уочивши да

[1)] Заправо ради се о принципу: од једноставнијег ка сложенијем.

[2)] Мари Енемон Камиј Жордан (Marie Ennemond Camille Jordan, 1838–1922), француски математичар

[3)] Ђузепе Пеано (Giuseppe Peano, 1858–1932), италијански математичар и логичар

је претпоставка о непрекидности таквог пресликавања недовољна. Да би то показао, он је 1890. године конструисао непрекидно пресликавање одређеног сегмента из $\mathbb{R}$ у $\mathbb{R}^2$ чија је слика цео квадрат. Тако је добио објекат који прекрива цео квадрат, то јест објекат чија је димензија већа од један. Илуструјмо то на следећем примеру, који је преузет из [11, страна 5].

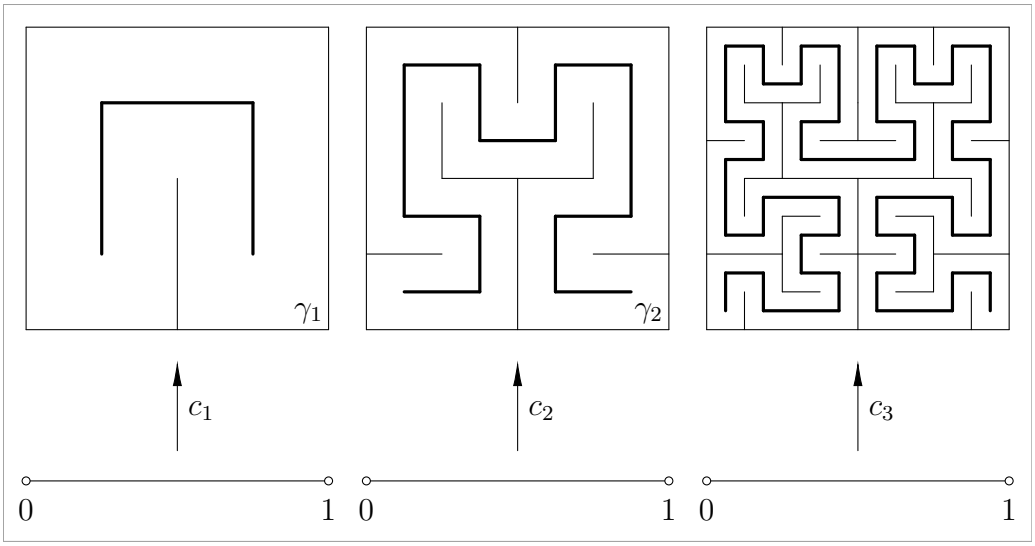
Пример 2.1. [**Пеанова крива**] Нека је

$$c_n : \mathbb{R} \supseteq [0,1] \to [0,1] \times [0,1] \subseteq \mathbb{R}^2,$$

где је n из $\mathbb{N}$, непрекидно пресликавање сегмента $[0,1]$ у квадрат $[0,1]\times[0,1]$ дефинисано са

$$c_n(t) = \gamma_n(t),\ t \in [0,1],$$

при чему је γ_n дато на следећи начин. Поделимо дати квадрат на 4 подударна квадрата. Обришимо три од укупно четири странице малих квадрата које не леже на страницама великог квадрата. Тада је γ_1 изломљена линија која спаја центре 4 мала квадрата и која је састављена од дужи паралелних страницама квадрата. Затим, поделимо дати квадрат на 16 подударних квадрата. Избацимо сада неколико унтрашњих страница 16 квадрата, тако да је комплемент преосталих страница и страница из првог корака повезан скуп. Тада је γ_2 изломљена линија која спаја центре 16 малих квадрата и која је састављена од дужи паралелних страницама квадрата.



Ако продужимо овај поступак, добијамо да је

$$\gamma(t) = \lim_{n\to\infty} \gamma_n(t), \quad t \in [0,1]$$

непрекидна слика сегмента $[0,1]$ која прекрива цео уочени квадрат.

Овако добијени објекат, не одговара нашој интуитивној представи о кривој. △

2.2 Разни начини задавања криве

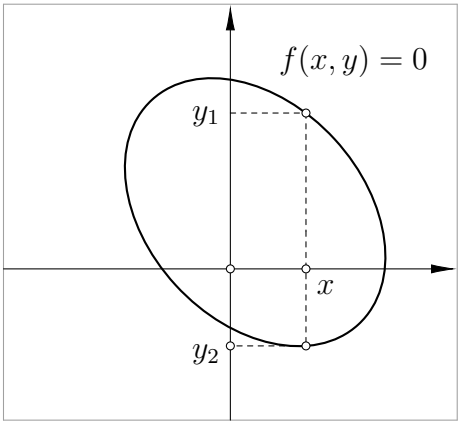
У различитим деловима математике крива има различито значење, у зависности од циљева и метода изучавања.

• Крива као скуп тачака

Једна од интуитивних представа о кривој потиче из геометрије. Тада криву посматрамо као *линију*, то јест као геометријски објекат. У овом случају, под кривом подразумевамо *скуп тачака* (x, y) у равни са одређеним својствима. Задајемо је *имплицитно*[4)] као скуп решења неке једначине

$$f(x, y) = 0. \tag{2.1}$$

Овакав начин задавања криве се веома често употребљава. Проучавање таквих кривих доводи нас до нетривијалних математичких проблема и даје нам могућност геометријског погледа на проблеме из других области математике.



У случају да је једначина (2.1) алгебарска, говоримо о *алгебарској кривој*, а ако је једначина (2.1) трансцендентна[5)] говоримо о *трансцендентној кривој*. Алгебарске криве су неопходне за разумевање *теорије струна*[6)], док трансцендентне криве примењујемо у *кинематици*.

[4)] Реч *имплицитан* потиче од латинске речи *implicare* што у преводу значи *онај који је обухваћен, садржан у нечему, прикривен*. У математичкој терминологији то значи, једноставно речено, *нерешен облик*, јер су и променљива и функција са исте стране знака једнакости.

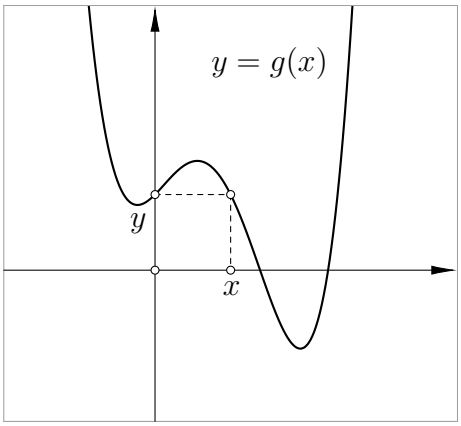
[5)] Реч *трансцендентан* потиче од латинске речи *transscendens* што у преводу значи *прелазити, превазилазити*. У математичкој терминологији има значење *оног који се не може изразити алгебарски*, то јест *чије описивање превазилази моћ алгебре*.

[6)] *Теорија струна* је покушај да се у оквиру *физике честица* помире принципи *опште теорије релативности* и *квантне механике*. По тој теорији, свемир нема 4 димензије – три просторне и четврту димензију време – већ најмање десет просторно-временских димензија. У Теорији струна, суперситне струне су смештене у просторима од 10 до 11 димензија. Такође, уколико се та теорија покаже као исправна, постаће главни кандидат за такозвану «Теорију свега», односно за покушај описивања свих познатих основних сила и стања материје, на коначан математички начин.

Ако је крива график неке фунције g у правоуглом координатном систему, то јест скуп тачака $(x, g(x))$, при чему је x из $\mathcal{D}$, где је $\mathcal{D}$ подскуп од $\mathbb{R}$ домен од g, тада криву можемо задати и *експлицитно*[7)]

$$y = g(x).$$

За разлику од функције, код које једном x одговара тачно једно y, за произвољну криву то не мора да важи. Због тога, криву није увек могуће задати експлицитно.

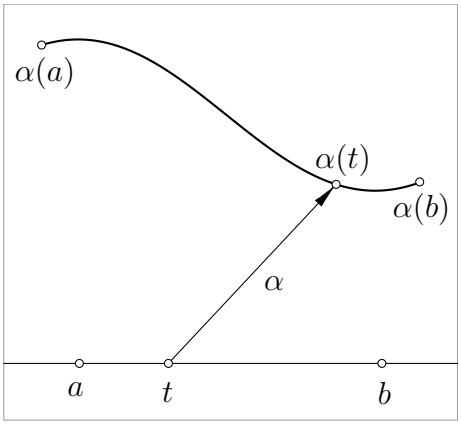


• Параметризована крива

Друга интуитивна представа о кривој потиче из механике. Тада криву посматрамо као *непрекидну путању* или *трајекторију* материјалне тачке у равни, при чему се та тачка креће под дејством неке силе у неком временском интервалу. У овом случају, под кривом подразумевамо *диференцијабилно пресликавање*

$$\alpha : (a, b) = I \to \mathbb{R}^2$$

интервала $I = (a, b)$ реалне праве $\mathbb{R}$ у раван $\mathbb{R}^2$.



[7)] Реч *експлицитан* потиче од новолатинске речи *explicitus* што у преводу значи *онај који је изразит*, *јасан*, *изражен по нечему*, а у математичкој терминологији има значење *решен по y*.

Задајемо је *параметарски*

$$\alpha(t) = (x(t), y(t)),\ t \in I \tag{2.2}$$

помоћу *параметарских једначина*

$$x = x(t) \quad \text{и} \quad y = y(t), \tag{2.3}$$

при чему је t *параметар*[8)] из I. Једначина (2.2) је *векторска параметарска једначина* и називамо је *параметризација криве*, а једначине (2.3) су *координатне параметарске једначине* и оне чине параметризацију криве.

У овом случају говоримо и о *параметризованој кривој*. Свака крива има бесконачно много параметризација, јер се параметар t увек може заменити са неким другим параметром $s = h(t)$, где је h неко бијективно пресликавање.

Дакле, овде смо криву дефинисали као диференцијабилно пресликавање α, а не као скуп тачака. Слику тог пресликавања, то јест скуп

$$\Gamma = \alpha(I) = \left\{c \in \mathbb{R}^2 \mid (\exists t \in I)\, \alpha(t) = c\right\} \subseteq \mathbb{R}^2$$

називамо *траг* или *носач*[10)] *параметризоване криве* α.

Често, уколико то не доводи до забуне, под кривом подразумевамо сам скуп Γ. Називамо га *непараметризована крива* у $\mathbb{R}^2$ и тада је $\alpha(t)$ једна њена параметризација или параметарски облик самог скупа Γ.

На основу (2.2) закључујемо да је свака тачка на кривој одређена једним параметром, то јест има *један степен слободе*, па за криву кажемо и да је *једнопараметарски скуп тачака*.

Задавање кривих помоћу параметара је нарочито погодно за цртање кривих, то јест њихову апроксимацију полигонским линијама, као и за опис кретања објеката дуж криве.

Пример 2.2. Круг са центром у тачки $O(0,0)$ и полупречником $r = 1$ је једна крива у равни. Њен имплицитни облик је

$$f(x, y) = x^2 + y^2 - 1 = 0.$$

Овом једначином није дефинисана функција јер за једно x имамо два решења за y. Међутим, горњу половину круга можемо изразити у експлицитном облику

$$y = g(x) = \sqrt{1 - x^2},$$

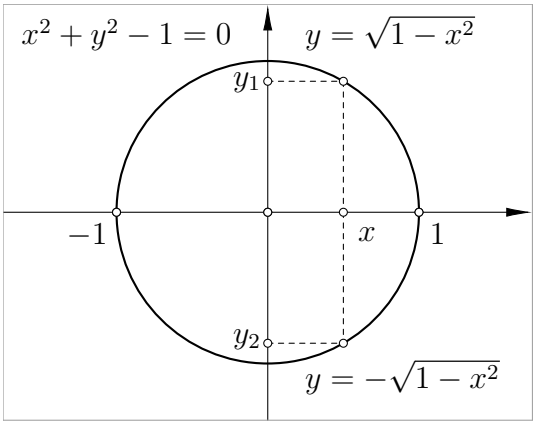
а доњу половину у облику

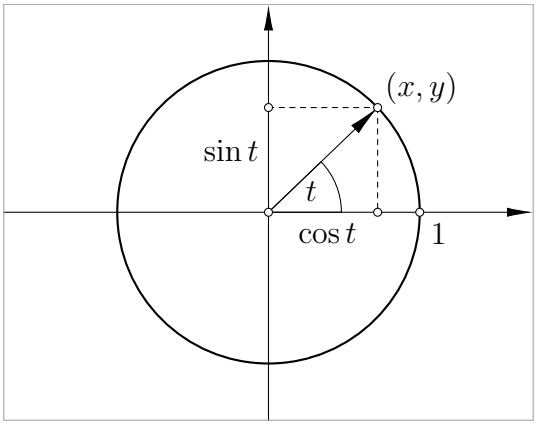
$$y = -g(x) = -\sqrt{1 - x^2}.$$

[8)] *Параметар*[9)] је променљива величина у математичким релацијама која има, у датим условима, константну вредност, и одређује међусобну зависност осталих променљивих величина.

[9)] Реч *параметар* потиче од грчке речи $\pi\alpha\rho\alpha\mu\varepsilon\tau\rho\sigma\nu$ што у преводу значи *мера*, *мерило*, *онај који одмерава*, *процењује*.

[10)] Отуда и ознака $\operatorname{supp}\alpha$ за скуп $\alpha(I)$ од енглеске речи *support* – *подршка*, *наслон*.





Једна од параметризација овог круга је

$$\alpha(t) = (\cos t, \sin t),$$

где је t угао између позитивног дела x-осе и вектора (x, y) и називамо је *параметризација круга централним углом*. Параметарске једначине

$$x = \cos t \quad \text{и} \quad y = \sin t, \ t \in [0, 2\pi)$$

овог круга представљају једно *кружно кретање са константном угаоном брзином*. Наиме, ако је t време изражено у секундама, тада је та угаона брзина *један круг за* 2π *секунди* или *радијан по секунди* ($\frac{\text{rad}}{\text{s}}$). △

У даљем излагању, ми ћемо криву посматрати као линију у равни, то јест као геометријски објекат, односно као скуп тачака у равни са одређеним својствима.

3
Алгебарске криве

Видели смо да су елиптичке криве посебна врста алгебарских кривих. Зато ово поглавље посвећујемо алгебарским кривама. Опширније у [12], [18] и [27].

Према [4], *алгебарске криве* су, сликовито речено, математички објекти који настају тамо где се састају *геометрија* и *полиноми*. Назив алгебарска крива потиче отуда што су алгебарске криве одређене или задате *алгебарским једначинама*. Кажемо и да алгебарске једначине описују алгебарске криве.

3.1 Алгебарске криве

Нека је $\mathbb{K}$ произвољно поље. Његово алгебарско затворење означаваћемо са $\overline{\mathbb{K}}$. Надаље, претпоставићемо да је поље $\mathbb{K}$ алгебарски затворено, то јест $\overline{\mathbb{K}} = \mathbb{K}$, и нећемо то посебно истицати.

• Афина алгебарска крива

Најједноставнији облик алгебарске криве је алгебарска крива у афиној равни $\mathbb{A}^2(\mathbb{K}) = \mathbb{K}^2$.

Дефиниција 3.1. *Алгебарска крива у афиној равни* $\mathbb{K}^2$ је скуп $\mathcal{C}_f/\mathbb{K}$ свих тачака (x, y) из $\mathbb{K}^2$ таквих да је $f(x, y) = 0$ за неки не-нула полином f из $\mathbb{K}[x, y]$, то јест

$$\mathcal{C}_f/\mathbb{K} = \left\{(x, y) \in \mathbb{K}^2 \mid f(x, y) = 0\right\}.$$

Називамо је и *афина алгебарска раванска крива над пољем* $\mathbb{K}$.

Ако је јасно о ком пољу $\mathbb{K}$ је реч или ако нема потребе то поље истицати, убудуће уместо $\mathcal{C}_f/\mathbb{K}$ писаћемо само $\mathcal{C}_f$. С обзиром да ћемо говорити о алгебарским кривама у равни, надаље нећемо истицати ни придев *раванска*.

Афина алгебарска крива $\mathcal{C}_f$ одговара полиному $f(x, y)$. Кажемо и да је она дефинисана тим полиномом. Степен $d^\circ f$ полинома f је и *степен* или *ред* афине алгебарске криве.

Афина алгебарска крива је одређена или задата алгебарском једначином

$$f(x, y) = 0, \tag{3.1}$$

са две непознате над пољем $\mathbb{K}$, коју, у овом случају, зовемо и *афином једначином*, па пишемо и

$$\mathcal{C}_f : f(x, y) = 0.$$

Кажемо и да је $f(x, y) = 0$ *једначина алгебарске криве у афиним координатама* или да је једначини $f(x, y) = 0$ придружена афина алгебарска крива $\mathcal{C}_f$.

Скуп тачака $\mathcal{C}_f$ се неће разликовати ако посматрамо полиноме који се разликују до на множење константом k различитом од нуле, то јест

$$\mathcal{C}_f = \mathcal{C}_{kf}$$

или ако полином f има и вишеструке факторе у факторизацији. Због тога, на ту константу нећемо обраћати пажњу, и допустићемо да полином f има и вишеструке факторе.

• Пројективна алгебарска крива

Потпунија слика о алгебарским кривама добија се пројективизацијом афине равни $\mathbb{A}^2(\mathbb{K})$, јер афина раван не покрива нашу интуицију. Због тога, алгебарске криве дефинисаћемо и у пројективној равни $\mathbb{P}^2(\mathbb{K})$. У том случају, хомогене координате тачке (x, y) означавамо са $(X : Y : Z)$, и при том важи $x = \frac{X}{Z},\ y = \frac{Y}{Z}$.

Дефиниција 3.2. *Алгебарска крива у пројективној равни* $\mathbb{P}^2(\mathbb{K})$ је скуп $\mathcal{C}_F/\mathbb{K}$ свих тачака $(X : Y : Z)$ из $\mathbb{P}^2(\mathbb{K})$ таквих да је $F(X, Y, Z) = 0$ за неки хомогени полином F из $\mathbb{K}[X, Y, Z]$, то јест

$$\mathcal{C}_F/\mathbb{K} = \left\{(X : Y : Z) \in \mathbb{P}^2(\mathbb{K}) \mid F(X, Y, Z) = 0\right\}.$$

Називамо је и *пројективна алгебарска раванска крива над пољем* $\mathbb{K}$.

Из истих разлога као и код афине алгебарске криве, уместо $\mathcal{C}_F/\mathbb{K}$ писаћемо само $\mathcal{C}_F$, и нећемо истицати придев *раванска*.

Пројективна алгебарска крива одговара полиному $F(X, Y, Z)$. Кажемо и да је она дефинисана тим полиномом. Степен $d^\circ F$ полинома F је и *степен* или *ред* пројективне алгебарске криве.

Пројективна алгебарска крива је одређена или задата алгебарском једначином

$$F(X, Y, Z) = 0, \tag{3.2}$$

са три непознате над пољем $\mathbb{K}$, коју, у овом случају, зовемо и *пројективном једначином*, па пишемо и

$$\mathcal{C}_F : F(X, Y, Z) = 0.$$

Кажемо и да је $F(X, Y, Z) = 0$ *једначина алгебарске криве у хомогеним координатама* или да је једначини $F(X, Y, Z) = 0$ придружена пројективна алгебарска крива $\mathcal{C}_F$.

Слично као и у афином случају је

$$\mathcal{C}_F = \mathcal{C}_{\lambda F},$$

па на константе λ различите од нуле нећемо обраћати пажњу, и допустићмо да полином F има и вишеструке факторе.

• Пројективна и афина репрезентација алгебарске криве

Пројективна алгебарска крива, за разлику од афине алгебарске криве, обухвата и бесконачно далеке тачке. Добијамо их заменом $Z = 0$ у једначину (3.2), то јест решавајући једначину

$$F(X, Y, 0) = 0.$$

Те тачке нам пружају потпунију слику о алгебарским кривама. Процесом *дехомогенизације*, то јест замењујући $Z = 1$ у (3.2) добијамо да је афини део алгебарске криве у пројективној равни $\mathbb{P}^2(\mathbb{K})$ дат једначином

$$F(X, Y, 1) = 0.$$

С друге стране, процесом *хомогенизације*, то јест преласком на хомогене координате, односно замењујући $x = \frac{X}{Z}$ и $y = \frac{Y}{Z}$ у (3.1), добијамо да је

$$f(x, y) = f\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \frac{1}{Z^d} F(X, Y, Z),$$

при чему је $d = d^\circ f$. То значи да алгебарској кривој у афиној равни $\mathbb{A}^2(\mathbb{K})$ можемо природно придружити криву

$$F(X, Y, Z) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right), \quad d = d^\circ f \tag{3.3}$$

у пројективној равни $\mathbb{P}^2(\mathbb{K})$. Стављајући да је $Z = 1$ у $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ и (3.3), добијамо да је $x = X$, $y = Y$, и $F(X, Y, 1) = 1^d f(X, Y) = f(X, Y)$, то јест

$$F(x, y, 1) = f(x, y).$$

Одавде закључујемо да су полиноми $F(X, Y, Z)$ и $f(x, y)$ истог степена, то јест $d^\circ F = d^\circ f$.

Због тога, свеједно је да ли смо алгебарску криву задали пројективном или афином једначином.

Другим речима, *пројективна и афина репрезентација алгебарске криве* су потпуно еквивалентне, и лако се прелази са једне на другу. То је и разлог због којег убудуће нећемо увек истицати да ли је нека алгебарска крива афина или пројективна. У том случају рећи ћемо само *алгебарска крива* и претпоставићемо да је она задата неком једначином, афином $f(x, y) = 0$ или пројективном $F(X, Y, Z) = 0$.

Алгебарску криву означаваћемо са $\mathcal{C}/\mathbb{K}$ или $\mathcal{C}$ уколико није потребно истицати поље $\mathbb{K}$ над којим је она дефинисана.

• $\mathbb{L}$-рационална тачка алгебарске криве

Нека је $\mathcal{C}/\mathbb{K} : f(x, y) = 0$ алгебарска крива и $\mathbb{L} \geq \mathbb{K}$ неко раширење поља $\mathbb{K}$.

Дефиниција 3.3. Тачку алгебарске криве $\mathcal{C}/\mathbb{K}$ чије су обе координате из $\mathbb{L}$ називамо $\mathbb{L}$-рационалном тачком те криве.

Скуп свих $\mathbb{L}$-рационалних тачака алгебарске криве $\mathcal{C}/\mathbb{K}$ означавамо са $\mathcal{C}(\mathbb{L})$, то јест

$$\mathcal{C}(\mathbb{L}) = \left\{(x, y) \in \mathbb{L}^2 \mid f(x, y) = 0\right\}.$$

Уместо $\mathbb{L}$-рационална тачка често кажемо краће $\mathbb{L}$-тачка.

Ако је $\mathbb{L} = \mathbb{Z}$, односно $\mathbb{L} = \mathbb{Q}$, говоримо о целобројним или $\mathbb{Z}$-тачкама, односно о рационалним или $\mathbb{Q}$-тачкама алгебарске криве $\mathcal{C}/\mathbb{K}$. Проналажењем тих тачака и изучавањем њихове структуре бави се *артиметика алгебарских кривих*.

За $\mathbb{L} = \mathbb{C}$ говоримо о комплексним или $\mathbb{C}$-тачкама алгебарске криве $\mathcal{C}/\mathbb{K}$, и њиховим проучавањем се бави *геометрија алгебарских кривих*.

3.2 Алгебарске криве над пољем $\mathbb{C}$

• Реална алгебарска крива

Алгебарску криву над пољем $\mathbb{R}$ реалних бројева називамо реална алгебарска крива. Прецизније,

Дефиниција 3.4. Алгебарска крива која одговара не-нула полиному f из $\mathbb{R}[x, y]$ са реалним коефицијентима је скуп $\mathcal{C}/\mathbb{R}$ свих тачака (x, y) из $\mathbb{R}^2$ таквих да је $f(x, y) = 0$, то јест

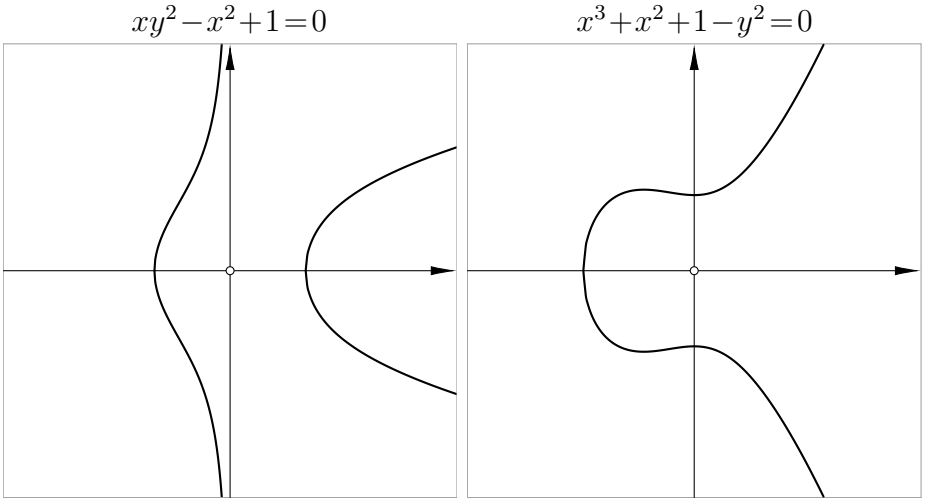
$$\mathcal{C}/\mathbb{R} = \left\{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\right\}.$$

Називамо је *реална алгебарска крива*.

Уколико је јасно да говоримо о реалној алгебарској кривој уместо $\mathcal{C}/\mathbb{R}$ писаћемо само $\mathcal{C}$.

Реалне алгебарске криве су биле познате још старим Грцима. Они нису знали за њихове једначине, него су их проучавали као скупове тачака са неким специфичним својствима. Једначине су се појавиле много касније, крајем XVII века, када је Декарт[1)], увођењем координатног система, спојио алгебру и геометрију и тако далекосежно повезао визуелно и апстрактно.

На следећем цртежу приказани су графици неких реалних алгебарских кривих.



• Алгебарска функција

Нека је $\mathcal{C}$ реална алгебарска крива задата једначином $f(x,y)=0$. За практично проучавање таквих кривих, корисно је ту једначину написати у облику $y=g(x)$, то јест експлицитно изразити y као неку функцију од x. Овај поступак није увек једноставан, често је и немогућ, осим када је једначина $f(x,y)=0$ линеарна или квадратна.

Другим речима, најчешће не постоји елементарна функција $y=g(x)$ помоћу које се може изразити веза $f(x,y)=0$, то јест за коју је

$$f(x,g(x))=0.$$

Када је могуће извести описани поступак, говори нам следећа теорема.

Теорема 3.1. Нека је (x_0,y_0) тачка на алгебарској кривој $\mathcal{C}/\mathbb{R}: f(x,y)=0$. Ако је $\frac{\partial f}{\partial y}(x_0,y_0)\neq 0$, тада постоји једнозначно одређена функција $y=g(x)$ дефинисана у довољно малој околини броја x_0 која има следеће особине:

1° $f(x,g(x))=0$,

2° $g(x_0)=y_0$. □

[1)] Рене Декарт (René Descartes, 1596–1650), француски филозоф и математичар

Ова теорема је специјалан случај *теореме о имплицитној функцији*, [1, страна 68].

Функцију $y = g(x)$[2)] о којој је реч у теореми (3.1) зовемо алгебарском функцијом. Прецизније,

Дефиниција 3.5. Функцију $y = g(x)$ такву да је $f(x, y) = 0$, то јест

$$f(x, g(x)) = 0,$$

за неки полином f из $\mathbb{R}[x, y]$, називамо *алгебарском функцијом.*

За алгебарску функцију $y = g(x)$ добијену описаним поступком кажемо и да је алгебарска функција коју смо *придружили* алгебарској кривој $\mathcal{C}$.

Уместо $y = g(x)$ је алгебарска функција, кажемо и да је y алгебарска функција од x, имајући на уму све претходно речено.

Чланове полинома f из претходне дефиниције можемо груписати по степенима неодређене y, па полином f често изражавамо у облику

$$p_n(x)y^n + p_{n-1}(x)y^{n-1} + \cdots + p_0(x) = 0,$$

при чему су $p_n, \ldots, p_0$ полиноми из $\mathbb{R}[x]$ и $p_n \neq 0$. Степен n полинома f по y је и *степен алгебарске функције* $y = g(x)$.

Алгебарску функцију која је написана у облику разломка $\frac{P(x)}{Q(x)}$, при чему су P и Q полиноми из $\mathbb{R}[x]$ и $Q \neq 0$, називамо *рационалном функцијом* од x. Другим речима, рационална функција промењиве x је алгебарска функција облика

$$y = \frac{a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0}{b_m x^m + \cdots + b_2 x^2 + b_1 x + b_0}, \tag{3.4}$$

при чему су n и m цели ненегативни бројеви, а a_i за $i = 0, \ldots, n$ и b_j за $j = 0, \ldots, m$ из $\mathbb{R}$ такви да је $a_n, b_m \neq 0$ и $(b_m, \ldots, b_0) \neq (0, \ldots, 0)$.

За $m = 0$, рационална функција (3.4) постаје

$$y = c_n x^n + \cdots + c_2 x^2 + c_1 x + c_0,$$

при чему је $c_k = \frac{a_k}{b_0}$ за $k = 1, \ldots, n$. Тада говоримо о *целој рационалној функцији* или *полиномној функцији.* Специјално, $y = c$ је *константна функција*, $y = ax + b$ *линеарна функција*, а $y = ax^2 + bx + c$ *квадратна фукција.*

Ако је $n = m = 1$, тада рационалну функцију називамо *билинеарном*[3)] *функцијом*, и она је облика

$$y = \frac{ax + b}{cx + d},$$

при чему је $(c, d) \neq (0, 0)$.

[2)] Прецизније би било рећи *функција g дефинисана са $y = g(x)$*, али ћемо и убудуће врло често користи овакав краћи начин изражавања.

[3)] Префикс *би-* потиче од латинске речи *bis* што у преводу значи *двапут.* Овај префикс налазимо у сложеницама којим се означава да се нешто јавља *двапут*, да је *удвојено*, *двоструко.*

• Комплексна алгебарска крива

Проучавањем реалних алгебарских кривих могу се јавити разни проблеми који су последица алгебарске незатворености поља $\mathbb{R}$. Такве проблеме решавамо *комплексификацијом* – проучавањем алгебарских кривих над пољем $\mathbb{C}$, то јест смештањем реалног афиног или пројективног простора над којим посматрамо алгебарске криве у одговарајући комплексни афини или пројективни простор. Комплексификација, уз пројективизацију, нам омогућава да потпуно схватимо алгебарске криве. Због тога ћемо дефинисати алгебарске криве над пољем $\mathbb{C}$. Прво ћемо дефинисати алгебарску криву у комплексној равни $\mathbb{C}^2$.

Дефиниција 3.6. Алгебарска крива која одговара не-нула полиному f из $\mathbb{C}[x, y]$ са комплексним коефицијентима је скуп $\mathcal{C}/\mathbb{C}$ свих тачака (x, y) из $\mathbb{C}^2$ таквих да је $f(x, y) = 0$, то јест

$$\mathcal{C}/\mathbb{C} = \left\{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\right\}.$$

Називамо је *алгебарска крива у комплексној равни.*

Уколико је јасно да говоримо о алгебарској кривој у комплексној равни уместо $\mathcal{C}/\mathbb{C}$ писаћемо само $\mathcal{C}$.

Реалне алгебарске криве се много боље «понашају» ако их посматрамо над комплексном равни $\mathbb{C}^2$, то јест потпунију слику о њима добијамо тако што их сместимо у $\mathbb{C}^2$.

Пример 3.1. Алгебарска крива $\mathcal{C}_1/\mathbb{R} : x^2 + y^2 = 0$ у реалној равни $\mathbb{R}^2$ је тачка $(0, 0)$, а иста та крива $\mathcal{C}_1/\mathbb{C} : x^2 + y^2 = 0$ посматрана у комплексној равни $\mathbb{C}^2$ представља пар комплексних правих које се секу.

Алгебарска крива $\mathcal{C}_2/\mathbb{R} : x^2 + y^2 = -1$ представља празан скуп у реалној равни $\mathbb{R}^2$, а иста та крива $\mathcal{C}_2/\mathbb{C} : x^2 + y^2 = -1$ посматрана у комплексној равни $\mathbb{C}^2$ је комплексна кружница. △

Две алгебарске криве могу представљати исти геометријски скуп тачака

$$\mathcal{C}/\mathbb{C} = \left\{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\right\} = \left\{(x, y) \in \mathbb{C}^2 \mid g(x, y) = 0\right\}.$$

У ком случају је то могуће, говори нам следећа теорема, [4, страна 6].

Теорема 3.2. Нека су f и g полиноми из $\mathbb{C}[x, y]$. Тада они одређују исту алгебарску криву у $\mathbb{C}^2$ ако и само ако имају исте нерастављиве факторе, то јест ако и само ако постоје природни бројеви m и n такви да

$$f \mid g^m \text{ и } g \mid f^n. \qquad \square$$

Теорема (3.2) је специјалан случај теореме познате као Хилбертов Нулштелензац[4)] – теореме која успоставља фундаментални однос између геометрије

[4)] Нулштелензац је немачка реч *Nullstellensatz* што у преводу значи *Теорема нула.*

и алгебре. Тај однос је основа алгебарске геометрије. Из [4, страна 7] важи и

Последица 3.1. Нека су f и g полиноми из $\mathbb{C}[x,y]$ који немају квадратне факторе[5]. Тада они одређују исту алгебарску криву у $\mathbb{C}^2$ ако и само ако су скаларни множиоци један другог, то јест за неко $\lambda \in \mathbb{C}\backslash\{0\}$ је

$$f = \lambda g. \qquad \square$$

Алгебарска крива реда d и права у $\mathbb{C}^2$ у општем случају имају d пресечних тачака, рачунајући вишеструкости. Природно је извршити комплетирање односно компактификацију алгебарске криве у пројективној равни, где ће она имати тачно d пресечних тачака са сваком правом. У том случају, «недостајуће» тачке из $\mathbb{C}^2$ ће се налазити на бесконачно далекој правој. Због тога, сада ћемо дефинисати и алгебарску криву у комплексној пројективној равни $\mathbb{P}^2(\mathbb{C})$.

Дефиниција 3.7. Алгебарска крива која одговара хомогеном полиному F из $\mathbb{C}[X,Y,Z]$ са комплексним коефицијентима је скуп $\overline{\mathcal{C}}/\mathbb{C}$ свих тачака $(X:Y:Z)$ из $\mathbb{P}^2(\mathbb{C})$ таквих да је $F(X,Y,Z)=0$, то јест

$$\overline{\mathcal{C}}/\mathbb{C} = \left\{(X:Y:Z) \in \mathbb{P}^2(\mathbb{C}) \mid F(X,Y,Z)=0\right\}.$$

Називамо је *алгебарска крива у комплексној пројективној равни.*

Уколико је јасно да говоримо о алгебарској кривој у комплексној пројективној равни уместо $\overline{\mathcal{C}}/\mathbb{C}$ писаћемо само $\overline{\mathcal{C}}$.

За алгебарску криву $\overline{\mathcal{C}}/\mathbb{C}$ кажемо и да је *пројективизација* алгебарске криве $\mathcal{C}/\mathbb{C}$. Та пројективизација се може посматрати и као компактификација алгебарске криве $\mathcal{C}/\mathbb{C}$ бесконачно далеким тачкама.

Граф алгебарске криве $\overline{\mathcal{C}}/\mathbb{C}$ тополошки је једна површ. Можемо је видети као реалну дводимензионалну површ у четвородимензионалном простору[6]. Штавише, та површ је компактна, глатка и повезана. Из топологије нам је познато да је свака таква површ хомеоморфна[7] сфери са коначним бројем «ручки», то јест она је или сфера или торус са n рупа, при чему је n из $\mathbb{N}$.

Дакле, алгебарске криве у $\mathbb{P}^2(\mathbb{C})$ имају облик сфере или торуса са n рупа, па их можемо проучавати и са становишта топологије.

[5] то јест не постоје полиноми u и v такви да $u^2 \mid f$ и $v^2 \mid g$

[6] Комплексни пројективни простор $\mathbb{P}^n(\mathbb{C})$ има реалну димензију $2n$, то јест дупло већу него одговарајући реални $\mathbb{P}^n(\mathbb{R})$. Због тога, $\mathbb{P}^2(\mathbb{C})$ има реалну димензију $2 \cdot 2 = 4$.

[7] то јест тополошки еквивалентна, односно у тополошком смислу их не разликујемо

Алгебарска крива $\overline{\mathcal{C}}/\mathbb{C}$ у $\mathbb{P}^2(\mathbb{C})$ је ограничен и затворен, то јест компактан скуп. На таквим скуповима је могуће дефинисати холоморфне[8)] и мероморфне[9)] функције, па се алгебарске криве у $\mathbb{P}^2(\mathbb{C})$ могу проучавати и са становишта комплексне анализе.

Алгебарске криве у $\mathbb{C}^2$ и алгебарске криве у $\mathbb{P}^2(\mathbb{C})$, уколико то не доводи до забуне, звaћемо једним именом – *комплексне алгебарске криве* или *алгебарске криве над пољем* $\mathbb{C}$.

Комплексне алгебарске криве су почеле да се проучавају тек хиљаду година након почетка проучавања реалних алгебарских кривих. Одмах је постало јасно да су комплексне алгебарске криве и једноставније и интересантније за проучавање од реалних алгебарских кривих. Тако је, на пример, много лакше полином са реалним коефицијентима – *реалан полином* – посматрати као полином са комплексним коефицијентима – *комплексан полином* – јер, према *основној теореми алгебре*, сваки комплексан полином степена већег од један је растављив над пољем $\mathbb{C}$, то јест има бар једну нулу у $\mathbb{C}$.

3.3 Сингуларне тачке алгебарских кривих

Особине алгебарских кривих, као и њихови различити облици, заинтересовали су многе математичаре. Тако је чувени математичар Њутн проучавао њихове сингуларитете[10)]. То су тачке у којима, сликовито речено, крива одступа од свог *стандардног облика*. Кажемо и да алгебарска крива у тим тачкама изгледа *деформисано* или *дегенерисано*[11)], то јест не изгледа «глатко».

• Сингуларна тачка. Врсте сингуларитета

Дефиниција 3.8. Тачка (x_0, y_0) на алгебарској кривој задатој полиномом $f(x, y)$ је *сингуларна* или један *сингуларитет* ако је

$$\frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0.$$

У супротном, за (x_0, y_0) кажемо да је *несингуларна*, *регуларна* или *обична тачка*.

[8)] Комплексна функција $f : \Omega \to \mathbb{C}$ је *холоморфна* на отвореном подскупу Ω комплексне равни $\mathbb{C}$ ако је она диференцијабилна у свакој тачки $z_0 \in \Omega$.

[9)] Холоморфна функција $f : \Omega \to \mathbb{C}$ је *мероморфна* на отвореном скупу Ω комплексне равни $\mathbb{C}$ ако она на том скупу нема других сингуларитета изузев полова, то јест тачака $a \in \mathbb{C}$ таквих да је $\lim\limits_{z \to a} f(z) = \infty$.

[10)] Реч *сингуларан* потиче од новолатинске речи *singularitas* што у преводу значи *посебност*, *појединачност*, *чудноватост*.

[11)] Реч *дегенерисан* потиче од латинске речи *degenerare* што у преводу значи *изрођен*, *изметнут*, *изопачен*. У математичкој терминологији значи *онај који одступа од стандардног облика*.

Ако је бар један од парцијалних извода другог реда

$$f^0_{x^2} = \frac{\partial^2 f}{\partial x^2}(x_0, y_0), \quad f^0_{xy} = \frac{\partial^2 f}{\partial xy}(x_0, y_0), \quad f^0_{y^2}\frac{\partial^2 f}{\partial y^2}(x_0, y_0)$$

различит од нуле, тада можемо да одредимо врсту сингуларне тачке (x_0, y_0) у зависности од знака израза

$$f^0_{x^2} f^0_{y^2} - (f^0_{xy}).$$

Могућа су три случаја:

1° $f^0_{x^2} f^0_{y^2} - (f^0_{xy})^2 < 0$ – тачка (x_0, y_0) је *двострука* или *двојна*,

2° $f^0_{x^2} f^0_{y^2} - (f^0_{xy})^2 > 0$ – тачка (x_0, y_0) је *изолована*,

3° $f^0_{x^2} f^0_{y^2} - (f^0_{xy})^2 = 0$ – за одређивање врсте тачке (x_0, y_0) потребна су додатна испитивања, јер у овом случају посматрана тачка може бити *повратна прве врсте*, *повратна друге врсте*, *изолована* или *тачка самододира*.

Дефиниција 3.9. Тачка $(X_0 : Y_0 : Z_0)$ на алгебарској кривој задатој хомогеним полиномом $F(X, Y, Z)$ је *сингуларна* или један *сингуларитет* ако је

$$\frac{\partial F}{\partial X}(X_0, Y_0, Z_0) = \frac{\partial F}{\partial Y}(X_0, Y_0, Z_0) = \frac{\partial F}{\partial Z}(X_0, Y_0, Z_0) = 0.$$

Према [12, страна 37] важи следећа теорема.

Теорема 3.3. Нека је $F(X, Y, Z)$ хомоген полином, $(X_0 : Y_0 : Z_0)$ тачка са хомогеним координатама и $F(X_0, Y_0, Z_0) = 0$, $Z_0 \neq 0$. Ако је $f(x, y) = F(X, Y, 1)$, тада је систем

$$\frac{\partial F}{\partial X}(X_0, Y_0, Z_0) = \frac{\partial F}{\partial Y}(X_0, Y_0, Z_0) = \frac{\partial F}{\partial Z}(X_0, Y_0, Z_0) = 0$$

еквивалентан са

$$\frac{\partial f}{\partial x}(\frac{X_0}{Z_0}, \frac{Y_0}{Z_0}) = \frac{\partial f}{\partial y}(\frac{X_0}{Z_0}, \frac{Y_0}{Z_0}) = 0. \qquad \square$$

Постоји ефективан поступак постепеног уклањања сингуларитета равне алгебарске криве. Називамо га *десингуларизација криве*.

Изучавањем сингуларитета алгебарских кривих бави се посебна област математике – *теорија сингуларитета*.

• Несводљива алгебарска крива

Дефиниција 3.10. Алгебарска крива је *иредуцибилна* или *несводљива* ако је полином којим је она дефинисана нерастављив.

Алгебарске криве дефинисане растављивим полиномима могу се представити као унија неколико несводљивих кривих. Због тога се у многим случајевима проучавање алгебарских кривих може ограничити само на проучавање несводљивих кривих.

Према [12, страна 35], можемо показати да несводљива алгебарска крива има само коначно много сингуларних тачака.

• Глатка алгебарска крива

Дефиниција 3.11. Алгебарска крива је *глатка* или *несингуларна* ако је глатка у свакој својој тачки, то јест ако је свака њена тачка регуларна. У супротном кажемо да је алгебарска крива *сингуларна*.

Глатка алгебарска крива има дефинисану тангенту у свакој својој тачки.

3.4 Ред алгебарске криве

Да бисмо детаљније упознали алгебарске криве, морамо их класификовати. То значи да морамо описати све могуће скупове тачака који задовољавају једначину којом је задата алгебарска крива.

Најприроднија, и историјски најранија, класификација алгебарских кривих је према степену или реду алгебарске криве. Као што знамо, *степен* или *ред алгебарске криве* је степен полинома којим је она дефинисана.

Овде ћемо дати кратак преглед неких алгебарских кривих, посматрајући их у афиној равни $\mathbb{R}^2$.

• Права

Најједноставнија алгебарска крива је крива првог реда.

Дефиниција 3.12. Алгебарску криву првог реда називамо *права*[12)].

Дакле, нејједноставнија алгебарска крива је права. Свака права је задата једначином $f(x, y) = 0$, при чему је f из $\mathbb{R}[x, y]$ полином првог степена по неодређенима x и y. Прецизније, свака права је задата линеарном једначином

$$ax + by + c = 0,$$

са две непознате x и y, где су a, b и c реалне константе за које важи да је $(a, b) \neq (0, 0)$.

[12)] Права се у свакодневном говору користи као придев у женском роду: права шипка, права стрела. У геометрији реч *права* је назив геометријског објекта, па је она именица женског рода, а не придев. Али се по падежима мења као придев: на *правој*, ван *праве*.

• Квадрика и коника

После правих, први примери алгебарских кривих су криве другог реда.

Дефиниција 3.13. Алгебарску криву другог реда називамо *квадрика*.

Од античких времена квадрике су познате и као *конусни пресеци*. Оне су довољно једноставне да се већина њихових особина може проучити елементарним средствима, па ипак омогућавају развој интересантних структура које представљају изазов и за савремене математичке технике.

Свака квадрика је одређена једначином $f(x, y) = 0$, при чему је f из $\mathbb{R}[x, y]$ полином другог степена по неодређенима x и y. Прецизније, свака квадрика је одређена квадратном једначином

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0, \tag{3.5}$$

са две непознате x и y, где су a, b, c, d, e и f реалне константе за које важи да је $(a, b, c) \neq (0, 0, 0)$.

Квадрика над пољем $\mathbb{R}$ може бити:

- *Елипса.* Погодним одабиром координатног система, једначину (3.5) можемо да напишемо у облику

  $$\beta^2 x^2 + \alpha^2 y^2 = \beta^2 \alpha^2 \quad \text{или} \quad \frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1.$$

  Називамо је *канонска* или *сведена* једначина елипсе.
- *Хипербола.* Канонска једначина хиперболе је

  $$\beta^2 x^2 - \alpha^2 y^2 = \beta^2 \alpha^2 \quad \text{или} \quad \frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 1.$$

- *Парабола.* Канонска једначина параболе је

  $$y = 2px^2, \qquad p \neq 0.$$

  Број p називамо *параметар параболе*.
- *Празан скуп.* На пример, $x^2 + y^2 + 1 = 0$.
- *Тачка.* На пример, $x^2 + y^2 = 0$.
- *Унија две праве.* Ово се дешава када је полином на левој страни једначине (3.5) растављив у производ два линеарна полинома:

  $$(a_1 x + b_1 y + c_1)(a_2 x + b_2 y + c_2) = 0.$$

  Овде се могу разликовати три подслучаја: те две праве могу да се поклапају, могу бити дисјунктне и могу се сећи у једној тачки.

Дефиниција 3.14. Елипсу, хиперболу и параболу називамо *коникама*, а празан скуп, тачку и унију две праве *дегенерисаним коникама*.

Не постоје квадрике које нису ни конике ни дегенерисане конике, што потврђује следећа теорема, [6, страна 57].

Теорема 3.4. Квадрика је или коника или дегенерисана коника. □

• Кубна крива или кубика. Елиптичка крива

Важна класа алгебарских кривих су алгебарске криве трећег реда.

Дефиниција 3.15. Алгебарску криву трећег реда називамо *кубна крива* или *кубика*.

Свака кубика је одређена једначином $f(x, y) = 0$, при чему је f из $\mathbb{R}[x, y]$ полином трећег степена по неодређенима x и y. Прецизније, свака кубика је одређена кубном једначином

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3 + 3ex^2 + 6fxy + 3gy^2 + 3hx + 3iy + j = 0,$$

са две непознате x и y где су a, b, c, d, e, f, g, h, i и j реалне константе за које важи да је $(a, b, c, d) \neq (0, 0, 0, 0)$.

Први покушај класификације кубних кривих дао је Њутн 1704. године у додатку своје *Оптике*.[13)] Он је описао 72 могућа случаја кубних кривих, и тиме поставио основу њиховог систематског проучавања. Уколико кубну криву посматрамо у пројективном простору, многе од ових 72 криве постају еквивалентне једна другој.

Посебно место у Њутновој класификацији кубика чине дивергентне[14)] параболе[15)].

Дефиниција 3.16. Кубну криву задату једначином облика

$$y^2 = f(x),$$

при чему је f из $\mathbb{R}[x]$ полином трећег степена по неодређеној x називамо *дивергентна парабола*.

Прецизније, дивергентна парабола је свака кубна крива задата једначином

$$y^2 = ax^3 + bx^2 + cx + d,$$

са две непознате x и y где су a, b, c и d реалне константе.

[13)] Isac Newton, *Enumeratio linearum tertii ordinis*

[14)] Реч *дивергентан* потиче од латинске речи *divergens* што у преводу значи *разилажење, одступање, оно што иде у различитим правцима или што се удаљава.*

[15)] на латинском *parabolae divergentes*

Постоје две специјалне поткласе дивергентних парабола: Њутнове дивергентне параболе и елиптичке криве.

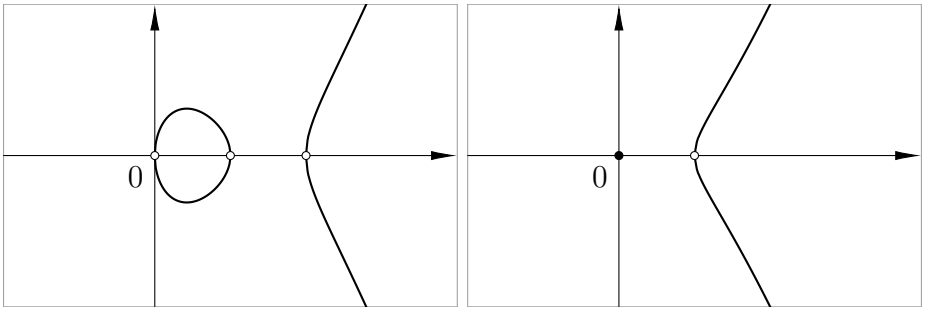
Дефиниција 3.17. Дивергентну параболу задату једначином

$$y^2 = x^3 + ax^2 + bx \tag{3.6}$$

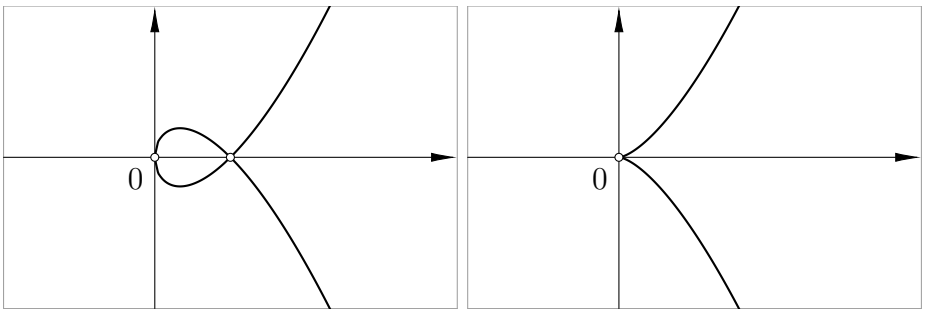
са две непознате x и y где су a и b реалне константе називамо *Њутнова дивергентна парабола.*

Њутнове дивергентне параболе можемо поделити на следеће врсте, зависно од корена полинома на десној страни једначине (3.6):

- сви корени су реални и различити. Крива се састоји од две компоненте – једног овала и неограниченог дела (приказана је на наредном цртежу лево);
- сви корени су реални, два мања су међусобно једнака. Крива се састоји од тачке и неограниченог дела (приказана је на наредном цртежу десно);

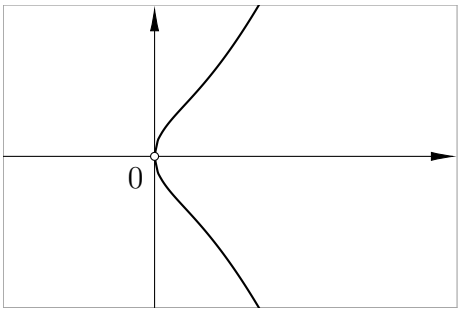


- сви корени су реални, два већа су међусобно једнака. Крива има тачку самопресека[16]. Позната је и као *алфа-крива* (приказана је на наредном цртежу лево);
- сви корени су реални и једнаки, једначина је $y^2 = x^3$. Ова крива, позната као *полукубна парабола*[17], се састоји из два глатка дела симетрична у односу на $x-$осу и има касп[19]у координатном почетку у коме се ти делови састају (приказана је на наредном цртежу десно);



[16] кажемо и чвор
[17] или *Нилова*[18] *парабола*
[18] Виљем Нил (William Neil, 1637–1670), енглески и математичар
[19] кажемо и шпиц, односно врх

- један корен је реалан, а два су конјуговано комплексна. Крива има само једну компоненту – глатку, звонастог облика.



Дефиниција 3.18. Дивергентну параболу задату једначином

$$y^2 = x^3 + ax + b,$$

са две непознате x и y где су a и b реалне константе називамо *елиптичка крива*.

Осим Њутнове класификације кубних кривих, постоји и она коју је предложио Пликер[20], а која се базира на особинама бесконачно далеких тачака кубних кривих.

Кубне криве су веома значајне за модерну математику. Читава теорија *елиптичких функција* и *елиптичких интеграла* заснована је на својствима ових кривих. Многи централни резултати анализе и геометрије везани су за кубне криве.

• Крива четвртог реда или квартика. Хиперелиптичка крива

Дефиниција 3.19. Алгебарску криву четвртог степена или четвртог реда називамо *квартика*.

Свака квартика је одређена једначином $f(x, y) = 0$, при чему је f из $\mathbb{R}[x, y]$ полином четвртог степена по неодређенима x и y. Прецизније, свака квартика је одређена једначином четвртог степена

$$\begin{aligned} ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4 + 4fx^3 + 12gx^2y + 12hxy^2 \\ + 4iy^3 + 6jx^2 + 12kxy + 6ly^2 + 4mx + 4ny + o = 0, \end{aligned}$$

са две непознате x и y где су a, b, c, d, e, f, g, h, i, j, k, l, m, n и o реалне константе за које важи да је $(a, b, c, d, e) \neq (0, 0, 0, 0, 0)$.

Генерализацијом елиптичких кривих долазимо до још једне важне класе алгебарских кривих.

[20] Јулијус Пликер (Julius Plücker, 1801–1868), немамчки математичар

Дефиниција 3.20. Алгебарску криву задату једначином облика

$$y^2 = f(x)$$

где је f из $\mathbb{K}[x]$ полином степена $d^\circ f > 4$ без вишеструких корена називамо *хиперелиптичка крива*.

Она има много заједничког са класом елиптичких кривих.

3.5 Род алгебарске криве

Класификација алгебарских кривих према степену или реду се испоставила као прилично груба. Лепша класификација алгебарских кривих је на основу рода алгебарске криве – геометријско-тополошке инваријанте[21)] коју можемо придружити свакој алгебарској кривој. Ова класификација је настала у 19. веку од стране Римана[22)] и Абела. Она је најбоља класификација по «компликованости» алгебарских кривих.

Пример 3.2. Алгебарска крива

$$\mathcal{C}_1 : 3x^4y^2 + 5x^2y + 11xy + 23x + 14 = 0,$$

је знатно сложенија од алгебарске криве

$$\mathcal{C}_2 : y - x^8 = 0,$$

иако алгебарска крива $\mathcal{C}_2$ има већи степен од алгебарске криве $\mathcal{C}_1$. △

• Геометријски приступ

Видели смо да алгебарска крива у пројективној комплексној равни $\mathbb{P}^2(\mathbb{C})$ има облик сфере или торуса са n рупа, уз напомену да је у случају сфере $n = 0$.

Дефиниција 3.21. Број рупа n називамо *генус* или *род* алгебарске криве, и означавамо са g.

Важно својство које има род алгебарске криве дат је следећом теоремом, уз напомену да су она и следећа три става формулисани на основу [48, страна 39].

[21)] Реч *инваријантан* потиче од латинских речи *in* – *у* и *variare* – *непромењен*, што у преводу значи *онај који остаје непромењен*. У математици и физици представља својство појединих математичких објеката и величина која се *не мењају* при неким пресликавањима, односно трансформацијама.

[22)] Георг Фридрих Бернхард Риман (Georg Friedrich Bernhard Riemann, 1826–1866), немачки математичар

Теорема 3.5. За сваки цео број $g \geq 0$ постоји алгебарска крива рода g. □

На основу овог својства можемо извршити класификацију алгебарских кривих према њиховом роду.

Да бисмо геометријски одредили род алгебарске криве $\mathcal{C}$ посматраћемо је као алгебарску криву $\overline{C}/\mathbb{C}$ у пројективној комплексној равни $\mathbb{P}^2(\mathbb{C})$. Род алгебарске криве $\overline{C}/\mathbb{C}$ биће и род алгебарске криве $\mathcal{C}$.

Пример 3.3. Афина права, то јест права има род $g = 0$. Заиста, праву $ax + by + c = 0$ пројективно представљамо као $aX + bY + cZ = 0$, а ово је изоморфно комплексној пројективној правој $\mathbb{P}^1(\mathbb{C})$.

С друге стране, $\mathbb{P}^1(\mathbb{C})$ се састоји од Гаусове равни $\mathbb{C}$ и једне бесконачно далеке тачке којом компактификујемо ту раван, па $\mathbb{P}^1(\mathbb{C})$ можемо видети и као сферу $\mathbb{S}^2$ у $\mathbb{P}^2(\mathbb{C})$, то јест $\mathbb{P}^1(\mathbb{C}) \cong \mathbb{S}^2$. Пошто сфера у себи не садржи рупе, род комплексне пројективне праве $\mathbb{P}^1(\mathbb{C})$, па самим тим и праве је $g = 0$. △

Пример 3.4. Конике такође можемо видети као сфере у $\mathbb{P}^2(\mathbb{C})$, па и оне имају род $g = 0$. △

• Алгебарски приступ

Став 3.1. Нека је $\mathcal{C}$ алгебарска крива реда n. Тада за *генус* или *род* g алгебарске криве $\mathcal{C}$ важи следећа неједнакост

$$g \leq \frac{(n-1)(n-2)}{2}. \qquad \square$$

Ако је алгебарска крива глатка, или ако су њене једине сингуларне тачке двојне, тада род алгебарске криве можемо и експлицитно да изразимо.

Став 3.2. Нека је $\mathcal{C}$ глатка алгебарска крива реда n. Тада за *род* g алгебарске криве $\mathcal{C}$ важи једнакост

$$g = \frac{(n-1)(n-2)}{2}. \ \square \tag{3.7}$$

Једнакост (3.7) је позната као *формула степена*.

Став 3.3. Нека је $\mathcal{C}$ алгебарска крива реда n са d двојних тачака, при чему је $d \geq 0$. Тада за *род* g алгебарске криве $\mathcal{C}$ важи једнакост

$$g = \frac{(n-1)(n-2)}{2} - d. \qquad \square$$

• Рационална крива

На основу дефиниције (3.2) алгебарска крива $\mathcal{C}$ има род $g = 0$, ако је она права или квадрика, то јест криве првог и другог реда су истог рода $g = 0$.

Дефиниција 3.22. Алгебарску криву рода $g = 0$ називамо *рационална крива*.

Назив рационална крива потиче отуда што алгебарска крива рода $g = 0$ има параметризацију помоћу рационалних функција, то јест координате тачака које припадају тој кривој можемо изразити рационалним функцијама неког параметра.

Пример 3.5. Круг $x^2 + y^2 = 1$ као алгебарска крива другог реда има род $g = 0$ и рационалну параметризацију

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}$$

помоћу параметра t из $\mathbb{R}$. △

• Елиптичка и хиперелиптичка крива

На основу става (3.3) алгебарске криве трећег реда – кубне криве – имају род $g = 1$ ако немају двојну тачку, то јест ако су глатке, или род $g = 0$ ако имају једну двојну тачку, то јест ако нису глатке. Због тога, поред дефиниције (3.18), елиптичку криву можемо дефинисати и овако:

Дефиниција 3.23. Алгебарску криву рода $g = 1$ називамо *елиптичка крива*.

Назив елиптичка крива потиче отуда што алгебарска крива рода $g = 1$ има параметризацију помоћу елиптичких функција, о којима ће детаљније бити речи у наредном поглављу.

Дакле, према роду, кубне криве можемо поделити на две класе:

- кубне криве чији је род $g = 0$ – *рационалне криве*;
- кубне криве чији је род $g = 1$ – *елиптичке криве*.

И хиперелиптичку криву, поред дефиниције (3.20), можемо дефинисати и овако:

Дефиниција 3.24. Алгебарску криву рода $g = 2$ називамо *хиперелиптичка крива*.

Уопште, хиперелиптичке криве имају род $g > 1$, уз напомену да су све алгебарске криве рода два хиперелиптичке, али за већи род постоје криве које нису хипереллиптичке. Према [44, страна 18], важи

Став 3.4. Алгебарске криве задате једначином $y^2 = f(x)$, где је f полином степена $d^\circ f \geq 3$ и без вишеструких корена, имају род

$$g = \left\lfloor \frac{n-1}{2} \right\rfloor,$$

то јест g је највећи цео део броја $\frac{n-1}{2}$ не већи од $\frac{n-1}{2}$. □

То посебно значи да, поред случаја када је $n = 3$, и у случају када је $n = 4$ алгебарске криве задате једначином $y^2 = f(x)$ имају род $g = 1$. Штавише, ако је f полином степена $d^\circ f \geq 3$ и без вишеструких корена, тада, ако је:

- $n = 1$ или $n = 2$ алгебарске криве задате једначином $y^2 = f(x)$ имају род $g = 0$;
- $n = 5$ или $n = 6$ алгебарске криве задате једначином $y^2 = f(x)$ имају род $g = 2$.

Дакле, степен $d^\circ f$ полинома f, без вишеструких корена, којим је дефинисана алгебарска крива облика $y^2 = f(x)$ одређује род те криве. Отуда и, на основу [11, страна 254]

Став 3.5. Полином f, без вишеструких корена, степена

$$d^\circ f = 2g + 1 \quad \text{или} \quad d^\circ f = 2g + 2$$

одређује алебарску криву $y^2 = f(x)$ рода g. □

• Род алгебарске криве и Диофантове једначине

Род алгебарске криве има важну улогу код класификације Диофантових једначина, јер свакој Диофантовој једначини можемо придружити неку алгебарску криву. Род придружене алгебарске криве одређује структуру скупа решења саме Диофантове једначине. Прво се подсетимо, [19, страна 129]:

Дефиниција 3.25. *Диофантова* или *диофантска једначина* је једначина облика $f(x_1, \ldots, x_n) = 0$ чија решења тражимо у скупу $\mathbb{Z}^n$, где је n из $\mathbb{N}$ и f нека функција n променљивих.

Функција f из дефиниције (3.25) је најчешће полином са целобројним коефицијентима, то јест $f \in \mathbb{Z}[x_1, \ldots, x_n]$. Тада говоримо о *алгебарским Диофантовим једначинама*. Због тога, када кажемо Диофантова једначина мислимо на алгебарску Диофантову једначину[23)] са две или више непознатих чији су коефицијенти цели бројеви за коју тражимо целобројна или рационална решења. Под Диофантовим једначинама, такође, подразумевамо и системе алгебарских

[23)] Треба имати на уму да нису ретке ни експоненцијалне Диофантове једначине, као и једначине које су задате формулом $g(x_1, \ldots, x_n) = 0$, где је g нека сложена функција.

једначина са целобројним коефицијентима.

Диофантове једначине се најприродније и најуспешније проучавају и решавају методама *алгебарске геометрије*. Део алгебарске геометрије који проучава Диофантове једначине користећи методе из алгебарске теорије бројева је *Аритметичка*[24] [*алгебарска*] *геометрија* или *Диофантова геометрија*.

Године 1887. Рунге[25] почиње да примењује алгебарску геометрију на решавање Диофантових једначина. Он свакој Диофантовој једначини придружи алгебарску криву, и уместо да тражи рационална или целобројна решења Диофантове једначине, он тражи рационалне или целобројне тачке алгебарске криве која је придружена тој једначини. Од рода g придружене алгебарске криве зависи број рационалних, односно целобројних решења те једначине. Ако је:

1° $g = 0$, тада су Диофантове једначине, у принципу, решиве. Може се догодити да она нема ниједно рационално решење, али ако има бар једно, онда их има бесконачно много. У овом случају Диофантова једначина има бесконачно много целобројних решења.

2° $g = 1$, тада су овакви проблеми најбогатији, и математички најзанимљивији. Може се догодити да она нема ниједно рационално решење, да их има коначно много или да их има бесконачно много. Ако има бесконачно много рационалних решења она су коначно генерисана, то јест сва рационална решења се могу добити из коначно много рационалних решења применом одређене операције. У овом случају Диофантова једначина има коначно много целобројних решења.

3° $g > 1$, тада за придружене алгебарске криве кажемо да су *општег тип*а, а Диофантове једначине којима су придружене такве алгебарске криве имају коначно много рационалних, па самим тим и целобројних решења.

• Род алгебарске криве и њене рационалне тачке

Претходно речено у вези са Диофантовим једначинама и њима придруженим алгебарским кривама је пример принципа *геометрија одређује аритметику* јер геометријско својство алгебарске криве – њен род – одређује аритметичко својство те криве – број њених рационалних тачака, односно број рационалних решења придружене Диофантове једначине. Та повезаност рода алгебарске криве са структуром скупа њених рационалних тачака дата је следећом веома важном теоремом, [44, страна 17]:

Теорема 3.6. Скуп $\mathcal{C}(\mathbb{Q})$ рационалних тачака алгебарске криве $\mathcal{C}$ рода g је:

[24] Аритметика је стара реч за теорију бројева

[25] Карл Давид Толме Рунге (Carl David Tolmé Runge, 1856–1927), немачки математичар и физичар

1° празан или бесконачан, ако је $g = 0$,

2° коначан или бесконачан, ако је $g = 1$,

3° коначан, ако је $g > 1$. □

Према теореми (3.6) алгебарска крива $\mathcal{C}$ рода $g = 0$ не мора да има рационалних тачака, то јест може бити $\mathcal{C}(\mathbb{Q}) = \emptyset$ или их има бесконачно много. За овакве криве важи теорема Хасе[26)]-Минковског[27)], [33, страна 5].

Теорема 3.7. [**Хасе-Минковски**] Нека је $\mathcal{C}$ алгебарска крива рода $g = 0$. Тада је $\mathcal{C}(\mathbb{Q}) \neq \emptyset$ ако и само ако је $\mathcal{C}(\mathbb{R}) \neq \emptyset$ и $\mathcal{C}(\mathbb{Q}_p)$[28)] $\neq \emptyset$ за сваки прост број p. □

Ову теорему не можемо примењивати у случају алгебарских кривих рода већег од један. Она је позната и као *локално-глобални принцип*, јер тврди да ће алгебарска крива рода нула имати тачке над $\mathbb{Q}$ – глобално – ако и само има тачке над $\mathbb{Q}_p$ за сваки прост број p и над $\mathbb{R}$ – локално.

Провера да ли алгебарска крива рода $g = 0$ има тачке над $\mathbb{Q}_p$ се може обавити у коначном броју корака јер је довољно проверити да ли једначина којом је она задата има решења по модулу p^k за коначно много p-ова и k-ова, то јест не треба проверавати да ли она има решења за сваки прост број p.

Опет, према теореми (3.6), алгебарска крива $\mathcal{C}/\mathbb{Q}$ рода $g > 1$ има коначно много рационалних тачака. То је формулисао Мордел 1922. године као хипотезу, а доказао Фалтингс[29)] 1983. године, због чега је 1986. године добио *Филдсову*[30)] *медаљу*[31)], [19, страна 283].

Теорема 3.8. [**Фалтингс**] Нека је $\mathcal{C}/\mathbb{Q}$ алгебарска крива рода $g > 1$. Тада је скуп $C(\mathbb{Q})$ њених рационалних тачака коначан. □

[26)] Хелмут Хасе (Helmut Hasse, 1898–1979), немачки математичар

[27)] Херман Минковски (Hermann Minkowski, 1864–1909), немачки математичар и физичар

[28)] Полазећи од поља $\mathbb{Q}$ рационалних бројева и могућих нетривијалних апсолутних вредности на њему, то поље $\mathbb{Q}$ можемо проширити тако да добијемо бесконачно много поља $\mathbb{Q}_p$ p-адичних бројева и поље $\mathbb{Q}_\infty = \mathbb{R}$ реалних бројева. Сва тако добијена поља $\mathbb{Q}_p$ су међусобно различита и не постоје друга комплетирања поља $\mathbb{Q}$.

[29)] Герд Фалтингс (Gerd Faltings, 1954), немачки математичар

[30)] Џон Чарлс Филдс (John Charles Fields, 1863–1932), канадски математичар

[31)] *Филдсова медаља* је најпрестижнија математичка награда, и у рангу је Нобелове награде, пошто се Нобелова награда не додељује за открића из математике. Сваке четврте године, један или више математичара добије ово уважено признање. Победника бира Међународна математичка унија, а званично име Филдсове медаље је *Међународна медаља за изузетна математичка достигнућа*. Она се додељује само активним математичарима који имају највише четрдесет година. Занимљиво је да Нобелова награда за математику, ипак, постоји! То је *Абелова награда* коју од 2003. сваке године додељује Норвешка академија науке као међународну награду за изузетан научни допринос на пољу математике. Вредност награде је 660 000 евра. Могу је добити и математичари преко четрдесет година, јер се та награда даје за животно дело.

3.6 Безуова теорема

Видели смо да у комплексној пројективној равни $\mathbb{P}^2(\mathbb{C})$ алгебарска крива степена d и права имају тачно d пресечних тачака узимајући у обзир и њихове вишеструкости. Другим речима, те две криве имају $d = d \cdot 1$ пресечних тачака.

Безуова[32)] теорема[33)] је уопштење овог својства на парове кривих произвољног степена. Она је суштински прво била истакнута од стране Њутна у доказу 28. леме првог тома своје књиге *Principia*, где тврди да је број заједничких тачака две алгебарске криве једнак производу њихових степена. Ова теорема је касније објављена 1779. године у Безуовој књизи *Théorie générale des équation algébrique*.

Безуова теорема је класичан резултат теорије алгебарских кривих. Она уопштава и *Основни став алгебре* по коме комплексни полином степена n има тачно n нула рачунајући вишеструкости.

• Мултиплицитет пресека две криве

Пре него што формулишемо теорему, треба да дефинишемо вишеструкост или мултиплицитет пресека две криве, посебно трансверзални[34)] пресек, [4, страна 16].

Дефиниција 3.26. Ако је P заједничка тачка две равне алгебарске криве $\mathcal{C}_1$ и $\mathcal{C}_2$ која је несингуларна за обе криве, и тангентне праве на $\mathcal{C}_1$ и $\mathcal{C}_2$ у P су различите, онда је *мултиплицитет* пресека 1 и сам пресек називамо *трансверзални*. Ако криве $\mathcal{C}_1$ и $\mathcal{C}_2$ имају заједничку тангенту у P, тада је овај пресек *мултиплицитета* бар 2.

Интуитивно, *мултиплицитет* пресека алгебарских кривих $\mathcal{C}_1$ и $\mathcal{C}_2$ у тачки P је *степен поклапања* кривих $\mathcal{C}_1$ и $\mathcal{C}_2$ у тачки P.

• Безуова теорема

Поред Безуове теореме, навешћемо и њену последицу, [4, страна 16].

Теорема 3.9. [Безу] Нека су $\mathcal{C}_1$ и $\mathcal{C}_2$ две пројективне алгебарске криве дефинисане над пољем $\mathbb{K}$ које немају заједничких компоненти, то јест дефинисане су различитим нерастављивим полиномима. Тада је укупан број тачака пресека $\mathcal{C}_1$ и $\mathcal{C}_2$ са координатама у алгебарском затворењу од $\mathbb{K}$, рачунајући мултиплицитете, једнак производу степена $\mathcal{C}_1$ и $\mathcal{C}_2$. □

[32)] Етјен Безу (Étienne Bézout, 1730–1783), француски математичар

[33)] Овде се мисли на такозвану *велику Безуову теорему*, док *мала Безуова теорема* – тврђење познато из школске алгебре – гласи: α је корен полинома p ако и само ако $x - \alpha$ дели тај полином, то јест $p(\alpha) = 0 \Leftrightarrow (x - \alpha) \mid p(x)$.

[34)] Реч *трансверзала* потиче од новолатинске речи *transversalis* што у преводу значи *попречница, линија или површина која пресеца систем линија или површина.*

Последица 3.2. Нека две пројективне алгебарске криве $\mathcal{C}_1$ и $\mathcal{C}_2$ имају тачно n^2 тачака пресека и нека mn од њих леже на несводљивој кривој $\mathcal{D}$ степена $m < n$. Тада преосталих $n(n-m)$ тачака леже на кривој степена највише $n-m$. □

3.7 Нормализација алгебарских кривих

• Сигма-процес

Нека је дата сингуларна алгебарска крива. Помоћу одговарајуће смене, сингуларна алгебарска крива може постати алгебарска крива без сингуларних тачака, то јест глатка алгебарска крива. Другим речима, од сингуларне алгебарске криве, помоћу смене, можемо доћи до глатке алгебарске криве за коју кажемо да је *придружена* сингуларној алгебарској кривој. Тада, ту придружену криву називамо *несингуларно придружење* или *нормализација* полазне криве, а описани поступак, који се увек може спровести у коначно много корака називамо *разрешавање сингуларитета* или *сигма-процес*.

Пример 3.6. Тачка $(0,0)$ је сингуларна тачка алгебарске криве

$$\mathcal{C} : y^2 = x^3 + x^2.$$

Ако означимо са $f(x,y) = y^2 - x^3 - x^2$, тада је

$$\frac{\partial f}{\partial x}(0,0) = -3x^2 - 2x \mid_{x=0,\, y=0} = 0 \quad \text{и} \quad \frac{\partial f}{\partial y}(0,0) = 2y \mid_{x=0,\, y=0} = 0.$$

Због тога је и алгебарска крива $\mathcal{C}$ сингуларна. Ако уведемо смену $y = tx$, једначина која дефинише $\mathcal{C}$ постаје $t^2 = x + 1$. Она одређује алгебарску криву без сингуларних тачака, јер је

$$\frac{\partial f}{\partial x}(x_0, t_0) = 1 \neq 0$$

за сваку тачку (x_0, t_0), па је глатка алгебарска крива

$$\widetilde{\mathcal{C}} : t^2 = x + 1$$

несингуларно придружење или нормализација алгебарске криве $\mathcal{C}$. △

• Елиптичка и хиперелиптичка крива

Сигма-процес нам омогућава да, на још један начин, еквивалентан претходном, дефинишемо елиптичку и хиперелиптичку криву, [12, страна 56].

Дефиниција 3.27. *Елиптичка крива* је нормализација алгебарске криве задате једначином

$$y^2 = f(x),$$

при чему је $d^\circ f = 3$ или $d^\circ f = 4$.

Дефиниција 3.28. *Хиперелиптичка крива* је нормализација алгебарске криве рода g задате једначином

$$y^2 = f(x),$$

при чему је $d^\circ f = 2g + 1$ или $d^\circ f = 2g + 2$.

4

Увод у елиптичке криве

До сада смо упознали алгебарске криве. Сада ћемо упознати и елиптичке криве. Ово поглавље је посвећено најосновнијим чињеницама у вези са њима. За више детаља погледати [33], [15], [57], [48], [8] и [49].

4.1 Развој теорије елиптичких кривих

Видели смо да се зачеци идеје о елиптичким кривама јављају још у 3. веку код Диофанта у поступку решавања Диофантових једначина, посебно неодређених кубних једначина.

Након много векова заборава, Баше[1)] је у 17. веку поново открио сличне поступке, а Њутн је дао и њихову геометријску интерпретацију. Развој те идеје је, преко Ферма у 17. веку, Поенкареа[2)] у 19. и 20. веку, затим Мордела, Веја[3)], Сера[5)] и других, крајем 20. века довео до доказа последње Фермаове теореме.

Уз тај аритметички, постоји геометријски и аналитички аспект елиптичких кривих. Аналитички аспект се може пратити кроз развој *елиптичких интеграла* и *елиптичких функција* од 17. века, па све до данашњих дана. У 17. веку за његов развој су заслужни Волис[6)] и Њутн, у 18. веку Бернули[7)],

---

[1)] Клод Баше (Claude Gaspard Bachet de Méziriac, 1581–1638), француски математичар

[2)] Жил Анри Поенкаре (Jules Henri Poincaré, 1854–1912), француски математичар и теоријски физичар

[3)] Андре Вej[4)] (André Weil, 1906–1998), француски математичар

[4)] Чешћа, мада неправилна, српска транскрипција његовог имена је Вејл.

[5)] Жан-Пиер Сер (Jean-Pierre Serre, 1926), француски математичар

[6)] Џон Волис (John Wallis, 1616–1703), енглески свештеник и математичар

[7)] Јакоб Бернули (Jakob Bernoulli, 1654–1705), швајцарски математичар

Маклорен[8)], Фањано[9)] и Ојлер, док су то у 19. веку Лежандр[10)], Гаус, Абел, Јакоби[11)], Риман, Вајерштрас[12)], Клајн[13)] и Поенкаре.

Елиптичке криве можемо дефинисати над произвољним пољем $\mathbb{K}$. Међутим, најважнији случајеви су кад је $\mathbb{K}$ једно од поља $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ или $\mathbb{F}_q$.

4.2 Вајерштрасове кубне криве

• Вајерштрасов општи облик кубне криве

У поглављу о алгебарским кривама дефинисали смо над пољем $\mathbb{R}$ *кубну криву* или *кубику* као алгебарску криву трећег реда која је одређена кубном једначином

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3 + 3ex^2 + 6fxy + 3gy^2 + 3hx + 3iy + j = 0$$

са две непознате x и y где су a, b, c, d, e, f, g, h, i и j реалне константе за које важи да је $(a, b, c, d) \neq (0, 0, 0, 0)$.

При проучавању кубне криве желимо да је преведемо у одређени облик у којем ћемо моћи лакше да радимо са њом. Зато ћемо прво дефинисати Вајерштрасову кубну криву, и то најпре у пројективној равни $\mathbb{P}^2(\mathbb{K})$, а затим и у афиној равни $\mathbb{A}^2(\mathbb{K}) = \mathbb{K}^2$, при чему је $\mathbb{K}$ неко поље.

Дефиниција 4.1. *Вајерштрасова кубна крива* је уређени пар $(E, \mathcal{O})$ скупа E тачака у пројективној равни $\mathbb{P}^2(\mathbb{K})$ чије су координате решења једначине

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{4.1}$$

и базне тачке $\mathcal{O}$ из E која има координате $(0 : 1 : 0)$, при чему су a_1, a_2, a_3, a_4 и a_6 из $\mathbb{K}$.

Једначина (4.1) је *пројективна Вајерштрасова једначина.*

Сваку кубну криву, погодним избором оса у пројективној равни и пројективним транформацијама, можемо свести на облик (4.1), што је детаљније објашњено у [48, страна 42].

Вајерштрасову кубну криву можемо дефинисанати и афином једначином преласком на нехомогене координате помоћу смене $x = \frac{X}{Z}$ и $y = \frac{Y}{Z}$. У том случају, базна тачка $\mathcal{O}$ постаје бесконачно далека тачка коју не можемо видети у афиној равни $\mathbb{K}^2$, али ћемо сматрати да се она налази на свакој вертикалној правој $x = c$, где је c неки елемент из $\mathbb{K}$.

[8)] Колин Маклорен (Colin Maclaurin, 1698–1746), шкотски математичар

[9)] Ђулио Фањано (Giulio Fagnano, 1682–1766), италијански математичар

[10)] Адријен-Мари Лежандр (Adrien-Marie Legendre, 1752–1833), француски математичар

[11)] Карл Густав Јакоб Јакоби (Carl Gustav Jacob Jacobi, 1804–1851), немачки математичар

[12)] Карл Теодор Вилхелм Вајерштрас (Karl Theodor Wilhelm Weierstraß, 1815–1897), немачки математичар

[13)] Феликс Кристијан Клајн (Felix Christian Klein, 1815–1897), немачки математичар

Дефиниција 4.2. *Вајерштрасова кубна крива* је уређени пар $(E, \mathcal{O})$ скупа E тачака у афиној равни $\mathbb{K}^2$ чије су координате решења једначине

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{4.2}$$

и бесконачно далеке тачке $\mathcal{O}$ из E, при чему су a_1, a_2, a_3, a_4 и a_6 из $\mathbb{K}$.

Једначина (4.2) је *афина Вајерштрасова једначина.*

Дефиниција 4.3. Сваку од једначина (4.1) и (4.2) називамо *Вајерштрасов општи облик* кубне криве E или *Вајерштрасова форма* од E.

Вајерштрасова кубна крива имају једну веома важну особину:

Свака права сече Вајерштрасову кубну криву у тачно три тачке, рачунајући вишеструкости[14)].

У пројективној равни $\mathbb{P}^2(\mathbb{K})$ то се лако види. У афиној равни $\mathbb{K}^2$, ако посматрамо једначину (4.2) примећујемо, пошто у њој нема члана y^3, да свака вертикална права $x = c$, за c из $\mathbb{K}$, сече Вајерштрасову кубну криву у две тачке. Али, ако се узме у обзир да бесконачно далека тачка $\mathcal{O}$ такође припада тој кривој, добијамо и трећу пресечну тачку.

Вајерштасову кубну криву краће називамо и *Вајерштрасова кубика.*

• Вајерштрасов нормални облик кубне криве

У случају када за поље $\mathbb{K}$ важе одређени додатни услови, афина Вајерштрасова једначина (4.2) може бити још поједностављена, [49, страна 25].

Став 4.1. Нека је Вајерштрасова кубна крива E дефинисана једначином (4.2) над пољем $\mathbb{K}$ чија је карактеристика[15)]различита од 2 и 3[16)]. Тада ту једначину можемо свести на облик

$$y^2 = x^3 + ax + b. \tag{4.3}$$

Доказ. Пошто је карактеристика поља $\mathbb{K}$ различита од 2, можемо комплетирати квадрат на левој страни једнакости (4.2), и тада је

$$\left(y + \frac{1}{2}(a_1x + a_3)\right)^2 - \frac{1}{4}(a_1x + a_3)^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{4.4}$$

[14)] На основу Безуове теореме, ово важи и за сваку кубну криву.

[15)] *Карактеристика поља* $\mathbb{K}$ је најмањи природан број n – ако он постоји – такав да је $n \cdot 1_{\mathbb{K}} = 0_{\mathbb{K}}$, при чему су $0_{\mathbb{K}}$ и $1_{\mathbb{K}}$ неутрални елементи за сабирање, односно множење у том пољу $\mathbb{K}$. Ако такво n не постоји, то јест ако је $n \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ за сваки природан број n, онда кажемо да је поље $\mathbb{K}$ *карактеристике* 0. Поља $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ су карактеристике 0, док је карактеристика поља $\mathbb{F}_q$ једнака p, где је p прост број и $q = p^m$ за неки природан број m.

[16)] То значи да смемо вршити допуну, то јест комплетирање до потпуног квадрата, односно потпуног куба, као и дељење бројем 2, односно бројем 3.

Уводећи смену $y + \frac{1}{2}(a_1x + a_3) = \eta$, и даљим упрошћавањем (4.4) биће

$$\eta^2 = x^3 + \frac{1}{4}\left(4a_2 + a_1^2\right)x^2 + \frac{1}{2}\left(2a_4 + a_1a_3\right)x + \frac{1}{4}\left(4a_6 + a_3^2\right).$$

Означавајући $4a_2 + a_1^2$ са b_2, $2a_4 + a_1a_3$ са b_4 и $4a_6 + a_3^2$ са b_6 добијамо

$$\eta^2 = x^3 + \frac{1}{4}b_2x^2 + \frac{1}{2}b_4x + \frac{1}{4}b_6. \tag{4.5}$$

Сада се види зашто су коефицијенти у једначини (4.2) тако означени. Наиме, индексе смо изабрали тако да све претходне формуле буду хомогене у индексу. Пошто је карактеристика поља $\mathbb{K}$ различита и од 3, можемо комплетирати куб на десној страни једнакости (4.5), и тада је

$$\eta^2 = \left(x + \frac{1}{12}b_2\right)^3 - \frac{1}{48}b_2^2x - \frac{1}{1728}b_2^3 + \frac{1}{2}b_4x + \frac{1}{4}b_6. \tag{4.6}$$

Уводећи смену $x + \frac{1}{12}b_2 = \xi$, и даљим упрошћавањем (4.6) биће

$$\eta^2 = \xi^3 - \frac{1}{48}(b_2^2 - 24b_4)\xi - \frac{1}{864}(-b_2^3 + 36b_2b_4 - 216b_6).$$

Означавајући $b_2^2 - 24b_4$ са c_4 и $-b_2^3 + 36b_2b_4 - 216b_6$ са c_6 добијамо једначину

$$\eta^2 = \xi^3 - \frac{1}{48}c_4\xi - \frac{1}{864}c_6.$$

Коначно, стављајући да је $\eta = y$, $\xi = x$, $-\frac{1}{48}c_4 = a$ и $-\frac{1}{864}c_6 = b$ добијамо

$$y^2 = x^3 + ax + b. \qquad \square$$

Став 4.2. Нека је Вајерштрасова кубна крива E дефинисана једначином (4.2) над пољем $\mathbb{K}$. Ако је карактеристика тог поља 2, тада једначину (4.2) можемо свести на један од следећа два облика

$$y^2 + cy = x^3 + ax + b \quad \text{или} \quad y^2 + xy = x^3 + ax + b, \tag{4.7}$$

а ако је његова карактеристика 3, једначину (4.2) можемо свести на

$$y^2 = x^3 + ax^2 + bx + c. \ \square \tag{4.8}$$

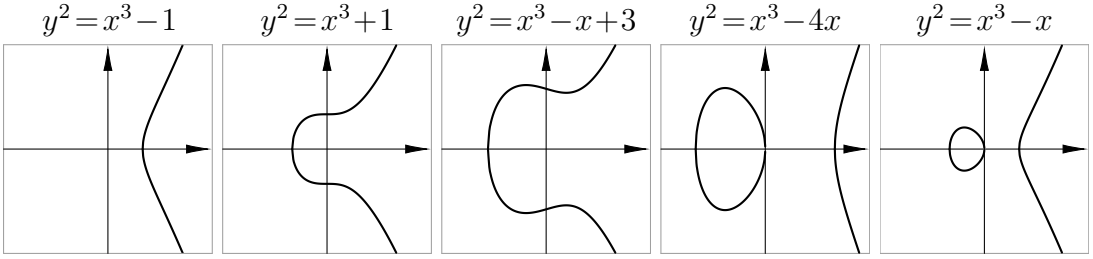
Дефиниција 4.4. Сваку од једначина (4.3), (4.7) и (4.8) називамо *Вајерштрасов нормалан облик* кубне криве E или *кратка Вајерштрасова форма* од E.

За кубну криву E задату једначном (4.3), (4.7) или (4.8) кажемо и да је *Вајерштрасова кубна крива у нормалном облику.*

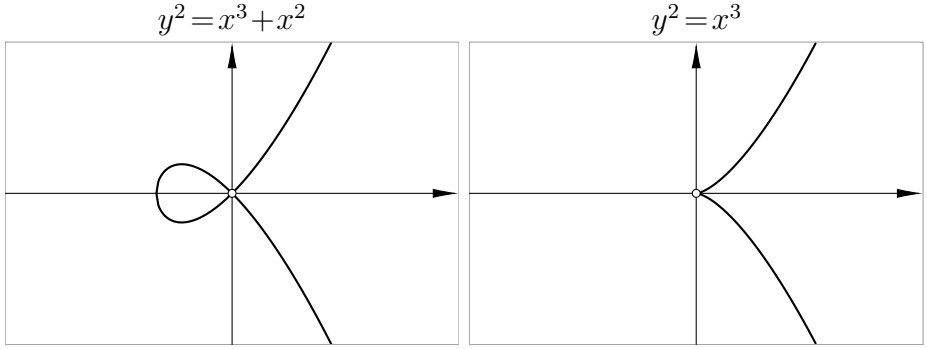
• Вајерштрасова кубна крива над пољем $\mathbb{R}$

Над већином поља, углавном није могуће дати смислен графички приказ Вајерштрасове кубне криве. Међутим, корисно је размотрити њен график над пољем $\mathbb{R}$ реалних бројева. Поље $\mathbb{R}$ има карактеристику 0, па елиптичка крива над пољем $\mathbb{R}$ има Вајерштрасов нормални облик $y^2 = x^3 + ax + b$.

На следећем цртежу приказани су неки графици Вајерштрасових кубних кривих над пољем $\mathbb{R}$.



Вајерштрасове кубне криве над пољем $\mathbb{R}$ могу бити глатке или сингуларне. Постоје два могућа облика реалне сингуларне кубне криве која зависе од тога да ли полином $x^3 + ax + b$ има двоструки или троструки реални корен.



У првом случају, реална кубна крива има тачку самопресека, а у другом касп.

• Дискриминанта Вајерштрасове кубне криве

Дефинишимо сада једну важну величину коју придружујемо свакој кубној кривој у Вајерштрасовом облику.

Дефиниција 4.5. Нека је кубна крива E задата једначином

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

у Вајерштрасовом општем облику. Величину

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

називамо *дискриминантом* Вајерштрасове кубне криве E, при чему је $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$.

Наредна дефиниција је специјалан случај претходне дефиниције (4.5).

Дефиниција 4.6. Нека је кубна крива E задата једначином

$$y^2 = x^3 + ax + b$$

у Вајерштрасовом нормалном облику. Величину

$$\Delta = -16(4a^3 + 27b^2)$$

називамо *дискриминантом* Вајерштрасове кубне криве E.

Иако фактор -16 делује небитно у дефиницији (4.14), испоставља се да је он згодан у напреднијем проучавању ових кривих. Ако желимо да истакнемо да је Δ дискриминанта криве E писаћемо и $\Delta(E)$.

Помоћу дискриминанте можемо дати критеријум када је кубна крива глатка, а када је сингуларна. У случају када је она сингуларна, можемо дати и тип сингуларитета. О томе нам говори следећа теорема, [48, страна 45].

Теорема 4.1. Нека је кубна крива E задата једначином $y^2 = x^3 + ax + b$ у Вајерштрасовом нормалном облику. Тада важи:

1° Крива E је глатка ако и само ако је $\Delta \neq 0$.

2° Крива E је сингуларна и има тачку самопресека ако и само ако је $\Delta = 0$ и $a \neq 0$.

3° Крива E је сингуларна и има касп ако и само ако је $\Delta = a = 0$.

Доказ. 1° Прво претпоставимо да је $\Delta \neq 0$, и докажимо да је крива E глатка. Напишимо једначину $y^2 = x^3 + ax + b$ у облику $F(x, y) = y^2 - f(x) = 0$, где је $f(x) = x^3 + ax + b$. Тада важи

$$\frac{\partial F}{\partial x} = -f'(x), \quad \frac{\partial F}{\partial y} = 2y. \tag{4.9}$$

Крива је глатка ако не постоји ниједна тачка на кривој у којој су парцијални изводи (4.9) истовремено једнаки нули. То значи да у свакој тачки на кривој постоји добро дефинисана тангента.

Претпоставимо супротно, нека крива E није глатка, то јест нека су парцијални изводи (4.9) истовремено једнаки нули у тачки (x_0, y_0), односно

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0.$$

Тада је $-f'(x_0) = 0$ и $2y_0 = 0$, то јест $f'(x_0) = 0$ и $y_0 = f(x_0) = 0$. Одавде следи да је

$$f'(x_0) = f(x_0) = 0,$$

односно да функције $f(x)$ и $f'(x)$ имају заједнички корен x_0. Тада је x_0 двоструки корен од $f(x)$, па је x_0 и двоструко решење једначине $f(x) = 0$. У

том случају, дискриминанта једначине $x^3 + ax + b = 0$[17] задовољава релацију $D = 0$, то јест

$$\frac{a^3}{27} + \frac{b^2}{4} = 0,$$

односно $4a^3 + 27b^2 = 0$, па је и $\Delta = -16(4a^3 + 27b^2) = 0$. Тиме смо, на основу закона контрапозиције[18], доказали да ако је $\Delta \neq 0$,тада је крива E глатка.

Сада претпоставимо да је крива E глатка и докажимо да је $\Delta \neq 0$. Претпоставимо супротно, нека је $\Delta = 0$. Тада је и $D = 0$, па $f(x)$ има бар један двоструки корен, на пример x_0, одакле следи да је $(x_0, 0)$ сингуларна тачка криве E. Дакле, постоји бар једна сингуларна тачка криве E, па она није глатка. И у овом случају смо, на основу закона контрапозиције, доказали да ако је крива E глатка, тада је $\Delta \neq 0$. Овим смо доказали тврђење 1°.

Слично бисмо доказали и тврђења под 2° и 3°. □

4.3 Елиптичке криве

• Дефиниција елиптичке криве

У претходном поглављу, елиптичку криву смо дефинисали као алгебарску криву рода $g = 1$. То је *геометријска дефиниција*. Сада ћемо елиптичку криву дефинисати и *алгебарски* преко Вајерштрасове кубне криве. Иако је елиптичка крива пројективна крива, ми ћемо је дефинисати афином једначином, јер ће нам то бити погоднije за даљи рад, [15, страна 451].

Дефиниција 4.7. *Елиптичка крива* $(E, \mathcal{O})$ над пољем $\mathbb{K}$ је глатка Вајерштрасова кубна крива задата афином једначином

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{4.10}$$

при чему је $\mathcal{O}$ из E бесконачно далека тачка, а a_1, a_2, a_3, a_4 и a_6 из $\mathbb{K}$.

Једначину (4.10) називамо *Вајерштрасов општи облик* елиптичке криве E или *Вајерштрасова форма* од E, и можемо је доста поједноставити уколико је карактеристика поља $\mathbb{K}$ различита од 2 и 3, [15, страна 452].

Дефиниција 4.8. *Елиптичка крива* $(E, \mathcal{O})$ над пољем $\mathbb{K}$ карактеристике различите од 2 и 3 је глатка Вајерштрасова кубна крива задата афином једначином

$$y^2 = x^3 + ax + b, \tag{4.11}$$

при чему је $\mathcal{O}$ из E бесконачно далека тачка, а a и b из $\mathbb{K}$.

[17] *Закон контрапозиције* је таутологија $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$.

[18] *Дискриминанта* D кубне једначине $x^3 + px + q = 0$ је $D = \frac{q^2}{4} + \frac{p^3}{27}$.

Једначину (4.11) називамо *Вајерштрасов нормални облик* елиптичке криве E или *кратка Вајерштрасова форма* од E.

У наставку, углавном ћемо разматрати елиптичке криве које су дефинисане над пољем $\mathbb{K}$ чија је карактеристика различита од 2 и 3, али навешћемо и дефиниције када је карактеристика поља $\mathbb{K}$ једнака 2, односно 3, [21, страна 234].

Дефиниција 4.9. *Елиптичка крива* $(E, \mathcal{O})$ над пољем $\mathbb{K}$ карактеристике 2 је глатка Вајерштрасова кубна крива задата једном од афиних једначина

$$y^2 + cy = x^3 + ax + b \quad \text{или} \quad y^2 + xy = x^3 + ax + b, \tag{4.12}$$

при чему је $\mathcal{O}$ из E бесконачно далека тачка, а a, b и c из $\mathbb{K}$.

Дефиниција 4.10. *Елиптичка крива* $(E, \mathcal{O})$ над пољем $\mathbb{K}$ карактеристике 3 је глатка Вајерштрасова кубна крива задата афином једначином

$$y^2 = x^3 + ax^2 + bx + c, \tag{4.13}$$

при чему је $\mathcal{O}$ из E бесконачно далека тачка, а a, b и c из $\mathbb{K}$.

Често ћемо уместо $(E, \mathcal{O})$ писати само E, када је јасно коју смо бесконачно далеку тачку изабрали. Такође, ако желимо да истакнемо да посматрамо елиптичку криву над пољем $\mathbb{K}$, писаћемо и $E/\mathbb{K}$.

За Вајерштрасову форму (4.10) кажемо да је «добра» над свим пољима.

Елиптичка крива је глатка Вајерштрасова кубна крива, па је дискриминанта Δ Вајерштрасове кубне криве уједно и дискриминанта елиптичке криве, у одговарајућем облику. Услов да је елиптичка крива E глатка еквивалентан је услову да је њена дискриминанта Δ различита од нуле.

• Изоморфне елиптичке криве

Сада ћемо видети када су две елиптичке криве изоморфне, [33, страна 18].

Дефиниција 4.11. Нека су $E_1/\mathbb{K}$ и $E_2/\mathbb{K}$ елиптичке криве задате једначинама

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$E_2 : y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6.$$

у Вајерштрасовом општем облику. Кажемо да су оне *изоморфне* над пољем $\mathbb{K}$, и пишемо $E_1 \cong E_2$, ако постоје u, r, s и t из $\mathbb{K}$, при чему је $u \neq 0$, такви да трансформација координата

$$(x, y) \to (u^2x + r, u^3y + u^2sx + t)$$

трансформише једначину од E_1 у једначину од E_2.

Наредна дефиниција је специјалан случај претходне дефиниције (4.11).

Дефиниција 4.12. Нека су $E_1/\mathbb{K}$ и $E_2/\mathbb{K}$ елиптичке криве задате једначинама

$$E_1 : y^2 = x^3 + ax + b$$
$$E_2 : y^2 = x^3 + a'x + b'.$$

у Вајерштрасовом нормалном облику. Кажемо да су оне *изоморфне* над пољем $\mathbb{K}$ чија је карактеристика различита од два и три, и пишемо $E_1 \cong E_2$, ако постоји u из $\mathbb{K}$, при чему је $u \neq 0$, такво да трансформација координата

$$(x, y) \to (u^2x, u^3y)$$

трансформише једначину од E_1 у једначину од E_2.

Дакле, за елиптичке криве $E_1/\mathbb{K}$ и $E_2/\mathbb{K}$ задате у Вајерштрасовом нормалном облику важи:

$$E_1 \cong E_2 \Leftrightarrow (u^3y)^2 = (u^2x)^3 + a'(u^2x) + b' \Leftrightarrow a' = u^4a, b' = u^6b$$

при чему (x, y) припада $E_1/\mathbb{K}$, и

$$\Delta(E_2) = -16(4(a')^3 + 27(b')^2) = u^{12}\Delta(E_1).$$

• *j*-инваријанта елиптичке криве

Поред дискриминанте $\Delta(E)$ елиптичке криве E, дефинисаћемо још једну важну величину коју придружујемо свакој елиптичкој кривој E, а која је повезана са том дискриминантом, [33, страна 19].

Дефиниција 4.13. Нека је елиптичка крива E задата једначином

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

у Вајерштрасовом општем облику. Величину

$$j = \frac{c_4^3}{\Delta},$$

називамо *j-инваријантом* елиптичке криве E, при чему је $c_4 = b_2^2 - 24b_4$, $b_2 = 4a_2 + a_1^2$ и $b_4 = 2a_4 + a_1a_3$.

Наредна дефиниција је специјалан случај претходне дефиниције (4.13).

Дефиниција 4.14. Нека је елиптичка крива E задата једначином

$$y^2 = x^3 + ax + b$$

у Вајерштрасовом нормалном облику. Величину

$$j = \frac{1728(-4a)^3}{\Delta}$$

називамо *j-инваријантом* елиптичке криве E.

Ако желимо да истакнемо j-инваријанту елиптичке криве E писаћемо и $j(E)$.

Помоћу j-инваријанте можемо утврдити када су две елиптичке криве над истим пољем изоморфне. О томе нам говори следећи став, [33, страна 19].

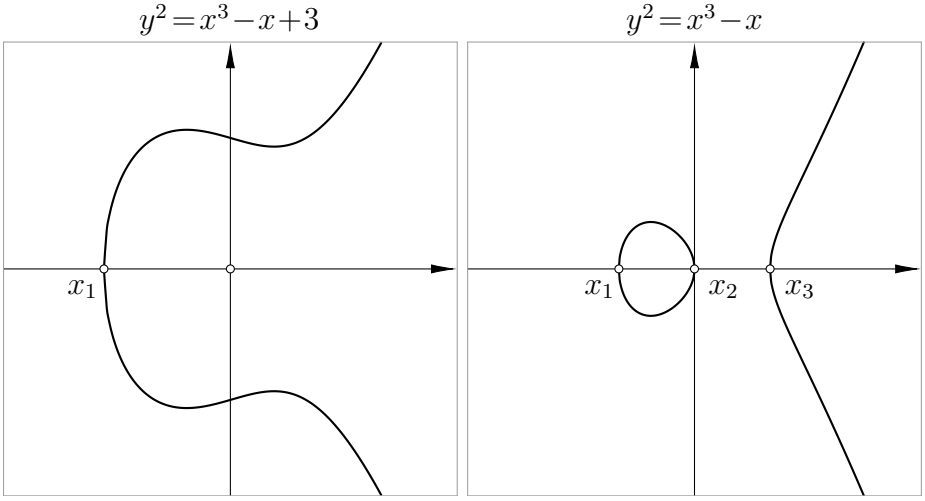
Став 4.3. Нека је $\mathbb{K}$ поље чија је карактеристика различита од два и три. Тада важи:

1° Елиптичке криве $E_1/\mathbb{K}$ и $E_2/\mathbb{K}$ су изоморфне над $\mathbb{K}$ ако и само ако је $j(E_1) = j(E_2)$.

2° За свако j из $\mathbb{K}$ постоји елиптичка крива $E/\mathbb{K}$ тако да је $J(E) = j$. □

• Елиптичка крива над пољем $\mathbb{R}$

Елиптичку криву $E/\mathbb{R}$, без тачке у бесконачности, можемо приказати као криву у $\mathbb{R}^2$, то јест као подскуп равни. Тада график елиптичке криве може имати један од два основна облика, као што је приказано.



Ако полином $x^3 + ax + b$ има један реалан корен, на пример x_1, тада се график елиптичке криве састоји од једне компоненте. У том случају једначина елиптичке криве $E/\mathbb{R}$ је $y^2 = (x - x_1)(x - x_2)(x - \bar{x}_2)$, при чему су x_2 и $x_3 = \bar{x}_2$ конјуговано комплексни корени датог полинома. Тада је и $4a^3 + 27b^2 > 0$, па график од $E/\mathbb{R}$ има једну компоненту ако је $\Delta < 0$.

Ако полином $x^3 + ax + b$ има три различита реална корена, на пример x_1, x_2 и x_3, тада се график елиптичке криве састоји од две компоненте. У том случају једначина елиптичке криве $E/\mathbb{R}$ је $y^2 = (x - x_1)(x - x_2)(x - x_3)$. Тада је и $4a^3 + 27b^2 < 0$, па график од $E/\mathbb{R}$ има две компоненте ако је $\Delta > 0$.

• Елиптичка крива и бирационална трансформација

Геометријска дефиниција елиптичке криве позната је и као «шира» дефиниција елиптичке криве, јер она укључује не само глатке кубне криве, већ и све оне криве које су им бирационално еквивалентне, то јест оне криве које се добијају помоћу бирационалних трансформација.

Дефиниција 4.15. *Бирационална трансформација* је рационална трансформација чији је инверз такође рационална трансформација.

Бирационалне трансформације чувају род криве, али не чувају њен ред.

Пример 4.1. Нека је $\mathcal{C}$ крива задата афином једначином

$$\mathcal{C} : y^2 = x^4 + 3x^2 + 2x.$$

Њена једначина је облика $y^2 = f(x)$, при чему је $d^\circ f = 4$. Смена

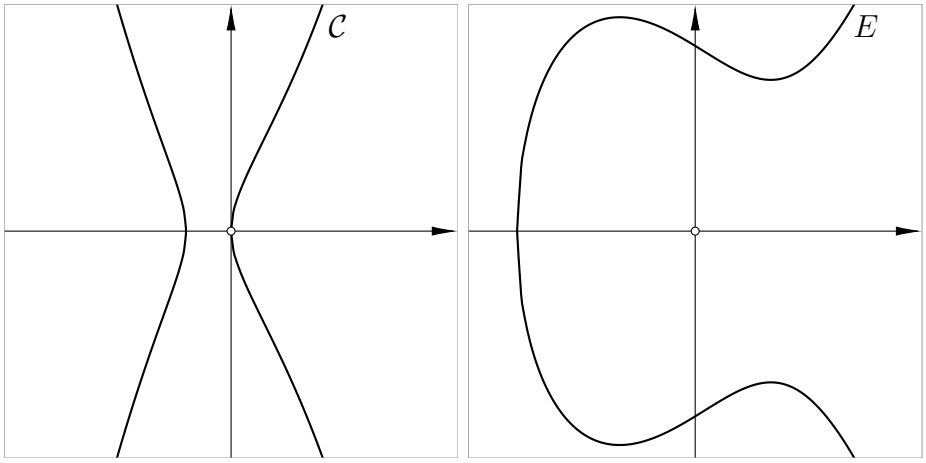
$$x = \frac{2}{s-1}, \quad y = \frac{2t}{(s-1)^2}, \tag{4.14}$$

је рационална трансформација јер x, односно y рационално изражавамо помоћу s, односно s и t. Њена инверзна трансформација

$$s = \frac{x+2}{x}, \quad t = \frac{2y}{x^2},$$

је, такође, рационална трансформација, па је (4.14) и бирационална трансформација. Због тога је крива $\mathcal{C}$ бирационално еквивалентна кривој

$$E : t^2 = s^3 - 3s + 6.$$



Како је крива E елиптичка, то је и полазна крива $\mathcal{C}$ елиптичка. △

Дакле, елиптичке криве могу бити и алгебарске криве задате једначином $y^2 = f(x)$, при чему је $d^\circ f = 4$, ако су оне бирационално еквивалентне некој елиптичкој кривој.

4.4 Елиптичке криве над пољем $\mathbb{C}$

Када се посматра над пољем $\mathbb{R}$, елиптичка крива E је крива, то јест једнодимензионални објекат. Ако елиптичку криву посматрамо над пољем $\mathbb{C}$, њен граф је, као и алгебарске криве над $\mathbb{C}$, површ, то јест дводимензионални објекат у четвородимензионалом простору. Да бисмо визуелизовали елиптичку криву $E/\mathbb{C}$, то јест ту површ, морамо дефинисати неколико нових појмова.

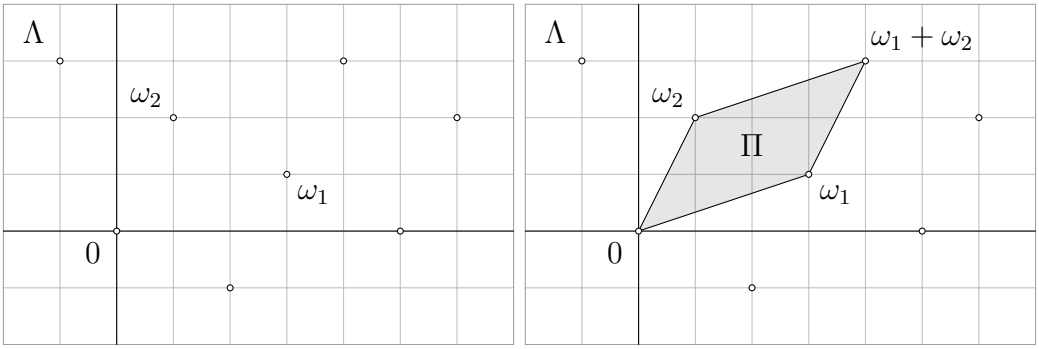
• Решетка и фундаментални паралелограм решетке на $\mathbb{C}$

Дефиниција 4.16. Нека су ω_1 и ω_2 комплексни бројеви линеарно независни над пољем $\mathbb{R}$. Тада скуп

$$\Lambda = \Lambda(\omega_1, \omega_2) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \left\{ n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z} \right\} \subset \mathbb{C}$$

називамо *решетка* или *мрежа* на $\mathbb{C}$ разапета са ω_1 и ω_2.

Јасно је да комплексни бројеви ω_1 и ω_2 чине базу решетке Λ, [33, страна 24].



Група $(\Lambda, +)$ је дискретна подгрупа Абелове групе $(\mathbb{C}, +)$. Према [35, страна 410] имамо следећу дефиницију.

Дефиниција 4.17. Скуп

$$\Pi = \left\{ a_1\omega_1 + a_2\omega_2 \mid 0 \leq a_i < 1, i = 1, 2 \right\}$$

називамо *фундаменталнi паралелограм* или *фундаменатлна област* решетке Λ.

• Комплексан торус

Решетка Λ је дискретна подгрупа од $\mathbb{C}$, па је и $\mathbb{C}/\Lambda$ такође група. Тада свака класа из $\mathbb{C}/\Lambda$ има по једног свог представника у Π. Операција у групи $\mathbb{C}/\Lambda$ је сабирање комплексних бројева по модулу Λ. Другим речима, свака тачка из $\mathbb{C}$ је конгруентна по модулу Λ тачно једној тачки из Π. Ово значи да елементе из $\mathbb{C}/\Lambda$ заправо можемо сматрати елементима из Π. Ако посматрамо затворење $\overline{\Pi}$, тада су наспрамне странице паралелограма Π идентификоване.

Да бисмо све ово визуелизовали, можемо замислити да смо најприје «слепили» две супротне странице паралелограма, и тако добили ваљак, а након тога да смо «слепили» и друге две супротне странице паралелограма, то јест базе добијеног ваљка. Тако смо добили торус који називамо *комплексни торус* и означавамо га са $\mathbb{T}(\omega_1, \omega_2)$ или краће само са $\mathbb{T}$.

Другим речима, количнички простор $\mathbb{C}/\Lambda$ је еквивалентан паралелограму $\overline{\Pi}$ са идентификованим наспрамним страницама, што је тополошки еквивалентно комплексном торусу $\mathbb{T}$. Дакле, количнички простор $\mathbb{C}/\Lambda$ тополошки је комплексни торус $\mathbb{T}$ на коме имамо структуру количничке групе $\mathbb{C}/\Lambda$ коју смо претходно описали.

Да бисмо показали да је елиптичка крива $E/\mathbb{C}$ исто што и торус $\mathbb{T} = \mathbb{C}/\Lambda$, конструисаћемо изоморфизам између $\mathbb{T} = \mathbb{C}/\Lambda$ и скупа $E(\mathbb{C})$ свих $\mathbb{C}$ -тачака елиптичке криве E заједно са тачком $\mathcal{O}$. То ћемо урадити помоћу Вајерштрасове $\wp$[19)]-функције, која је важан и нетривијалан пример елиптичке функције. Зато прво дефинишимо елиптичку функцију.

• Елиптичка функција

Да бисмо дефинисали елиптичку финкцију, морамо да дефинишемо периодичну функцију, [35, страна 408].

Дефиниција 4.18. Комплексну функцију f називамо *периодична*, ако постоји број $\omega \neq 0$ такав да за све вредности промењљиве z из домена функције f важи

$$f(z + \omega) = f(z).$$

Константу ω називамо *периодом* комплексне функције f.

Нека је f периодична мероморфна функција у односу на решетку Λ. Тада, за свако z из $\mathbb{C}$ и свако ω из Λ важи $f(z + \omega) = f(z)$. Пошто финкцију f посматрамо у односу на решетку Λ која је разапета са ω_1 и ω_2, на основу претходног можемо закључити да је $f(z + \omega_1) = f(z)$ и $f(z + \omega_2) = f(z)$, то јест $f(z + \omega_1) = f(z + \omega_2)$, односно

$$f(z + m\omega_1 + n\omega_2) = f(z),$$

при чему су m и n из $\mathbb{Z}$, а количник $\frac{\omega_1}{\omega_2}$ није реалан[21)].

[19)] знак $\wp$ [20)] се чита *пе*

[20)] Вајерштрас је на почетку своје каријере радио у гимназији где је предавао и лепо писање, па је за своју функцију измислио калиграфску верзију слова p која је постала стандардна ознака.

[21)] што је исто као и $\operatorname{Im} \frac{\omega_1}{\omega_2} \neq 0$

Другим речима, посматрана мероморфна функција f је периодична у односу на два линеарно независна периода у комплексној равнини $\mathbb{C}$. На основу [35, страна 408] имамо

Дефиниција 4.19. Функцију која има два различита периода ω_1 и ω_2 чији количник $\frac{\omega_1}{\omega_2}$ није реалан називамо *двопериодичном* или *двоструко периодичном функцијом.*

Према [35, страна 410], имамо и

Дефиниција 4.20. Двопериодичне мероморфне функције називамо *елиптичким функцијама.*

Дакле, елиптичка функција у односу на решетку Λ је мероморфна функција f таква да за свако z из $\mathbb{C}$ и свако ω из Λ важи

$$f(z+\omega) = f(z).$$

Уколико за елиптичку функцију f треба нагласити решетку Λ њених периода ω_1 и ω_2[22)], тада пишемо $f(z \mid \Lambda)$ или $f(z \mid \omega_1, \omega_2)$. На основу [50, страна 1] имамо

Теорема 4.2. [Абел] Мероморфна функција f може имати највише два линеарно независна периода, то јест постоје највише два периода ω_1 и ω_2 таква да је

$$\omega = m\omega_1 + n\omega_2$$

за било који период ω од f. □

Према Абеловој теореми, мероморфне функције можемо поделити у три класе:

- непериодичне,
- периодичне са једним периодом – *простопериодичне*,
- двопериодичне – елиптичке.

Дакле, елиптичке функције су посебна класа мероморфних функција. Елиптичке функције имају велику примену у разним деловима математике и механике.

• Вајерштрасова $\wp$-функција и њене особине

Пошто смо дефинисали елиптичку функцију, можемо сада дефинисати и Вајерштрасову $\wp$-функцију, [35, страна 414].

[22)] Из традиционалних разлога – основни период синуса и косинуса је 2π, а период функције $z \mapsto e^z$ је $2\pi i$ – неки аутори периоде елиптичких функција означавају са $2\omega_1$ и $2\omega_2$, а решетку њима одређену са 2Λ.

Дефиниција 4.21. Нека је Λ решетка на $\mathbb{C}$ и $\Lambda' = \Lambda \setminus \{0\}$. Тада *Вајерштрасову $\wp$-функцију* дефинишемо помоћу следећег реда

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{4.15}$$

Основне особине Вајерштрасове $\wp$-функције дате су у наредној теореми, [59, страна 262].

Теорема 4.3. Нека је дата решетка Λ на $\mathbb{C}$. Тада за Вајерштрасову $\wp$-функцију важе следећа тврђења:

1° Ред (4.15) који дефинише $\wp(z)$ конвергира апсолутно и равномерно на сваком компактном скупу који не садржи елементе из Λ.

2° $\wp(z)$ је мероморфна на $\mathbb{C}$ и има двоструки пол у сваком ω из Λ.

3° $\wp(z)$ је непарна, то јест важи $\wp(-z) = \wp(z)$ за свако z из $\mathbb{C}$.

4° $\wp(z)$ је елиптичка у односу на решетку Λ, то јест важи $\wp(z+\omega) = \wp(z)$ за свако ω из Λ. □

Следеће две теореме (4.4) и (4.5) нам говоре о Вајерштрасовој $\wp$-функцији и њеном изводу $\wp'$. Прва од њих је преузета из [12, страна 46], а друга из [59, страна 262]

Теорема 4.4. Вајерштрасова $\wp$-функција задовољава диференцијалну једначину облика

$$(\wp')^2 = 4\wp^3 + a\wp + b \tag{4.16}$$

за неке a и b из $\mathbb{C}$. □

Дакле, Вајерштрасова $\wp$-функција и њен извод $\wp'$ задовољавају једноставну алгебарску релацију (4.16). Ово представља повод за детаљније проучавање кривих облика

$$y^2 = 4x^3 + ax + b$$

за неке a и b из $\mathbb{C}$.

Теорема 4.5. Скуп свих елиптичких функција f у односу на решетку Λ је $\mathbb{C}(\wp, \wp')$. □

На основу [35, страна 422] имамо и следећу теорему у вези са $\wp$ и $\wp'$.

Теорема 4.6. Нека је $\wp$ Вајерштрасова и f елиптичка функција са мрежом периода Λ. Тада постоје рационалне функције R и S са комплексним коефицијентима тако да је

$$f(z) = R(\wp(z)) + S(\wp(z))\wp'(z). \qquad \square$$

Другим речима, свака елиптичка функција је рационална комбинација функције $\wp$ и њеног извода $\wp'$.

Да бисмо конструисали тражени изоморфизам између $\mathbb{T} = \mathbb{C}/\Lambda$ и скупа $E(\mathbb{C})$, потребно је да уведемо још један појам – Ајзенштајнов[23)] ред.

• Ајзенштајнов ред

Дефиниција 4.22. Нека је Λ решетка на $\mathbb{C}$, $\Lambda' = \Lambda \setminus \{0\}$ и нека је $k \geq 2$ цео број. *Ајзенштајнов ред* тежине $2k$, у односу на решетку Λ је ред

$$G_{2k} = G_{2k}(\Lambda) = \sum_{\omega \in \Lambda'} \omega^{-2k}.$$

Приметимо да је $G_{2k+1} = 0$, јер се чланови $\omega^{-(2k+1)}$ и $(-\omega)^{-(2k+1)}$ поништавају, па због тога дефинишемо Ајзенштајнов ред само за парне целе бројеве.

Следећом теоремом дата је веза између Вајерштрасове $\wp$-функције и Ајзенштајновог реда, [12, стране 46 и 47].

Теорема 4.7. Нека је $\wp(z)$ Вајерштрасова $\wp$-функција и G_{2k} Ајзенштајнов ред. Тада је

$$(\wp'(z))^2 = 4(\wp(z))^3 - 60G_4\wp(z) - 140G_6. \quad \square \tag{4.17}$$

Уобичајено је да се користе ознаке $g_2 = 60G_4$ и $g_3 = 140G_6$. Тада једнакост (4.17) гласи

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3. \tag{4.18}$$

• Изоморфизам између $\mathbb{T}$ и $E(\mathbb{C})$

На основу једнакости (4.18), тачке $(\wp(z), \wp'(z))$ леже на кривој

$$y^2 = 4x^3 - g_2x - g_3. \tag{4.19}$$

Традиционално се оставља 4 као коефицијент уз x^3, уместо да се изврши смена променљивих како би коефицијент уз x^3 био 1. Дискриминанта кубног полинома на десној страни је

$$\Delta = 16(g_2^3 - 27g_3^2)$$

Тада важи следећи став, [59, страна 269].

Став 4.4. За кубни полином $4x^3 - g_2x - g_3$ важи да је $\Delta \neq 0$. $\square$

Из става (4.4) следи да је крива (4.19) елиптичка крива. Дакле, функција

$$z \mapsto (\wp(z), \wp'(z))$$

[23)] Фердинанд Готхолд Макс Ајзенштајн (Ferdinand Gotthold Max Eisenstein, 1823–1852), немачки математичар

сваком комплексном броју z придружује неку тачку $(\wp(z), \wp'(z))$ на елиптичкој кривој $E : y^2 = 4x^3 - g_2x - g_3$. Ако променимо z за неки елемент из Λ вредност функција $\wp(z)$ и $\wp'(z)$ се неће променити, јер су оне двопериодичне.

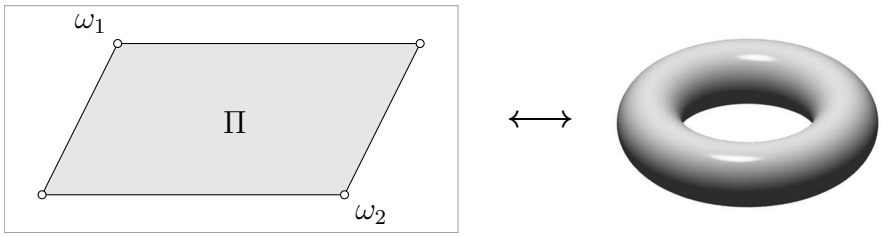
Дакле, $\wp(z)$ и $\wp'(z)$ зависе само од $z(\bmod \Lambda)$, па имамо дефинисано пресликавање из $\mathbb{T} = \mathbb{C}/\Lambda$ у $E(\mathbb{C})$. Отуда и на основу [59, страна 270],

Теорема 4.8. Нека је Λ решетка на $\mathbb{C}$ и нека је $E : y^2 = 4x^3 - g_2x - g_3$ елиптичка крива. Тада, пресликавање $\Phi : \mathbb{T} = \mathbb{C}/\Lambda \to E(\mathbb{C})$ дефинисано са

$$z \mapsto (\wp(z), \wp'(z))$$
$$0 \mapsto \infty$$

је изоморфизам између комплексног торуса $\mathbb{T} = \mathbb{C}/\Lambda$ и комплексних тачака $E(\mathbb{C})$ елиптичке криве E. □

Дакле, елиптичку криву над $\mathbb{C}$ можемо поистоветити са количничком групом $\mathbb{C}/\Lambda$, то јест комплексним торусом $\mathbb{T}$.



На основу теореме (4.4) Вајерштрасова $\wp$-функција задовољава и диференцијалну једначину

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3.$$

То значи да комплексне тачке на елиптичкој кривој $y^2 = 4x^3 - g_2x - g_3$ можемо параметризовати помоћу $(\wp(t), \wp'(t))$, слично као што јединични круг можемо параметризовати помоћу $(\cos t, \sin t)$, јер функција $y = \sin x$ задовољава диференцијалну једначину $y^2 + (y')^2 = 1$.

Горе наведена параметризација тачака на елиптичкој кривој помоћу Вајерштрасове $\wp$-функције представља изоморфизам из $E(\mathbb{C})$ у $\mathbb{T} = \mathbb{C}/\Lambda$. Вајерштрасова $\wp$-функција је у потпуности одређена својим вредностима у фундаменталном паралелограму који се састоји од свих комплексних бројева облика $a_1\omega_1 + a_2\omega_2$, $0 \leq a_i < 1, i = 1, 2$.

4.5 Елиптичка крива и елиптички интеграл

Историјски, појам *елиптичка крива* је настао од појма *елиптички интеграл*, који се појављује у проблему израчунавања дужине лука, то јест обима *елипсе*.

• **Обим елипсе**

Из почетних курсева анализе је позната формула за израчунавање дужине лука криве.

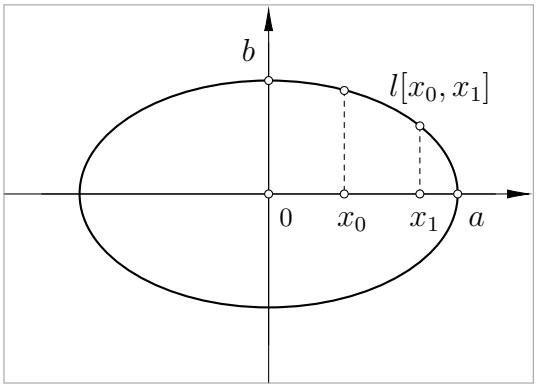
Дефиниција 4.23. Ако је $y = f(x)$ непрекидна функција која има непрекидан извод на сегменту $[a, b]$, тада је дужина l криве на сегменту $[a, b]$ дата формулом

$$l[a, b] = \int_a^b \sqrt{1 + (f'(x))^2}dx \tag{4.20}$$

Искористимо формулу (4.20) за налажење дужине лука $l[x_0, x_1]$ елипсе између тачака x_0 и x_1, па самим тим и за израчунавање обима елипсе. Нека су a и b позитивни бројеви, при чему је $a > b$. Посматрајмо елипсу

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \tag{4.21}$$

чије су полуосе a и b.



Када решимо једначину (4.21) по y и узмемо позитиван квадратни корен, добијамо функцију $y = f(x) = \frac{b}{a}\sqrt{a^2 - x^2}$. Затим, када израчунамо $\sqrt{1 + (f'(x))^2}$ и ставимо да је $k = \frac{\sqrt{b^2-a^2}}{a}$, формула (4.20) за дужину лука постаје

$$l[x_0, x_1] = \int_{x_0}^{x_1} \frac{a^2 - k^2x^2}{\sqrt{(a^2 - x^2)(a^2 - k^2x^2)}}dx,$$

одакле се добија да је обим O елипсе дат са

$$O = 4\int_0^a \frac{a^2 - k^2x^2}{\sqrt{(a^2 - x^2)(a^2 - k^2x^2)}}dx. \tag{4.22}$$

Сменом $x = at$, $dx = adt$ интеграл (4.22) постаје

$$O = 4a\int_0^1 \frac{1 - k^2t^2}{\sqrt{(1 - t^2)(1 - k^2t^2)}}dt. \tag{4.23}$$

Његовим упрошћавањем добијамо

$$O = 4a \int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}} - 4ak^2 \int_0^1 \frac{t^2 dt}{\sqrt{(1-t^2)(1-k^2t^2)}}. \tag{4.24}$$

• Елиптички интеграл

Интеграл (4.23), односно оба интеграла у (4.24) не можемо изразити преко елементарних функција, то јест не можемо их рационалисати рационалним функцијама. Помоћу рационалне смене, можемо их свести на интеграл

$$\int R(x, \sqrt{P(x)})dx$$

рационалне функције $R(x, \sqrt{P(x)})$ две промењљиве, при чему је P полином трећег степена. Како се интеграли (4.23) и (4.24) појављују у решавању проблема одређивања обима елипсе називамо их елиптичким интегралима. На основу [12, страна 51] имамо следећу дефиницију.

Дефиниција 4.24. *Елиптички интеграл* је интеграл облика

$$\int R(x, \sqrt{P(x)})dx$$

где је R рационална функција, а P полином трећег или четвртог степена[24)].

Елиптичке интеграле су открили Ојлер и Фањано. Са елиптичким интегралима започиње једна од најлепших теорија у математици – *Теорија елиптичких функција.*

Нека је дата алгебарска крива афином једначином

$$f(x, y) = 0. \tag{4.25}$$

Према теореми 3.1, под одређеним условима, из једначине (4.25) можемо изразити промењљиву y као неку функцију од x, на пример $y = g(x)$. Тада је и $f(x, g(x)) = 0$ за свако x где је функција g дефинисана. Нека је сада $R(x, y)$ рационална функција две промењљиве x и y. Функција R је количник два полинома. Ако у $R(x, y)$ заменимо $y = g(x)$ добијамо алгебарску функцију $R(x, f(x))$ која је повезана са алгебарском кривом (4.25). Интеграл те алгебарске функције је интеграл облика

$$\int R(x, y)dx = \int R(x, g(x))dx. \tag{4.26}$$

За интеграл (4.26) кажемо и да је *придружен* алгебарској кривој (4.25). Сада можемо дефинисати елиптички интеграл и помоћу елиптичке криве.

[24)] то јест, $P = ax^3 + bx^2 + cx + d$ или $P = ax^4 + bx^3 + cx^2 + dx + e$

Дефиниција 4.25. Интеграл

$$\int R(x, g(x))dx$$

је *елиптички интеграл* ако је алгебарска крива $\mathcal{C} : f(x, y) = 0$ којој је он придружен елиптичка, R рационална функција и $y = g(x)$.

Видели смо да су елиптички интеграли примери интеграла чијим се решавањем не добија увек елементарна функција[25)]. Ову чињеницу су доказали Абел и Лиувил[26)]. Уколико се решавањем елиптичких интеграла добија елементарна функција, називамо их *псеудоелиптичким интегралима*. Показано је да се сваки елиптички интеграл може изразити помоћу елементарних функција и интеграла облика

$$\int \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}, \int \frac{x^2dx}{\sqrt{(1-x^2)(1-k^2x^2)}}, \int \frac{dx}{(1+hx^2)\sqrt{(1-x^2)(1-k^2x^2)}} \tag{4.27}$$

при чему је k из $(0, 1)$, а параметар h може имати и комплексне вредности. Називамо их *елиптичким интегралима*, редом, *прве*, *друге* и *треће врсте*[27)]. Сменом $x = \sin\varphi$, φ из $[0, \frac{\pi}{2}]$, Лежандр је интеграле (4.27) свео на облике

$$\int \frac{d\varphi}{\sqrt{1-k^2\sin^2\varphi}}, \int \sqrt{1-k^2\sin^2\varphi}\, d\varphi, \int \frac{d\varphi}{(1+h\sin^2\varphi)\sqrt{1-k^2\sin^2\varphi}} \tag{4.28}$$

које називамо *елиптичким интегралима у Лежандровом облику*, редом, *прве*, *друге* и *треће врсте*.

Ако у сваком од интеграла (4.27) и (4.28) ставимо нулу за доњу границу интеграције, добијамо *одређене елиптичке интеграле* у *Јакобијевом*, односно *тригонометријском облику*, тим редом:

$$F(k, x) = \int_0^x \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}, \quad F(k, \varphi) = \int_0^\varphi \frac{d\psi}{\sqrt{1-k^2\sin^2\psi}}; \tag{4.29}$$

$$E(k, x) = \int_0^x \frac{t^2dt}{\sqrt{(1-t^2)(1-k^2t^2)}}, \quad E(k, \varphi) = \int_0^\varphi \sqrt{1-k^2\sin^2\psi}\, d\psi; \tag{4.30}$$

[25)] У општем случају, интеграли облика $\int R(x, \sqrt{P(x)})dx$, где је R рационална функција, а P полином степена већег од два нису елементарне функције

[26)] Жозеф Лиувил (Joseph Liouville, 1809–1882), француски математичар

[27)] или првог, другог и трећег реда

$$\begin{aligned}\Pi(h,k,x) &= \int_0^x \frac{dt}{(1+ht^2)\sqrt{(1-t^2)(1-k^2t^2)}},\\ \Pi(h,k,\varphi) &= \int_0^\varphi \frac{d\psi}{(1+h\sin^2\psi)\sqrt{1-k^2sin^2\psi}};\end{aligned} \tag{4.31}$$

при чему је k из $(0,1)$, x из $[0,1]$ и φ из $[0,\frac{\pi}{2}]$. Називамо их *непотпуним елиптичким интегралима*, редом, *прве*, *друге* и *треће врсте*. У тригонометријском облику непотпуних елиптичких интеграла, аргумент φ називамо *амплитудом елиптичког интеграла*.

Ако у интеграле (4.29), (4.30) и (4.31) ставимо да x, односно φ узимају највећу вредност из сегмента $[0,1]$, односно $[0,\frac{\pi}{2}]$, то јест ставимо да је $x=1$, односно $\varphi=\frac{\pi}{2}$, добијамо *потпуне елиптичке интеграле*, редом, *прве*, *друге* и *треће врсте*:

$$K = K(k) = \int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}} = \int_0^{\frac{\pi}{2}} \frac{d\psi}{\sqrt{1-k^2\sin^2\psi}},$$

$$E = E(k) = \int_0^1 \frac{t^2dt}{\sqrt{(1-t^2)(1-k^2t^2)}} = \int_0^{\frac{\pi}{2}} \sqrt{1-k^2\sin^2\psi}\,d\psi,$$

$$\Pi = \Pi(h,k) = \int_0^1 \frac{dt}{(1+ht^2)\sqrt{(1-t^2)(1-k^2t^2)}} = \int_0^{\frac{\pi}{2}} \frac{d\psi}{(1+h\sin^2\psi)\sqrt{1-k^2\sin^2\psi}}.$$

Сада лако уочавамо да се обим елипсе

$$O = 4a\int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}} - 4ak^2\int_0^1 \frac{t^2dt}{\sqrt{(1-t^2)(1-k^2t^2)}}.$$

може изразити као разлика

$$O = 4aK(k) - 4ak^2E(k).$$

потпуног елиптичког интеграла прве врсте $K(k)$ помноженог са $4a$ и потпуног елиптичког интеграла друге врсте $E(k)$ помноженог са $4ak^2$. Вредности за $K(k)$ и $E(k)$, у зависности од k, читамо из табела, и тако одређујемо тражени обим O дате елипсе.

Пошто се елиптички интеграли не могу изразити као елементарне функције, математичари их, у савременом приступу, третирају као нове функције. Отуда и дефиниција:

Дефиниција 4.26. *Елиптички интеграл* је функција f облика

$$f(x) = \int_c^x R(t, \sqrt{P(t)})dt$$

где је R рационална функција, P полином трећег или четвртог степена, а c константа.

Елиптички интеграл не можемо увек изразити помоћу елементарних функција, али га можемо увек изразити помоћу Вајерштрасове $\wp$-функције. Другим речима, елиптичке интеграле, у општем случају, не можемо рационалисати рационалним функцијама него то радимо помоћу елиптичких функција. Улога Вајерштрасове $\wp$-функције код елиптичких интеграла аналогна је улози функције *синус* или *косинус* код рачунања интеграла код којих се испод корена јављају полиноми другог степена. Та аналогија потиче отуда што су тригонометријске функције специјалан случај елиптичких функција.

• Јакобијеве елиптичке функције

Осим Вајерштрасове $\wp$-функције, постоје и друге важне елиптичке функције.

Дефиниција 4.27. Функцију инверзну непотпуном елиптичком интегралу прве врсте

$$z = F(k, x) = \int_0^x \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}, \tag{4.32}$$

где је k реална константа, $|k| \leq 1$, називамо *елиптичком синусном функцијом*, а k њеним *елиптичким модулом*, и означавамо је са

$$x = \mathrm{sn}(z) = \mathrm{sn}(z; k)^{28)}.$$

Надаље, када год то не доводи до забуне, уместо $\mathrm{sn}(z)$ писаћемо само $\mathrm{sn}\, z$.

На основу претходне дефиниције можемо рећи да је елиптичка синусна функција sn везана за инверзију елиптичког интеграла (4.32), то јест она се појављује у односу на тај елиптички интеграл.[29)]

Функција sn је двопериодична са периодима

$$4\int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}} \quad \text{и} \quad 2i\int_1^{\frac{1}{k}} \frac{dt}{\sqrt{(t^2-1)(1-k^2t^2)}}$$

и непарна, то јест важи

$$\mathrm{sn}(-z) = -\mathrm{sn}(z)$$

[28)] Функцију sn читамо *ес-ен* или *сен*.

[29)] Слично, $y = \sin x$ се појављује као инверзна функција интеграла $x = \int_0^y \frac{dt}{\sqrt{1-t^2}}$.

за свако z.

Помоћу елиптичке синусне функције sn увешћемо још две елиптичке функције

$$\operatorname{cn} z = \sqrt{1 - \operatorname{sn}^2 z}, \quad \operatorname{dn} z = \sqrt{1 - k^2 \operatorname{sn}^2 z}.$$

Прву од њих, cn[30)], називамо *елиптичком косинусном функцијом*, а другу, dn[31)], *делта амплитудно*. Целокупна класична теорија елиптичких функција може се свести на проучавање ове три елиптичке функције и њихових комбинација, па зато кажемо да су sn, cn и dn *основне елиптичке функције*. Називамо их и *Јакобијевим елиптичким функцијама*. Веза између Јакобијевих елиптичких функција дата је релацијама

$$\operatorname{sn}^2 z + \operatorname{cn}^2 z = 1, \quad k^2 \operatorname{sn}^2 z + \operatorname{dn}^2 z = 1,$$

од којих је прва иста као и релација која изражава везу између тригонометријских функција синус и косинус. Може се показати да су функције $x = \operatorname{cn} z$ и $x = \operatorname{dn} z$ инверзне, редом, интегралима

$$z = \int_x^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2+k^2t^2)}} \quad \text{и} \quad z = \int_x^1 \frac{dt}{\sqrt{(1-t^2)(t^2+k^2-1)}}.$$

Ако у једнакост (4.32) ставимо да је вредност елиптичког модула $k = 0$, добијамо да се интеграл

$$z = \int_0^x \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}$$

који дефинише функцију $x = \sin z$ своди на интеграл

$$z = \int_0^x \frac{dt}{\sqrt{1-t^2}} = \arcsin x,$$

а одговарајућа инверзна функција $\operatorname{sn} z$ се своди на $\sin z$. Слично се функција $\operatorname{cn} z$ своди на $\cos z$, а функција $\operatorname{dn} z$ на 1, па су тригонометријске функције, заиста, специјалан случај – за $k = 0$ – елиптичких функција. Због тога, Јакобијеве елиптичке функције sn, cn и dn, тим редом, називамо и *псеудо-синус*, *псеудо-косинус* и *псеудо-полупречник*, као аналогију на чињеницу да су тригонометријске функције синус и косинус дефинисане на тригонометријском кругу полупречника 1.

На крају, напоменимо да смо елиптичку синусну функцију sn могли да дефинишемо и као функцију инверзну непотпуном елиптичком интегралу прве врсте

$$z = F(k, \varphi) = \int_0^{\varphi} \frac{d\psi}{\sqrt{1 - k^2 \sin^2 \psi}}.$$

[30)] Функцију cn читамо *це-ен* или *кен*.

[31)] Функцију dn читамо *де-ен* или *ден*.

У специјалном случају, када је $k = 0$, добијамо да је $z = \varphi$. Променљиву φ називамо *амплитудом* променљиве z, означавамо је са

$$z = \operatorname{am} \varphi.$$

Ако је $k = 0$ важи $\sin z = \sin \varphi$ и $\cos z = \cos \varphi$, а за $k \neq 0$ елиптичке функције $\operatorname{sn} z$ и $\operatorname{cn} z$ означавао, редом, са $\sin(\operatorname{am} \varphi)$ и $\cos(\operatorname{am} \varphi)$. Називамо их *синус амплитудни* и *косинус амплитудни*. Ознаке $\sin(\operatorname{am} \varphi)$ и $\cos(\operatorname{am} \varphi)$ су претходиле ознакама $\operatorname{sn} z$ и $\operatorname{cn} z$.

• Дирихле о елиптичким функцијама

На крају, наведимо шта је Дирихле[32)] 1852. године рекао о елиптичким функцијама.

„Док су претходни истраживачи у овој области елиптички интеграл прве врсте посматрали као функцију његове горње границе, Абел и Јакоби су независно један од другог – иако први неколико месеци раније – схватили неопходност да се посматрање обрне, то јест да се границе и још две једноставне величине које су тако неразложиво са њима повезане – као што синус припада косинусу – разматрају као функције интеграла; управо као што се раније дошло до сазнања о најважнијим особинама трансцендената које зависе од круга посматрањем синуса и косинуса као функције лука, а не посматрањем лука као функција синуса и косинуса. Још веће значење је имала друга, за Абела и Јакобија заједничка идеја, да се у теорију уведу комплексни бројеви.”

[32)] Јохан Петер Густав Лежен Дирихле (Johann Peter Gustav Lejeune Dirichlet, 1805–1859), немачки математичар

5

Тангентно-тетивни закон

Елиптичке криве имају једно важно својство. На њима се – на природан начин – може увести операција уз коју оне постају Абелове групе. То је и један од најлепших примера групе у математици, и један од централних резултата Теорије елиптичких кривих. Ту операцију увешћемо помоћу тангенто-тетивног закона. Њему је посвећено ово поглавље, уз напомену да ћемо све илустрације у вези са тим приказати над пољем $\mathbb{R}$, иако све што радимо важи и над било којим другим пољем. Опширније у [14], [17], [15], [48] и [57].

5.1 Сабирање тачака на елиптичкој кривој

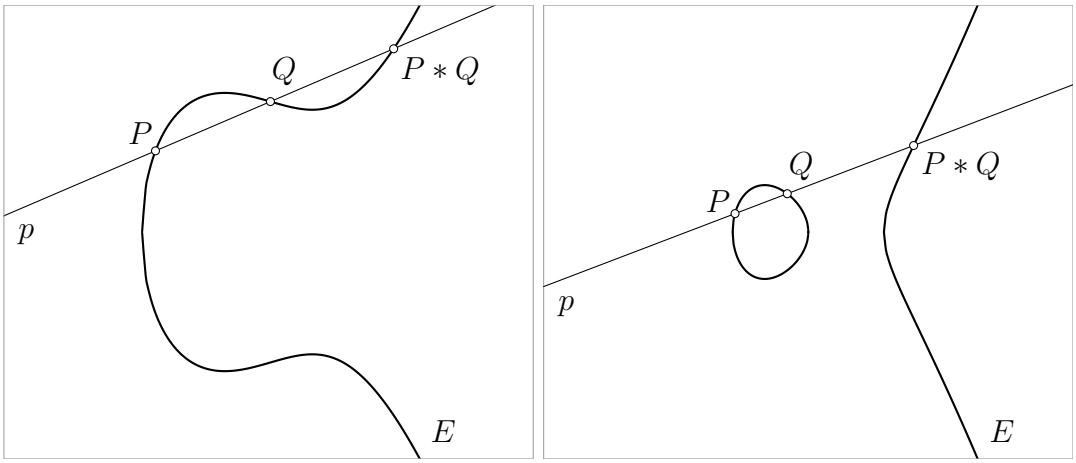
• Композиција тачака

У претходном поглављу видели смо да свака права сече Вајерштрасову кубну криву у тачно три тачке, рачунајући вишеструкости. С обзиром да су елиптичке криве посебна врста Вајерштрасових кубних кривих, ова геометријска особина је од фундаменталног значаја и за елиптичке криве, то јест важи:

> Свака права сече елиптичку криву у тачно три тачке, рачунајући вишеструкости.

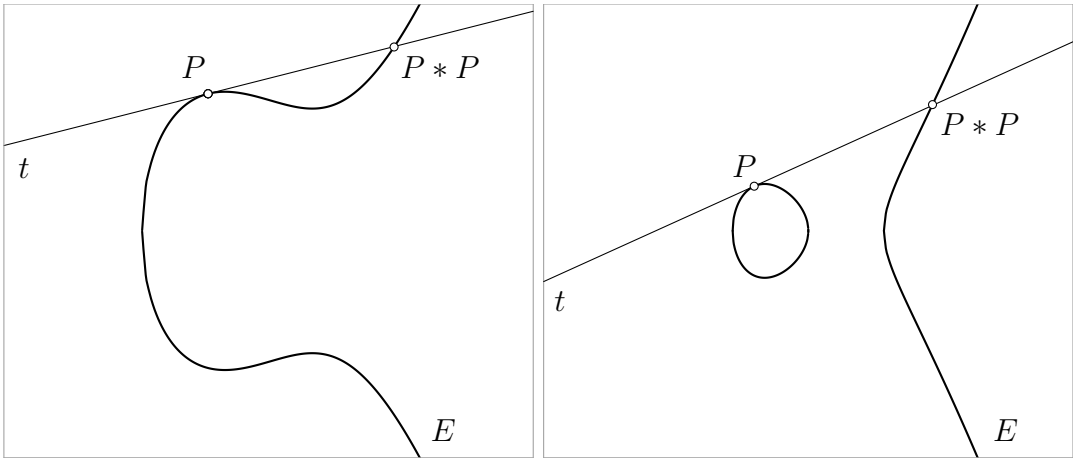
То значи да права која садржи две – не нужно различите – тачке елиптичке криве сече ту криву у још једној тачки. То нам омогућава да геометријски уведемо операције на елиптичкој кривој, [21, страна 234].

Дефиниција 5.1. Нека су P и Q две различите тачке на елиптичкој кривој E и нека је p права одређена тим тачкама. Трећу пресечну тачку праве p и елиптичке криве E, не нужно различиту од P и Q, називамо *композицијом* тачака P и Q и означавамо са $P * Q$.



Уколико се тачке P и Q поклапају, тада говоримо о композицији $P * P$ тачке P са самом собом. Конструкцијом тангенте t на елиптичку криву кроз P, конструисали смо, слободније речено, праву кроз P и P, јер тачка додира тангенте и криве има вишеструкост пресека 2. Отуда и следећа дефиниција, [21, страна 234]:

Дефиниција 5.2. Нека је P тачка на елиптичкој кривој E и нека је t тангента на E у тој тачки. Тада *композицију* $P * P$ дефинишемо као трећу пресечну тачку тангенте t и елиптичке криве E.



Дакле, за сваке две тачке P и Q са елиптичке криве E можемо дефинисати трећу тачку $P * Q$ која такође припада тој кривој.

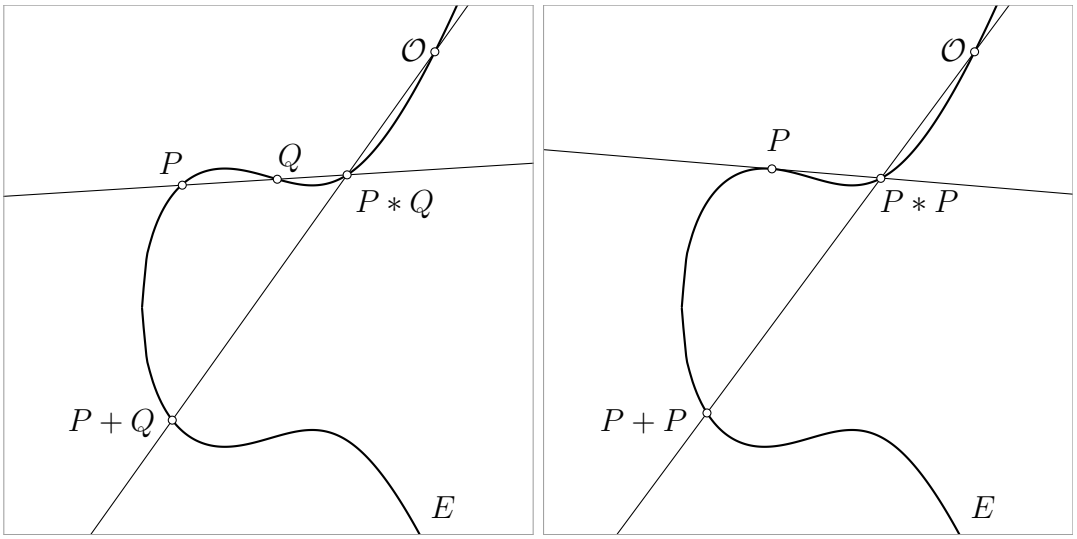
Надаље, приликом графичких илустрација, када је то довољно, приказиваћемо само елиптичке криве које се састоје од једне компоненте.

• Збир тачака

Посматрајмо структуру $(E, *)$. Та структура није група, јер немамо неутрал у односу на $*$. Међутим, ако фиксирамо произвољну тачку $\mathcal{O}$ на елиптичкој кривој E – коју ћемо сматрати неутралом – и на други начин дефинишемо операцију на E, [49, страна 12], добићемо структуру групе. Штавише, $(E, +)$ ће бити и Абелова група.

Дефиниција 5.3. Нека су P и Q две произвољне тачке на елиптичкој кривој E на којој је фиксирана тачка $\mathcal{O}$. Тада *збир* $P+Q$ *тачака* P и Q на елиптичкој кривој E дефинишемо као

$$P + Q = \mathcal{O} * (P * Q). \tag{5.1}$$



Дакле, помоћу тангенте и сечице, односно тангенте и тетиве, за сваке две тачке P и Q са елиптичке криве E можемо одредити трећу њену тачку $P+Q$. Зато кажемо да смо на елиптичкој кривој E геометријски увели операцију $+$ сабирања тачака помоћу *тангентно-тетивног* закона.

Посматрајмо, тачке P, Q и $P * Q$. Оне припадају елиптичкој кривој E, колинеарне су, и њихов збир је једнак неутралном елементу $\mathcal{O}$. Заиста,

$$P + Q + P * Q = (P + Q) + P * Q = \mathcal{O} * ((P + Q) * (P * Q)) = \mathcal{O} * \mathcal{O} = \mathcal{O}.$$

Ако тачку $P*Q$ означимо са R, тада је $P+Q+R = \mathcal{O}$ за неке три колинеарне тачке P, Q и R. Слично, ако, тачку $P*P$ означимо са S, тада је и $P+P+S = \mathcal{O}$.

Операцију $+$ сабирање тачака на елиптичкој кривој можемо да уведемо, уместо дефиницијом (5.3), помоћу наредне дефиниције, [33, страна 10].

Дефиниција 5.4. Три тачке P, Q и R на елиптичкој кривој E су *колинеарне* ако и само ако је $P + Q + R = \mathcal{O}$.

5.2 Структура групе на елиптичкој кривој

• Кејли-Бахарахова теорема

Да бисмо доказали да је $(E, +)$ Абелова група, потребна нам је Кејли[1)]-Бахарахова[2)] теорема која говори о пресеку кубних кривих, [20, страна 301].

[1)] Артур Кејли (Arthur Cayley, 1821–1895), британски математичар

[2)] Исак Бахарах (Isaak Bacharach, 1854–1942), немачки математичар јеврејског порекла

Теорема 5.1. [**Кејли-Бахарах**] Нека су $\mathcal{C}_1$ и $\mathcal{C}_2$ две кубне криве у пројективној равни $\mathbb{P}^2(\mathbb{K})$ које се секу у 9 тачака, рачунајући вишеструкости. Нека је $\mathcal{C}$ трећа кубна крива која пролази кроз 8 од 9 поменутих тачака пресека. Тада $\mathcal{C}$ пролази и кроз девету пресечну тачку.

Скица доказа. Општа једначина кубне криве је задата једначином

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$

која је збир 10 чланова, па је она одређена са 10 коефицијената. Ако помножимо све ове коефицијенте не-нула константом, добијена једначина дефинисаће исту криву. Зато је скуп свих могућих кубних кривих 9-димензионалан над пољем $\mathbb{K}$. Ако желимо да кубна крива пролази кроз неку тачку (x_0, y_0) чије су координате фиксиране, то нам намеће један линеарни услов

$$ax_0^3 + bx_0^2y_0 + cx_0y_0^2 + dy_0^3 + ex_0^2 + fx_0y_0 + gy_0^2 + hx_0 + iy_0 + j = 0$$

који коефицијенти $a, b, c, d, e, f, g, h, i, j$ треба да задовољавају. Тако добијамо да је скуп свих кубних кривих које садрже неку фиксирану тачку 8-димензионалан.

Дакле, сваки пут када задамо услов да кубна крива садржи неку тачку, имамо један додатни линеарни услов за коефицијенте. Тако добијамо да је фамилија свих кубних кривих које пролазе кроз 8 пресечних тачака кривих $\mathcal{C}_1$ и $\mathcal{C}_2$ заправо једнодимензионална фамилија.

Нека су $\mathcal{C}_1 : f_1(x, y) = 0$ и $\mathcal{C}_2 : f_2(x, y) = 0$ две кубне криве. Тада можемо наћи кубне криве које пролазе кроз 8 заједничких тачака кривих $\mathcal{C}_1$, $\mathcal{C}_2$ и $\mathcal{C}$ тако што ћемо узети линеарне комбинације $\lambda_1 f_1(x, y) + \lambda_2 f_2(x, y)$, при чему је бар један од бројева λ_1 и λ_2 различит од нуле. Морамо имати на уму да још увек не знамо да ли се међу овим линеарним комбинацијама налазе све кубне криве које садрже 8 поменутих тачака пресека.

Међутим, на основу претходног разматрања, знамо да је фамилија свих кубних кривих које садрже ових 8 пресечних тачака једнодимензионална. Са друге стране, фамилија $\lambda_1 f_1(x, y) + \lambda_2 f_2(x, y)$ је такође једнодимензионална. Иако видимо 2 параметра λ_1 и λ_2, једначину $\lambda_1 f_1(x, y) + \lambda_2 f_2(x, y) = 0$ можемо поделити са једним од њих – пошто је бар један различит од нуле – при чему ће добијена једначина описивати исту криву. То значи да заправо имамо један параметар.

Дакле, сада закључујемо да фамилија $\lambda_1 f_1(x, y) + \lambda_2 f_2(x, y)$ описује све кубне криве које пролазе кроз 8 заједничких тачака кривих $\mathcal{C}_1$, $\mathcal{C}_2$ и $\mathcal{C}$. То значи да и крива $\mathcal{C}$ има једначину $\lambda_1 f_1(x, y) + \lambda_2 f_2(x, y) = 0$ за неки избор константи λ_1, λ_2. Сада, пошто се девета тачка налази и на кривој $\mathcal{C}_1$ и на кривој $\mathcal{C}_2$, следи да је и $f_1(x, y) = 0$ и $f_2(x, y) = 0$ у тој тачки. Дакле, мора и $\lambda_1 f_1(x, y) + \lambda_2 f_2(x, y) = 0$ у тој тачки, што управо значи да и крива $\mathcal{C}$ садржи ту тачку.

Претходна теорема позната је и као *принцип «осам на три»*, и можемо је исказати и на следећи начин, [11, страна 254]:

Теорема 5.1. [Принцип «осам на три»] Ако три кубне криве у $\mathbb{P}^2(\mathbb{K})$ имају 8 заједничких тачака, тада оне имају још једну заједничку тачку. □

• Структура Абелове групе

Према [33, страна 13] имамо следећу теорему.

Теорема 5.2. Структура $(E, +)$ је Абелова група чији је неутрал $\mathcal{O}$ фиксирана тачка из E.

Доказ. Све аксиоме Абелове групе, осим асоцијативности, се лако доказују, па ћемо, због тога, асоцијативност оставити за крај доказа.

Нека су P и Q две произвољне тачке на елиптичкој кривој E. На основу дефиниције композиције тачака $*$, прво закључујемо да је на E и тачка $P*Q$, а затим да исто важи и за тачку $\mathcal{O}*(P*Q)$, јер је и $\mathcal{O}$ на E. Дакле, на елиптичкој кривој E је и тачка $P + Q = \mathcal{O} * (P * Q)$, па је елиптичка крива E затворена у односу на операцију $+$ сабирање тачака. Та операција је и комутативна јер важи

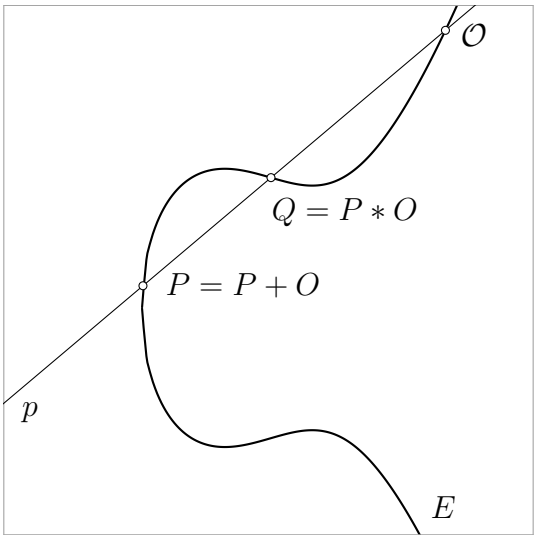
$$P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P$$

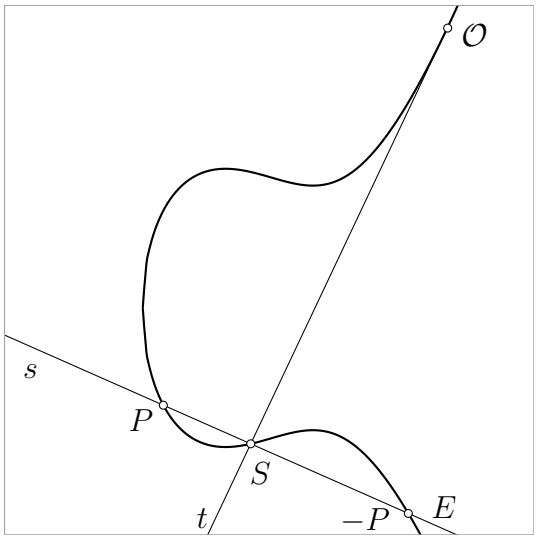
због тога што $P * Q$ и $Q * P$ представљају исту тачку на елиптичкој кривој E.

Докажимо да је тачка $\mathcal{O}$ неутрал у односу на операцију $+$, то јест да је $P + \mathcal{O} = P$ за сваку тачку P на E. Нека је P произвољна тачка, p права одређена тачкама P и $\mathcal{O}$ и нека је Q трећа пресечна тачка праве p и елиптичке криве E. Наравно, ако је p тангента на криву E, тачке P, Q и $\mathcal{O}$ не морају бити различите. Тада је

$$P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) = \mathcal{O} * Q = P$$

па је тачка $\mathcal{O}$ из E неутрал за операцију $+$.





Докажимо да свака тачка P на E има инверз у односу на операцију $+$. Нека је P произвољна тачка, t тангента на криву E у тачки $\mathcal{O}$ и S друга пресечна тачка праве t и криве E. Означимо са s праву одређену тачкама P и S. Покажимо да је инверз тачке P трећа пресечна тачка праве s и криве E, то јест да је $-P = P * S$. Како је

$$P + (-P) = P + (P * S) = \mathcal{O} * (P * (P * S)) = \mathcal{O} * S = \mathcal{O}$$

тачка $-P = P * S$ је заиста инверз тачке P, па за сваку тачку P на E постоји њен инверз, тачка $-P$.

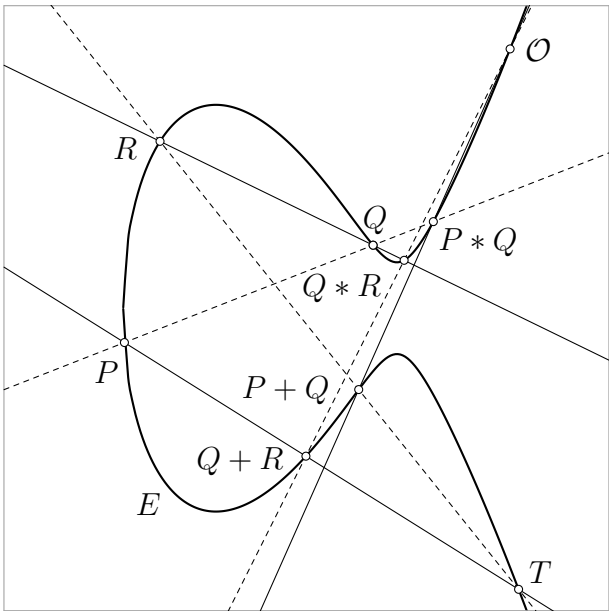
Докажимо да је операција $+$ и асоцијативна. Нека су P, Q и R три произвољне тачке на елиптичкој кривој E. Треба доказати да важи

$$(P + Q) + R = P + (Q + R),$$

то јест $O * ((P + Q) * R) = O * (P * (Q + R))$, односно

$$(P + Q) * R = P * (Q + R).$$

Приметимо да свака од тачака O, P, Q, R, $P * Q$, $P + Q$, $Q * R$ и $Q + R$ припада једној правој која је представљена пуном линијом и једној правој која је представљена испрекиданом линијом.



Посматрајмо тачку T која је пресечна тачка праве одређене тачкама $P + Q$ и R и праве одређене тачкама P и $Q + R$. Докажимо да та тачка T припада и елиптичкој кривој E.

Свака права је описана линеарном једначином, а три праве су одређене једначином коју добијамо множењем три линеарне једначине, а то је једначина трећег степена. Као што смо видели, таква једначина одређује једну кубну криву. Због тога, можемо сматрати да три праве које су представљене пуном

линијом, односно три праве које су представљене испрекиданом линијом одређују две дегенерисане кубне криве $\mathcal{C}_1$, односно $\mathcal{C}_2$. Оне садрже свих девет поменутих тачака, по конструкцији. Елиптичка крива E је кубна крива која садржи осам од тих девет тачака – све тачке осим тачке T. Према теореми 5.1 она мора да садржи и девету тачку, то јест тачку T. Дакле, тачка T такође припада елиптичкој кривој E. Како је она пресек правих које су одређене тачкама $P+Q$ и R, односно P и $Q+R$, важи

$$(P+Q)*R = P*(Q+R).$$

Одавде закључујемо да важи и $O*((P+Q)*R) = O*(P*(Q+R))$, то јест

$$(P+Q)+R = P+(Q+R),$$

па је операција $+$ и асоцијативна на E. Дакле, структура $(E,+)$ је једна Абелова група. □

Нека је $E/\mathbb{K}$ елиптичка крива и $E(\mathbb{K})$ скуп свих њених $\mathbb{K}$-тачака. Тада, на основу претходне теореме (5.2), важи:

Теорема 5.3. Скуп

$$E(\mathbb{K}) \cup \{\mathcal{O}\}$$

је једна подгрупа од $E/\mathbb{K}$. □

Овом теоремом успостављамо структуру Абелове групе и на скупу $E(\mathbb{K})$. То ће нам посебно помоћи приликом даљег испитивања тог скупа.

5.3 Експлицитне формуле за сабирање тачака

Раније смо напоменули, а и види се из дефиниција (5.1), (5.2) и (5.3) да смо композицију, односно збир тачака на елиптичкој кривој дефинисали геометријски. Збир тачака можемо алгебарски представити помоћу експлицитних формула. Пре него што то покажемо, подсетимо се и утврдимо неке чињенице у вези са елиптичким кривама које ће нам за то бити потребне.

Нека је елиптичка крива задата афином

$$y^2 = x^3 + ax + b, \tag{5.2}$$

односно пројективном једначином

$$Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{5.3}$$

Заменом $Z = 0$ у (5.3) добијамо једначину $X^3 = 0$, која има троструки корен $X = 0$. То значи да елиптичка крива и бесконачно далека права имају троструки пресек у једној, бесконачно далекој тачки. Узмимо ову бесконачно далеку тачку да буде наша тачка $\mathcal{O}$ – која има улогу неутрала у групи

на елиптичкој кривој. Сада можемо сматрати да се елиптичка крива састоји од «обичних» тачака у афиној равни, укључујући још само једну додатну, бесконачно далеку тачку $\mathcal{O}$, коју не можемо видети у тој афиној равни.

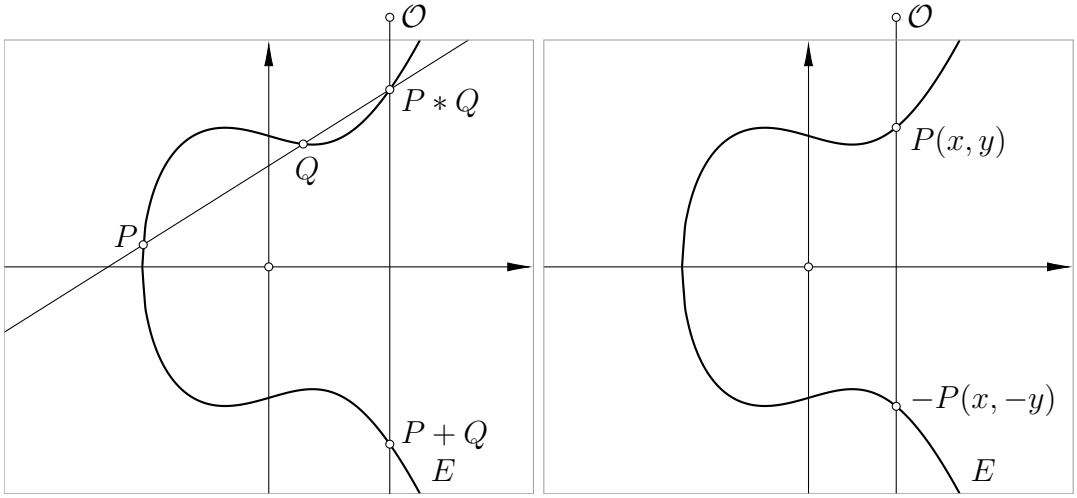
Дакле, с обзиром да свака права сече елиптичку криву у тачно три тачке, рачунајући вишеструкости, можемо закључити следеће:

- бесконачно далека права сече елиптичку криву у бесконачно далекој тачки $\mathcal{O}$ – троструки пресек,
- вертикална права сече елиптичку криву у две «обичне» тачке и у бесконачно далекој тачки $\mathcal{O}$,
- невертикална права сече елиптичку криву у три «обичне» тачке.

Ове чињенице нам омогућавају да сабирање тачака у афиној равни $\mathbb{K}^2$ алгебарски представимо помоћу експлицитних формула.

• Сабирање тачака над пољем $\mathbb{R}$

Алгебарску дефиницију збира тачака на елиптичкој кривој E показаћемо у афиној равни $\mathbb{R}^2$. Нека су P и Q две тачке на E. Да бисмо одредили $P+Q$ прво треба да одредимо тачку $P*Q$, која се добија као трећа пресечна тачка праве одређене тачкама P и Q и елиптичке криве E. Даље, права кроз $P*Q$ и $\mathcal{O}$ је вертикална права кроз $P*Q$, јер је $\mathcal{O}$ бесконачно далека тачка и она припада свакој вертикалној правој. Пошто је елиптичка крива у Вајерштрасовом нормалном облику симетрична у односу на x-осу, тачку $P+Q$ ћемо добити када тачку $P*Q$ пресликамо осном симетријом у односу на x-осу.



Нека је $P=(x,y)$ тачка на елиптичкој кривој E. Покажимо да је њен инверз тачка $-P=(x,-y)$, то јест да је $P+(-P)=\mathcal{O}$. Прво одредимо тачку $P*(-P)$. Права кроз P и $-P$ је вертикална, па је трећа пресечна тачка те праве са E тачка $\mathcal{O}$. Тачка $P+(-P)$ је трећа пресечна тачка праве која садржи $\mathcal{O}$ и $P*(-P)$, то јест $\mathcal{O}$ и $\mathcal{O}$. Међутим, та права је у ствари тангента у тачки O, то јест, бесконачно далека права, па је њена трећа пресечна тачка са кривом E поново $\mathcal{O}$. Дакле, важи да је $P+(-P)=\mathcal{O}$.

Сада можемо извести ескплицитне формуле за сабирање тачака на елиптичкој кривој у афиној равни $\mathbb{R}^2$. Ту ће нам помоћи знање из аналитичке геометрије. Нека је $x(P)$ ознака за x-координату тачке P, а $y(P)$ ознака за њену y-координату. У следећој теореми ћемо одредити $x(P+Q)$ и $y(P+Q)$, при чему су P и Q тачке на елиптичкој кривој E. Размотрићемо случај када је $P \neq Q$, а затим и $P = Q$, [49, страна 25].

Теорема 5.4. Нека су $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ тачке на елиптичкој кривој E датој у Вајерштрасовом нормалном облику $y^2 = x^3 + ax + b$, где је $P \neq \pm Q$ и ниједна од тачака P и Q није бесконачно далека тачка $\mathcal{O}$. Тада је

$$x(P+Q) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 + x_2), \tag{5.4}$$

$$y(P+Q) = -\frac{y_2 - y_1}{x_2 - x_1} x(P+Q) - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}. \tag{5.5}$$

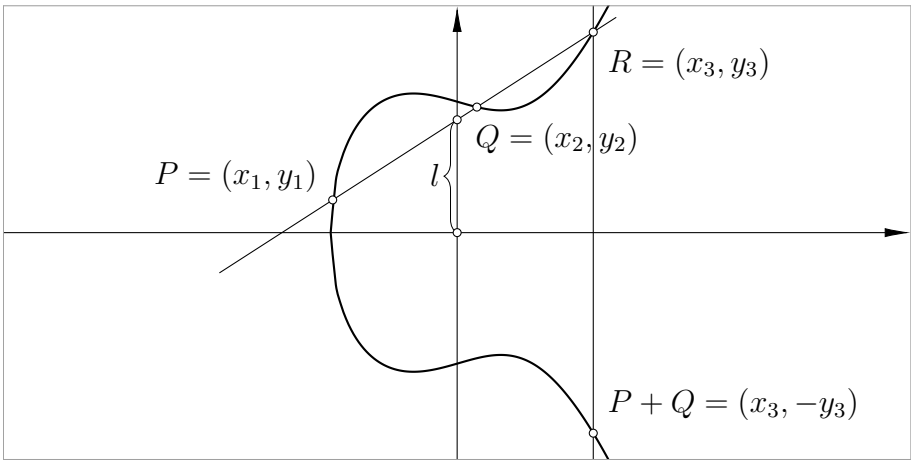
Ако је $P(x_1, y_1) \neq \mathcal{O}$ и $y_1 \neq 0$, тада је

$$x(P+P) = x(2P) = \frac{(3x_1^2 + a)^2}{4(x_1^3 + ax_1 + b)} - 2x_1, \tag{5.6}$$

$$y(P+P) = y(2P) = -\frac{3x_1^2 + a}{2y_1} x(2P) - \frac{2y_1^2 - x_1(3x_1^2 + a)}{2y_1}. \tag{5.7}$$

Доказ. Да бисмо одредили $x(P+Q)$, прво нађимо једначину праве кроз P и Q:

$$y = \frac{y_2 - y_1}{x_2 - x_1} x + l. \tag{5.8}$$



Затим, да бисмо нашли координату x_3 тачке $R = (x_3, y_3)$ која се добија у пресеку праве (5.8) са кривом $y^2 = x^3 + ax + b$, заменићемо y из једначине (5.8) у једначину $y^2 = x^3 + ax + b$. На тај начин добијамо једначину

$$x^3 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 x^2 + \left(a - 2l\frac{y_2 - y_1}{x_2 - x_1}\right) x + b - l^2 = 0. \tag{5.9}$$

Пошто су x_1, x_2 и x_3 три решења једначине (5.9), њена лева страна је

$$(x-x_1)(x-x_2)(x-x_3) = x^3 - (x_1+x_2+x_3)x^2 + (x_1x_2+x_1x_3+x_2x_3)x - x_1x_2x_3. \tag{5.10}$$

Упоређујући коефицијенте уз x^2 у једначинама (5.9) и (5.10) и имајући у виду да тачке R и $P+Q$ имају исту x-координату, добијамо

$$x(P+Q) = x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - (x_1+x_2).$$

Да бисмо добили y-координату тачке R, израчунаћемо l из једнакости (5.8). Пошто права (5.8) садржи тачку $P=(x_1,y_1)$, имамо

$$l = y_1 - \frac{y_2-y_1}{x_2-x_1}x_1 = \frac{y_1x_2-y_2x_1}{x_2-x_1}.$$

Сада, y-координату тачке R добијамо заменом добијених израза за x_3 и l у једначину (5.8), то јест

$$y_3 = \frac{y_2-y_1}{x_2-x_1}x_3 + \frac{y_1x_2-y_2x_1}{x_2-x_1}.$$

Формулу (5.5) добијамо имајући у виду да је y-координата тачке $P+Q$ симетрична тачки R у односу на x-осу, то јест $y(P+Q) = -y_3$. Дакле,

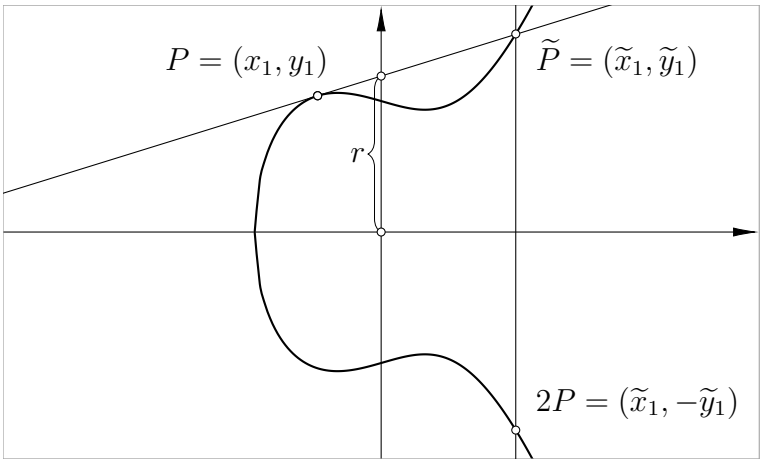
$$y(P+Q) = -y_3 = -\frac{y_2-y_1}{x_2-x_1}x(P+Q) - \frac{y_1x_2-y_2x_1}{x_2-x_1}.$$

Да бисмо одредили $x(2P)$, треба нам једначина тангенте на елиптичку криву E у тачки P. Помоћу извода имплицитно задате функције[3)] добијамо коефицијент правца тангенте у тачки P, па је једначина тангенте дата са

$$y = \frac{3x_1^2+a}{2y_1}x + r. \tag{5.11}$$

Нека је $\widetilde{P} = (\widetilde{x}_1, \widetilde{y}_1)$ тачка различита од P која се добија у пресеку тангенте (5.11) и елиптичке криве E.

[3)] Извод имплицитно задате функције $F(x,y)=0$ тражимо тако што једну промењиву – обично је то y – схватимо као функцију оне друге промењиве – обично је то x, то јест $y=y(x)$ – и диференцирамо обе стране једначине $F(x,y)=0$ користећи правило за извод сложене функције.



Координату $\widetilde{x}_1$ ћемо добити када у једначину $y^2 = x^3 + ax + b$ заменимо (5.11). Добијамо

$$x^3 - \frac{(3x_1^2 + a)^2}{4y_1^2}x^2 + \left(a - 2r\frac{3x_1^2 + a}{2y_1}\right)x + b - r^2 = 0. \tag{5.12}$$

Знамо да су x_1 и $\widetilde{x}_1$ решења једначине (5.12), при чему је решење x_1 вишеструкости 2, па из

$$(x - x_1)^2(x - \widetilde{x}_1) = x^3 - (2x_1 + \widetilde{x}_1)x^2 + (2x_1\widetilde{x}_1 + x_1^2)x - x_1^2\widetilde{x}_1,$$

упоређујући коефицијенте уз x^2 и имајући у виду да је $y_1^2 = x_1^3 + ax_1^2 + b$ добијамо

$$x(2P) = \widetilde{x}_1 = \frac{(3x_1^2 + a)^2}{4(x_1^3 + ax_1 + b)} - 2x_1.$$

Да бисмо добили y-координату тачке $\widetilde{P}$, треба да нађемо r из једначине тангенте (5.11). Пошто тангента (5.11) садржи тачку P, добијамо да је

$$r = y_1 - \frac{3x_1^2 + a}{2y_1}x_1 = \frac{2y_1^2 - x_1(3x_1^2 + a)}{2y_1}.$$

Сада $\widetilde{y}_1$ добијамо када r из претходне једнакости заменимо у једначину тангенте (5.11)

$$\widetilde{y}_1 = \frac{3x_1^2 + a}{2y_1}x(2P) + \frac{2y_1^2 - x_1(3x_1^2 + a)}{2y_1},$$

а формула (5.7) следи из једнакости $y(2P) = -\widetilde{y}_1$. Дакле,

$$y(P + P) = y(2P) = -\widetilde{y}_1 = -\frac{3x_1^2 + a}{2y_1}x(2P) - \frac{2y_1^2 - x_1(3x_1^2 + a)}{2y_1}. \qquad \square$$

Формуле (5.4) - (5.7) су алгебарска репрезентација сабирања тачака на елиптичкој кривој, то јест тангентно-тетивног закона помоћу кога вршимо то сабирање. Зато их називамо и *формулама тангентно-тетивног закона сабирања на елиптичким кривама.*

Добијене формуле важе и у случају било којег поља $\mathbb{K}$ чије је карактеристика различита од 2 и 3. Ако је поље карактеристике 2 или 3, формуле су сличне добијеним формулама уз мале модификације.

Уз помоћ формула тангентно-тетивног закона сабирања такође можемо установити и структуру групе на елиптичкој кривој. Међутим, испоставља се да је доказ асоцијативности тежи него што се чини на први поглед. Постоји много специјалних случајева које треба посебно испитати, на пример када је нека од тачака једнака $\mathcal{O}$, када је збир две тачке једнак $\mathcal{O}$, или када је збир две тачке једнак трећој, и слично. Штавише, за проверу неких идентитета је потребно неколико сати рада на модерном компјутеру, тако да овај доказ није ни био изведен пре 1980. године.

• Сабирање тачака над пољем $\mathbb{C}$

Покажимо, укратко, како сабирамо тачке на елиптичкој кривој

$$y^2 = 4x^3 + ax + b$$

над пољем $\mathbb{C}$. Видели смо да комплексне тачке на елиптичкој кривој $E/\mathbb{C}$ можемо параметризовали помоћу $(\wp(t), \wp'(t))$, јер важи

$$(\wp'(z))^2 = 4(\wp(z))^3 + a\wp(z) + b.$$

Нека су $P = (\wp(t), \wp'(t))$ и $Q = (\wp(u), \wp'(u))$ две тачке на $E/\mathbb{C}$. Тада је

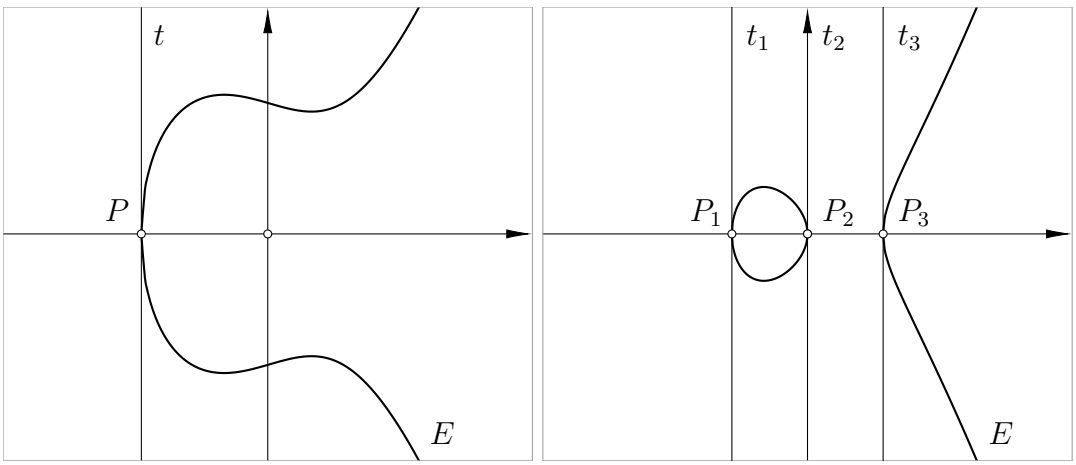
$$P + Q = (\wp(t+u), \wp'(t+u)),$$

па сабирање тачака на $E/\mathbb{C}$ одговара сабирању комплексних бројева. Познавање ове чињенице омогућава нам да елегантно докажемо асоцијативност сабирања тачака на елиптичкој кривој.

5.4 Тачке коначног реда

• Тачке реда 2

Посматрајмо тачке у којима елиптичка крива E сече x-осу.



У тим тачкама тангента је нормална на x-осу, то јест паралелна је y-оси. Ако такву тачку означимо са P, тада је

$$P + P = \mathcal{O} * (P * P) = \mathcal{O} * \mathcal{O} = \mathcal{O},$$

то јест

$$2P = \mathcal{O},$$

јер је трећа пресечна тачка те тангенте са елиптичком кривом бесконачно далека тачка $\mathcal{O}$. Поред ознаке $2P$ у употреби је и ознака $[2]P$, [16, 8. лекција, страна 1].

Дефиниција 5.5. Ако је P тачка елиптичке криве за коју је

$$2P = \mathcal{O}$$

тада ту тачку називамо *тачком реда* 2 или 2-*торзионом*[4] *тачком*.

За тачку P за коју је $2P = \mathcal{O}$, лако закључујемо да важи и

$$P = -P.$$

С друге стране, ако је $P(x, y)$ тачка реда два, тада је

$$(x, y) = (x, -y)$$

одакле следи да је $y = -y$, то јест $y = 0$. Дакле, тачке реда 2 елиптичке криве E су управо тачке са y-координатом једнаком 0. Таквих тачака на елиптичкој кривој можемо имати нула, једну или три.

• Тачке коначног и бесконачног реда. Ред тачке

Тачке реда 2 су примери тачака коначног реда или торзионих тачака. На основу [16, 8. лекција, страна 1], имамо и

Дефиниција 5.6. Тачку P елиптичке криве E за коју постоји природан број n такав да је

$$nP = \underbrace{P + P + \cdots + P}_{n} = \mathcal{O} \tag{5.13}$$

називамо *тачком коначног реда* или *торзионом тачком*. Најмању такву вредност броја n називамо *ред тачке* P.

Ред тачке елиптичке криве одговара стандардном реду елемента у некој групи. Због тога, тачке коначног реда елиптичке криве чине групу, то јест

$$\langle P \rangle = \{\mathcal{O}, P, 2P, \ldots, (n-1)P\}$$

[4] Реч *торзија* потиче од новолатинске речи *torsio* што у преводу значи *увртање*, *увијање*, *упредање*.

је циклична група n-тог реда са генератором P, која је изоморфна групи $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Ту групу можемо реализовати као скуп $\{0, 1, 2, \ldots, n-1\}$ уз сабирање $+_n$ по модулу n. Тачку $\mathcal{O}$ називамо *тривијалном торзионом тачком*.

Ако не постоји природан број n такав да важи (5.13), сви елементи низа

$$\mathcal{O}, P, 2P, 3P, \ldots$$

су различити. У том случају кажемо да је тачка P *бесконачног реда*. Тада је

$$\langle P \rangle = \{\ldots, -2P, -P, O, P, 2P, \ldots\}$$

бесконачна циклична група генерисана са P, односно $-P$, која је изоморфна групи $\mathbb{Z}$.

6

Елиптичке криве над пољем рационалних бројева

Видели смо да елиптичке криве можемо дефинисати над произвољним пољем $\mathbb{K}$. Један од најважнијих случајева – нарочито у теорији бројева – је за $\mathbb{K} = \mathbb{Q}$. Зато ово поглавље посвећујемо елиптичким кривама над пољем $\mathbb{Q}$ рационалних бројева. За више детаља погледати [33], [16], [48], [49] и [57].

6.1 Рационалне тачке и рационалне криве

• Рационална тачка. Рационална права

Нека је $\mathbb{R}^2$ реална раван. Тада имамо, [44, страна 1]:

Дефиниција 6.1. За тачку $P = (x, y)$ из $\mathbb{R}^2$ кажемо да је *рационална тачка* ако су обе њене координате x и y рационални бројеви.

Дефиниција 6.2. Права p из $\mathbb{R}^2$ је *рационална права* ако су у њеној једначини $ax + by + c = 0$ коефицијенти a, b и c рационални бројеви.

За рационалне тачке и рационалне праве важи, [44, страна 1]:

Ако су две тачке рационалне, тада је и њима одређена права рационална. Пресек две рационалне праве је рационална тачка.

Коефицијент правца рационалне праве је рационалан број $k = -\frac{b}{a}$, па уместо рационална права кажемо и *права рационалног нагиба*.

• Рационална крива. Рационална коника

У једном од ранијих поглавља, рационалну криву смо дефинисали као алгебарску криву рода $g = 0$. Сада ћемо рационалну криву дефинисати и овако, [44, страна 1]:

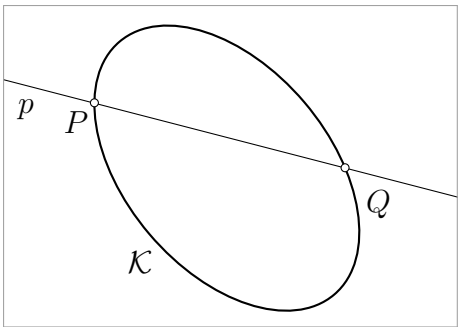
Дефиниција 6.3. Крива $\{(x, y) \mid f(x, y) = 0\}$, која одговара полиному f са две неодређене x и y, је *рационална крива* ако су сви коефицијенти полинома f рационални бројеви, то јест f припада $\mathbb{Q}[x, y]$.

Видели смо и да назив рационална крива потиче отуда што координате тачака које припадају тој кривој можемо изразити рационалним функцијама неког параметра, то јест она има параметризацију помоћу рационалних функција. Рационална коника је специјалан случај рационалне криве, [44, страна 1].

Дефиниција 6.4. Коника $ax^2 + bxy + cy^2 + dx + ey + f = 0$ је *рационална коника* ако су коефицијенти a, b, c, d, e и f рационални бројеви. Рационалну конику означаваћемо са $\mathcal{K}$.

• Рационална права и рационална коника

Нека је p рационална права и $\mathcal{K}$ рационална коника. У општем случају, постоје две тачке њиховог пресека, на пример P и Q, то јест $p \cap \mathcal{K} = \{P, Q\}$.



Координате пресечне тачке морају да задовољавају једначину праве p и једначину конике $\mathcal{K}$, али оне не морају бити рационалне. Другим речима, пресечне тачке рационалне праве и рационалне конике не морају бити рационалне тачке. Отуда и закључак:

Рационална коника не мора да садржи рационалну тачку.

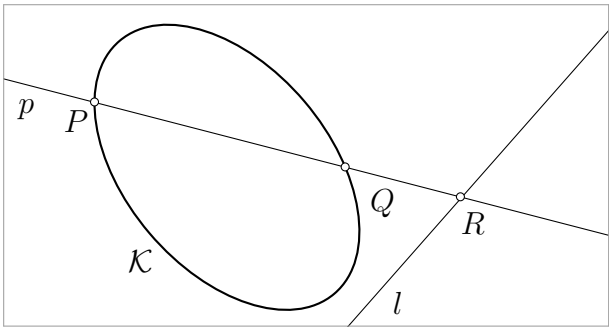
С друге стране, на основу Вијетових[1)] формула, важи следеће:

Ако је једна од пресечних тачака рационалне праве и рационалне конике рационална, тада и друга њихова пресечна тачка мора бити рационална.

[1)] Франсоа Вијет (François Viète, 1540–1603), француски математичар и правник

• Конструкција рационалних тачака

Претходно својство нам омогућава *конструкцију* помоћу које можемо одредити све рационалне тачке конике и тако је рационално параметризовати. Изаберимо једну рационалну тачку P на рационалној коници $\mathcal{K}$ и посматрајмо рационалну праву p која садржи тачку P и сече конику $\mathcal{K}$. Добијена пресечна тачка Q праве p и конике $\mathcal{K}$, према већ реченом, мора бити рационална.



Пресек те рационалне праве p и унапред фиксиране рационалне праве l је такође рационална тачка R. Називамо је *пројекцијом* тачке Q конике $\mathcal{K}$ на праву l.

Понављањем описане конструкције за било коју рационалну тачку Q успостављамо *бијекцију* између свих рационалних тачака Q конике $\mathcal{K}$ и унапред фиксиране рационалне праве l. Кажемо и да смо, тим поступком, рационалну конику $\mathcal{K}$ *пројектовали* на рационалну праву l.

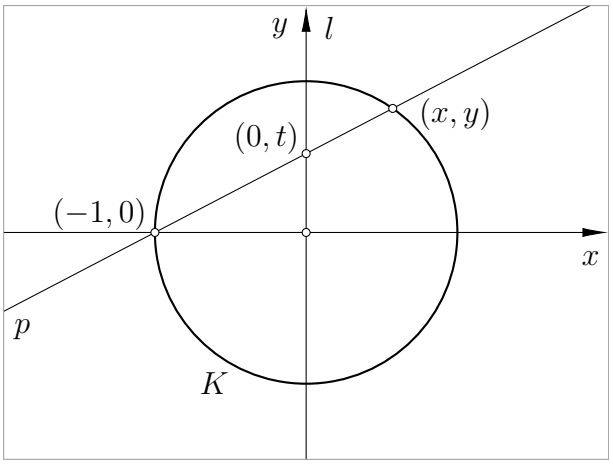
Дакле, ако рационална коника има једну рационалну тачку, тада можемо, описаним поступком, конструисати, то јест одредити све њене рационалне тачке.

• Рационална параметризација круга

Претходно речено применићемо на круг, то јест одредићемо све његове рационалне тачке. Нека је K јединични круг чија је једначина

$$K : x^2 + y^2 = 1. \tag{6.1}$$

Одредимо све његове рационалне тачке.



Коефицијенти у (6.1) су рационални бројеви, па је круг K рационалан. Применимо на њега претходно описану конструкцију, то јест успоставимо бијекцију између рационалних тачака круга K и неке фиксиране рационалне праве l. За рационалну тачку P изаберимо тачку $(-1,0)$, а за рационалну праву l узмимо y-осу. Друга пресечна тачка праве p и круга K је рационална тачка (x,y). Пројектујмо круг K на праву l, то јест на y-осу. Нека је тачка $(0,t)$ пројекција рационалне тачке (x,y) на y-осу. Једначина праве p кроз тачке $(-1,0)$ и $(0,t)$ је $y-0=\frac{t-0}{0-(-1)}(x-(-1))$, то јест

$$y=t(x+1). \tag{6.2}$$

Решавањем система (6.1) и (6.2) по x и y добијамо да је

$$y=t(x+1) \quad \text{и} \quad t^2(x+1)^2=(1-x)(1+x). \tag{6.3}$$

Једно решење система једначина (6.3) је тачка $P(-1,0)$. После скраћивања са $x+1$, уз услов да је $x+1\neq 0$, то јест $x\neq -1$[2)], и након сређивања, добијамо координате

$$x=\frac{1-t^2}{1+t^2}, \quad y=\frac{2t}{1+t^2}. \tag{6.4}$$

рационалне тачке (x,y) круга K која је различита од тачке $P(-1,0)$. Ако овим тачкама додамо тачку P добијамо све *рационалне тачке круга* K. Те тачке, то јест њихове координате, зависе само од броја t. Зато број t називамо *параметар*. Због тога кажемо да смо круг K *параметризовали* и да је једначинама (6.4) дата његова *рационална параметризација*[3)]. Једначине (6.4) називамо *параметарским једначинама круга* K.

Успостављење описане бијекције значи да се, са гледишта *Диофантове анализе*[4)], круг K и права l не разликују. Њихови одговарајући скупови рационалних тачака су еквивалентни без обзира што су њихови степени различити.

Видели смо, према теореми (3.6) да је скуп $\mathcal{C}(\mathbb{Q})$ рационалних тачака алгебарске криве $\mathcal{C}$ рода $g=0$ – рационалне криве – празан или бесконачан. С друге стране, теорема (3.7) Хасе-Минковски нам даје алгоритам помоћу кога утврђујемо да ли рационална крива има коначно много рационалних тачака. Управо приказани поступак нам илуструје како да одредимо све рационалне тачке такве криве ако знамо једну њену рационалну тачку, и на тај начин је рационално параметризујемо.

[2)] Овај услов је испуњен јер тражимо координате тачака које су различите од тачке $P(-1,0)$, па је $x\neq -1$.

[3)] то јест, једна од могућих рационалних параметризација, јер бисмо за избор неке друге тачке P добили другу параметризацију круга K

[4)] *Диофантова анализа* је део теорије бројева који изучава начине за решавање алгебарских једначина, или система оваквих једначина, са целим коефицијентима у целим или рационалним бројевима. У другој половини 20. века Диофантова анализа постала је модерна због повезаности са алгебарском геометријом.

• Питагорине тројке

Нека је K јединични круг чија је једначина

$$K : x^2 + y^2 = 1. \tag{6.5}$$

Ако у једначини (6.5) заменимо $x = \frac{X}{Z}$ и $y = \frac{Y}{Z}$, при чему су X, Y и Z природни бројеви, тада једначина (6.5), након множења са Z^2 прелази у

$$X^2 + Y^2 = Z^2. \tag{6.6}$$

Дефиниција 6.5. Једначину (6.6) називамо *Питагорина*[5] *Диофантова једначина* или краће *Питагорина једначина*.

Питагорина једначина је специјалан случај *опште квадратне Диофантове једначине*

$$X^2 + aXY + Y^2 = Z^2,$$

при чему је a из $\mathbb{Z}$. Настаје када у ту једначину ставимо да је $a = 0$. Питагорина једначина је посебно важна у *тригонометрији* и *аналитичкој геометрији*. Њен специјалан случај, за $X = Y$, то јест $X^2 + X^2 = Z^2$, односно

$$2X^2 = Z^2$$

је повезан са најједноставнијим доказом постојања *ирационалних бројева*.

Дефиниција 6.6. Уређену тројку (X, Y, Z) природних бројева X, Y и Z која задовољава Питагорину једначину називамо *Питагорина тројка*.

Дефиниција 6.7. Природне бројеве X, Y и Z који чине Питагорину тројку називамо *Питагорини бројеви*.

Кажемо и да је (X, Y, Z) [уређена] тројка Питагориних бројева. Проблем одређивања Питагориних бројева познат је као *Питагорин проблем*.

Питагорине бројеве можемо и геометријски схватити, то јест они имају и геометријску интерпретацију.

Дефиниција 6.8. Троугао чији су мерни бројеви страница природни бројеви који задовољавају Питагорину једначину називамо *Питагорин троугао*.

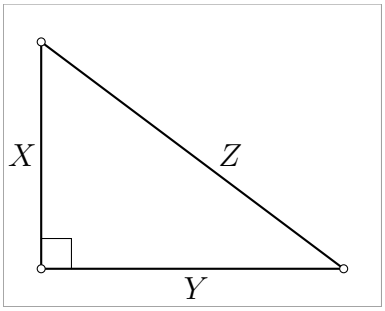
На основу обрата Питагорине теореме[6] такав троугао је правоугли. Отуда и

[5] Питагора (Πυθαγόρας, 580–500 пре нове ере), грчки математичар и фолозоф

[6] *Обрат Питагорине теореме*[7]: Ако је $AC^2 + BC^2 = AB^2$, тада је троугао ABC правоугли са правим углом код темена C.

[7] *Питагорина теорема*: Површина квадратне површи чија је ивица хипотенуза неког правоуглог троугла једнака је збиру површина двеју квадратних површи којима су ивице катете тог троугла. Другим речима, ако је угао код темена C троугла ABC прав, тада је $AC^2 + BC^2 = AB^2$. Питагорина теорема је једна од најзначајних теорема у математици и има много доказа – бар 365 до априла 1940 – и низ уопштења. Она представља и врхунац I књиге Еуклидових *Елемената*.

Дефиниција 6.9. Уређена тројка (X, Y, Z) природних бројева X, Y и Z је *Питагорина тројка*, ако су бројеви X и Y дужине катета, а Z дужина хипотенузе Питагориног троугла.



Интересовање за Питагорине бројеве потиче још од Вавилонаца – 2 000 година пре нове ере. Они су знали да ако затворени конопац чворовима поделе на 12 једнаких делова и штаповима га затегну у односу $3 : 4 : 5$, онда је добијени троугао правоугли, а прав угао се налази наспрам странице са 5 делова. Како су Вавилонци били познати градитељи, прав угао им је био свакодневна потреба, па су истраживали да ли и други троуглови имају исту особину.

Теорија Питагориних троуглова обједињује више математичких дисциплина, а посебно алгебру, геометрију, комбинаторику и теорију бројева.

Јасно је да ако нека два од бројева X, Y и Z који задовољавају Питагорину једначину имају заједнички делилац $d > 1$, онда је и трећи од њих дељив са d. Зато ћемо надаље претпоставити да су бројеви X, Y и Z узајамно прости у паровима, јер у супротном добијену једначину можемо скратити са d^2.

Дефиниција 6.10. Питагорину тројку (X, Y, Z) у којој су природни бројеви X, Y и Z такви да су свака два узајамно проста називамо *примитивном* или *основном Питагорином тројком*.

За примитивну Питагорину тројку кажемо и да је *примитивно* или *основно решење* Питагорине једначине $X^2 + Y^2 = Z^2$.

Налажењем свих примитивних Питагориних тројки (X, Y, Z) налазимо и све остале Питагорине тројке, јер су оне облика $(\alpha X, \alpha Y, \alpha Z)$, за неко α из $\mathbb{N}$. Стога Питагориних тројки има *бесконачно много*. Другим речима, свака примитивна Питагорина тројка генерише бесконачно много нових Питагориних тројки. На основу [44, страна 5], имамо

Теорема 6.1. У свакој примитивној Питагориној тројци (X, Y, Z) тачно један од бројева X и Y је непаран, то јест бројеви X и Y су различите парности. □

Ми ћемо надаље претпоставити да је рецимо X непаран, а Y је паран број.

Из теореме 6.1 лако закључујемо да у свакој Питагориној тројци (X, Y, Z) број Z мора бити непаран.

Важан корак у проучавању Питагориних тројки је одређивање формула за проналажење примитивних Питагориних тројки[8)], па самим тим и свих осталих Питагориних тројки, [44, страна 6].

Теорема 6.2. Нека су m и n два релативно проста природна броја таква да је $n-m$ позитиван и непаран број. Тада је

$$(n^2-m^2, 2mn, n^2+m^2)$$

примитивна Питагорина тројка, и свака примитивна Питагорина тројка је овог облика за неки избор природних бројева m и n.

Доказ. Нека је (X,Y,Z) примитивна Питагорина тројка. Тада је она и примитивно решење једначине $X^2+Y^2=Z^2$. Ако целу једначину поделимо са Z^2, добијамо

$$\left(\frac{X}{Z}\right)^2+\left(\frac{Y}{Z}\right)^2=1.$$

Одатле закључујемо да је $\left(\frac{X}{Z},\frac{Y}{Z}\right)$ рационална тачка круга $x^2+y^2=1$, па на основу рационалне параметризације круга постоји рационалан број $t=\frac{m}{n}$, при чему су природни бројеви m и n узајамно прости, такав да је

$$\frac{X}{Z}=\frac{1-\left(\frac{m}{n}\right)^2}{1+\left(\frac{m}{n}\right)^2}=\frac{n^2-m^2}{n^2+m^2} \quad \text{и} \quad \frac{Y}{Z}=\frac{2\cdot\frac{m}{n}}{1+\left(\frac{m}{n}\right)^2}=\frac{2mn}{n^2+m^2}.$$

Одавде лако закључујемо да је и $(n^2-m^2, 2mn, n^2+m^2)$ примитивна Питагорина тројка за неки избор природних бројева m и n који су узајамно прости, и такви да је $n-m$ позитиван и непаран број. □

Из претходне теореме можемо закључити да су све примитивне Питагорине тројке (X,Y,Z) дате формулама:

$$X=n^2-m^2,\ Y=2mn,\ Z=n^2+m^2. \tag{6.7}$$

при чему су m и n два параметра. Другим речима, формулама (6.7) можемо да *генеришемо* све примитивне Питагорине тројке. Кажемо и да је формулама (6.7) дата *параметризација* свих примитивних Питагориних тројки. На основу доказа теореме (6.2) можемо закључити и да је поступак одређивања Питагориних тројки сличан поступку рационалне параметризације круга.

Наведене формуле (6.7) често је користио Диофант у својим проблемима.

Последица 6.1. Постоји бесконачно много примитивних Питагориних тројки. □

[8)] то јест свих примитивних или основних решења Питагорине једначине $X^2+Y^2=Z^2$

6.2 Група $E(\mathbb{Q})$

• Елиптичке криве над пољем $\mathbb{Q}$

Нека је

$$E/\mathbb{Q} : y^2 = x^3 + ax + b$$

елиптичка крива над пољем $\mathbb{Q}$ рационалних бројева. По дефиницији, коефицијенти a и b су рационални бројеви и важи да је $\Delta = -16(4a^3 + 27b^2) \neq 0$. Тада постоје цели бројеви m и p, и природни бројеви n и q такви да је

$$E/\mathbb{Q} : y^2 = x^3 + \frac{m}{n}x + \frac{p}{q}.$$

На основу дефиниције (4.12), стављајући да је $u = \text{НЗС}(n, q)$, $a' = u^4\frac{m}{n}$ и $b' = u^6\frac{p}{q}$ добијамо да је и

$$E/\mathbb{Q} : y^2 = x^3 + a'x + b'$$

елиптичка крива, али са коефицијентима a' и b' који су цели бројеви. Због тога, надаље када кажемо елиптичка крива $E/\mathbb{Q}$ подразумеваћемо да су њени коефицијенти цели бројеви.

• Група $E(\mathbb{Q})$

Нека је $E(\mathbb{Q})$ *скуп свих рационалних тачака* елиптичке криве $E/\mathbb{Q}$, то јест

$$E(\mathbb{Q}) = \big\{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b \text{ и } \Delta \neq 0\big\} \cup \{\infty\}.$$

Основни *проблем* у вези са елиптичком кривом $E/\mathbb{Q}$ састоји се у томе да се одреди скуп $E(\mathbb{Q})$ свих њених рационалних тачака – уколико он постоји.

Као што смо видели у претходном поглављу, операцију $+$ сабирање тачака на елиптичкој кривој $E/\mathbb{R}$ увели смо геометријски помоћу тангентно-тетивног закона, и тада смо напоменули да формуле (5.4) - (5.7) важе и у случају било ког поља $\mathbb{K}$ чије је карактеристика различита од 2 и 3. С обзиром да је поље $\mathbb{Q}$ карактеристике нула, помоћу тангентно-тетивног закона, то јест формулама (5.4) - (5.7) можемо увести и сабирање тачака на елиптичкој кривој $E/\mathbb{Q}$.

Теорема 6.3. Структура $(E/\mathbb{Q}, +)$ је Абелова група у односу на операцију $+$ дефинисану формулама (5.4) - (5.7). □

Према теореми (5.3) и на скупу $E(\mathbb{Q})$ можемо успоставити структуру Абелове групе. Отуда и

Теорема 6.4. Структура $(E(\mathbb{Q}), +)$ је Абелова група у односу на операцију $+$ дефинисану формулама (5.4) - (5.7). □

• **Торзиони део групе $E(\mathbb{Q})$**

Абелова група $E(\mathbb{Q})$ садржи тачке коначног и бесконачног реда. Све тачке коначног реда чине њену подгрупу коју називамо *торзиона подгрупа* или *торзиони део* групе $E(\mathbb{Q})$ и означавамо је са $\mathcal{T}or(E)$ или $E(\mathbb{Q})_{\text{tors}}$.

6.3 Ранг елиптичке криве над пољем $\mathbb{Q}$

• **Морделова теорема**

Структура $(E(\mathbb{Q}),+)$ није само Абелова група, него је и више од тога, [33, страна 13].

Теорема 6.5. [Мордел] Структура $(E(\mathbb{Q}),+)$ је коначно генерисана Абелова група. □

У част Мордела, често групу $E(\mathbb{Q})$ називамо и *Морделова група*.

Морделова теорема представља најважнију чињеницу о скупу $E(\mathbb{Q})$. Она нам, другим речима, каже да постоји коначан скуп рационалних тачака такав да се свака друга рационална тачка на елиптичкој кривој $E/\mathbb{Q}$ може добити помоћу тангентно-тетивног закона сабирања.

Како је свака коначно генерисана Абелова група изоморфна производу цикличних група, добијамо следећу непосредну последицу Моределове теореме, која нам описује структуру групе $E(\mathbb{Q})$, [33, страна 14].

Последица 6.2. За коначно генерисану Абелову групу $E(\mathbb{Q})$ важи

$$E(\mathbb{Q}) = \underbrace{\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}}_{r}\oplus\mathcal{T}or(E) = \mathbb{Z}^r\oplus\mathcal{T}or(E),$$

где је $\mathbb{Z}^r$ *слободна подгрупа* или *слободни део* групе $E(\mathbb{Q})$ – подгрупа која се састоји од свих елемената бесконачног реда и неутрала групе $E(\mathbb{Q})$. □

• **Торзија елиптичке криве**

На основу [44, страна 11] имамо

Дефиниција 6.11. Торзиону подгрупу $\mathcal{T}or(E)$ групе $E(\mathbb{Q})$ називамо *торзија групе* $E(\mathbb{Q})$ или *торзија елиптичке криве* $E/\mathbb{Q}$.

Мазур[9)] је 1978. године доказао да постоји[10)] тачно 15 могућих њених торзија, [44, страна 11].

[9)] Бари Мазур (Barry Charles Mazur, 1937), амерички математичар
[10)] до на изоморфизам

Теорема 6.6. [**Мазур**] Ако је $E/\mathbb{Q}$ елиптичка крива, тада је $\mathcal{T}or(E)$ једна од следећих 15 група:

$$\mathbb{Z}_n \text{ [11)]}, \text{ за } n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12;$$
$$\mathbb{Z}_{2m} \oplus \mathbb{Z}_2, \text{ за } m = 1, 2, 3, 4. \qquad \square$$

Другим речима, $\mathcal{T}or(E)$ је циклична група или производ две цикличне групе.

Из Мазурове теореме закључујемо да у случају $E/\mathbb{Q}$ не постоји торзиона тачка реда већег од 12, као ни торзиона група већег реда од 16.

Да бисмо одредили $\mathcal{T}or(E)$, то јест све тачке (x, y) коначног реда, прво претпоставимо да је (x, y) тачка реда 2. То је тачка са y-координатом једнаком 0, то јест тачка $(x, 0)$. Можемо имати 0, 1 или 3 такве тачке, што зависи од броја рационалних нула полинома $x^3 + ax + b$. Те тачке, заједно са тачком $\mathcal{O}$, чине подгрупу од $\mathcal{T}or(E)$ која је или тривијална или $\mathbb{Z}_2$ или $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Остале тачке коначног реда одређујемо помоћу Луц[12)] – Нагелове[13)] теореме која нам и омогућава да ефикасно израчунамо торзиону групу $\mathcal{T}or(E)$, [44, страна 11].

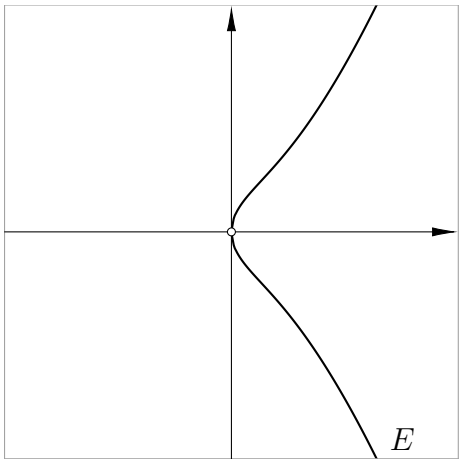
Теорема 6.7. [**Луц – Нагел**] Нека је $E/\mathbb{Q} : y^2 = x^3 + ax + b$ елиптичка крива. Ако је (x, y) из $\mathcal{T}or(E)$ и $(x, y) \neq \infty$, тада су x и y из $\mathbb{Z}$ и важи

$$y = 0 \quad \text{или} \quad y^2 \mid 4a^3 + 27b^2 = \frac{-\Delta}{16}. \qquad \square$$

Луц – Нагелова теорема нам показује да имамо само коначно много кандидата за y-координату торзионе тачке (x, y) које морамо проверити. Наведимо примере који ће нам илустровати ту теорему.

Пример 6.1. Одредити торзију елиптичке криве

$$E/\mathbb{Q} : y^2 = x^3 + x. \tag{6.8}$$



[11)] Са $\mathbb{Z}_n$ смо означили групу $\mathbb{Z}/n\mathbb{Z}$ бројева по модулу n, јер је $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ за свако n из $\mathbb{N}$.
[12)] Елизабет Луц (Élisabeth Lutz, 1914–2008), француска математичарка
[13)] Трајгве Нагел (Trygve Nagell, 1895–1988), норвешки математичар

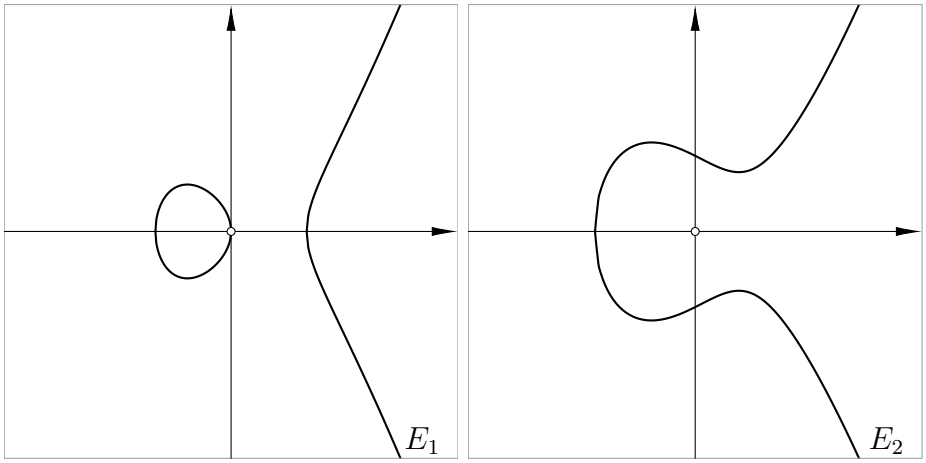
Како је $4a^3 + 27b^2 = 4$, према Луц – Нагеловој теореми за сваку торзиону тачку (x, y) мора важити $y = 0$ или $y^2 \mid 4$, при чему су x, y из $\mathbb{Z}$, па је

$$y \in \{0, 1, -1, 2, -2\}.$$

Уврштавањем $y = \pm 1$ у (6.8) добијамо једначину $x^3 + x = 1$ која нема целобројних решења. Слично, за $y = \pm 2$ добијамо да једначина $x^3 + x = 4$ нема целобројних решења. Нека је $y = 0$. Тада је $x = 0$ једино целобројно решење једначине $x^3 + x = 0$. То значи да је

$$\mathcal{T}or(E) = \{\mathcal{O}, (0, 0)\} \cong \mathbb{Z}_2. \qquad \triangle$$

Пример 6.2. Према [33, страна 14], торзија елиптичке криве $E_1/\mathbb{Q} : y^2 = x^3 - x$ је $\mathcal{T}or(E_1) = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, а елиптичке криве $E_2/\mathbb{Q} : y^2 = x^3 - x + 1$ је тривијална, то јест $\mathcal{T}or(E_1) = \{\mathcal{O}\}$. $\triangle$



Дакле, за дату елиптичку криву $E/\mathbb{Q}$ лако израчунавамо њену торзију $\mathcal{T}or(E)$, то јест постоје алгоритми за њено израчунавање, и они су у пракси врло ефикасни.

• Ранг елиптичке криве

На основу [44, страна 9], имамо

Дефиниција 6.12. Ненегативан цео број r из релације $E(\mathbb{Q}) = \mathbb{Z}^r \oplus \mathcal{T}or(E)$ називамо *ранг групе* $E(\mathbb{Q})$ или *ранг елиптичке криве* $E/\mathbb{Q}$.

Уколико желимо да нагласимо да је r ранг групе $E(\mathbb{Q})$, односно ранг елиптичке криве E над $\mathbb{Q}$ писаћемо $r(E(\mathbb{Q}))$, односно $r(E)$.

Последица (6.2) нам каже да постоји r рационалних тачака $P_1, P_2, \ldots, P_r$ бесконачног реда на елиптичкој кривој $E/\mathbb{Q}$ са својством да се свака тачка P из $E(\mathbb{Q})$ може представити у облику

$$P = n_1P_1 + n_2P_2 + \cdots + n_rP_r + T$$

за неке целе бројеве $n_1, n_1, \ldots, n_r$, где је T нека тачка коначног реда.

Ранг *мери величину* како елиптичке криве $E/\mathbb{Q}$, тако и саме групе $E(\mathbb{Q})$, то јест број њених независних рационалних тачака. Ако је:

- $r(E(\mathbb{Q})) = 0$, група $E(\mathbb{Q})$ је коначна,
- $r(E(\mathbb{Q})) > 0$, група $E(\mathbb{Q})$ је бесконачна.

Пример 6.3. Ранг елиптичке криве $E_1 : y^2 = x^3 - x$ је $r(E_1) = 0$, јер је $E_1(\mathbb{Q}) = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ а ранг елиптичке криве $E_2 : y^2 = x^3 - x + 1$ је $r(E_2) = 1$, јер је $E_2(\mathbb{Q}) = \mathbb{Z}$. △

Ранг елиптичке криве је, за разлику од торзије елиптичке криве, доста теже описати. Само рачунање ранга елиптичке криве над $\mathbb{Q}$ је врло тежак проблем, јер за ранг елиптичке криве не постоје аналогони теорема (6.6) и (6.7), то јест:

- не постоји алгоритам за одређивање ранга произвољне елиптичке криве; постоје алгоритми за рачунање горње и доње границе ранга,
- не зна се који цели бројеви могу бити рангови неке елиптичке криве; не зна се ни да ли је ранг елиптичке криве ограничен.

С друге стране, није познато да ли ранг може бити произвољно велик или постоји апсолутна горња граница. Према [44, страна 9] важи

Хипотеза. Ранг елиптичке криве може бити произвољан природан број, то јест постоји елиптичка крива $E/\mathbb{Q}$ чија је група рационалних тачака $E(\mathbb{Q})$ произвољно великог ранга.

Другим речима, за сваки природан број n постоји елиптичка крива $E/\mathbb{Q}$ таква да је $r(E) > n$.

Данас се тек зна да постоји елиптичка крива $E/\mathbb{Q}$ ранга најмање 28. Њу је 2006. године пронашао Елкис[14)]. Отуда и, према [44, страна 10]

Теорема 6.8. Елиптичка крива

$$E : y^2 + xy + y = x^3 - x^2 - ax + b,$$

где је $a = 20067762415575526585033208209338542750930230312178956502$ и $b = 34481611795030556467032985690390720374855944359319180361266008296291939448732243429$ над пољем $\mathbb{Q}$ има ранг најмање 28, то јест $r(E) \geq 28$. Генератори групе $E(\mathbb{Q})$ су:

$P_1 = [-212415009125438107329213746 3,$
$259854492051899599030515511070780628911531];$

$P_2 = [233450986603470175688475 4537,$
$188720041954944691808683165528036279315 31];$

$P_3 = [-167173605406236906387903 8663,$

[14)] Ноам Давид Елкис (Noam David Elkies, 1966–), амерички математичар

$$251709377261144287808506947241319126049131];$$

$$P_4 = [213913026013915666649298213 7,$$
$$366395091714397292024214596929412975275 31];$$

$$P_5 = [153470676446712072388547733 7,$$
$$854295853460176942890210328627810727995 31];$$

$$P_6 = [-27310794878756770333415750 63,$$
$$262521815484332191641284072623902143387531];$$

$$P_7 = [27757262668445716497054585 37,$$
$$128457554740140602488694876990826403699 31];$$

$$P_8 = [14943857293271889575418338 17,$$
$$884866055277334059861164945140492334114 51];$$

$$P_9 = [18684382286208873585090652 57,$$
$$592374032144377087127251403930593585891 31];$$

$$P_{10} = [20089451088257437748665425 37,$$
$$476906778801255528821517507815414247115 31];$$

$$P_{11} = [23483605409180251696516329 37,$$
$$174929300062005578573403324764488043635 31];$$

$$P_{12} = [-14720840070904811744700086 63,$$
$$246643450653503714199947441549759798469131];$$

$$P_{13} = [29241286077080612133632889 37,$$
$$283502644314888785014883564747673758995 31];$$

$$P_{14} = [53749938910660618932939345 37,$$
$$286188908427263386451175031916479893731531];$$

$$P_{15} = [17096907682333545233340085 57,$$
$$718988349746860894661597005292159809216 31];$$

$$P_{16} = [24509540113535931440725951 87,$$
$$4445228173532634357049262550610714736531];$$

$$P_{17} = [29692547092735591674646749 37,$$
$$327668930753662708013336825431604696875 31];$$

$$P_{18} = [27119149349416926013328829 37,$$
$$206843661277838169865041398150659061353 1];$$

$$P_{19} = [20078586077996854528778328 937,$$
$$277960854\ 113780660465605172562462403009153 1];$$

$$P_{20} = [21580824502407347743178106 97,$$
$$349943734019640268099696622418009012547 31];$$

$$P_{21} = [20046454582470590224032249 37,$$
$$480493297807046455224398669998884754675 31];$$

$P_{22} = [29757494509479962649470913 37,$
$3339898982607532232020893441010485786913 1];$
$P_{23} = [-21024904676862851501473478 63,$
$2595763914598757895716773931716872032275 31];$
$P_{24} = [31158317991506303490219453 7,$
$1681043852299806035401094729156601534739 31];$
$P_{25} = [27739310083418652314437718 17,$
$1263216283464992100241411627376927581345 1];$
$P_{26} = [21565811881437684093634613 87,$
$3512509296402290889700415051637517808733 1];$
$P_{27} = [38663304998724125088156591 37,$
$1211977556559442262930369267150258473225 31];$
$P_{28} = [22308682897735760237786787 37,$
$2855876003059748566338702060076864002853 1].$ □

Постоји и хипотеза Голдфелда[15], [33, страна 14].

Хипотеза. [Голдфелд] Ако поређамо елиптичке криве $E/\mathbb{Q}$ по величини коефицијената, асимптотски 50% кривих има ранг 0, а 50% их има ранг 1.

Дакле, Голдфелдова хипотеза предвиђа да је просечни ранг једнак $0,5$.

На крају наведимо и теорему Баргаве[16] и Шанкара[17] из 2011. године, [33, страна 14].

Теорема 6.9. [Баргава-Шанкар] Ако поређамо елиптичке криве $E/\mathbb{Q}$ по величини коефицијената, тада је просечни ранг мањи од 0,99. □

[15] Дориан Морис Голдфелд (Dorian Morris Goldfeld, 1947), амерички математичар

[16] Манџул Баргава (Manjul Bhargava , 1974), канадско-амерички математичар индијског порекла, добитник Филдсове медаље 2014. године

[17] Арул Шанкар (Arul Shankar), индијски математичар

7

Елиптичке криве над коначним пољима

Одређивање структуре групе $E(\mathbb{Q})$ може бити врло тешко. Због тога, посматраћемо елиптичку криву E над неким коначним пољем. Другим речима, уместо да тражимо рационалне тачке елиптичке криве $E/\mathbb{Q}$ посматраћемо елиптичку криву E над неким коначним пољем и тражити њене рационалне тачке у том пољу, што је очигледно лакше јер је такво поље коначно. Слично је и са одређивањем њене торзије $\mathcal{T}or(E)$. Ово поглавље је посвећено елиптичким кривама над коначним пољима. Опширније у [57], [33] [16] и [15].

7.1 Коначна поља

• Коначно поље и његова реализација

Коначна поља су први проучавали Ферма, Ојлер, Лежандр, Лагранж[1)] и Гаус због својих истраживања у теорији бројева.

Коначно поље $\mathbb{F}$ реда q, то јест са тачно q елемената означавамо са $\mathbb{F}_q$[2)]. Наравно, његова карактеристика мора бити неки прост број p.

Основно коначно поље је $\mathbb{F}_p$, и оно настаје стављајући да је $q = p$, при чему је p прост број. Тада, за сваки прост број p постоји поље од p елемената. Можемо га реализовати као скуп $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ заједно са операцијама сабирање $+_p$ и множење $\cdot_p$ по модулу p, то јест

$$\mathbb{F}_p = \left(\mathbb{Z}_p, +_p, \cdot_p\right).$$

[1)] Жозеф-Луј Лагранж (Joseph-Louis Lagrange, 1736–1813), италијанско-француски математичар и астроном

[2)] Користи се још и ознака $GF(q)$ јер се коначна поља називају и *Галоаова*[3)] *поља*

[3)] Еварист Галоа (Évariste Galois, 1811–1832), француски математичар

Аналогно, $\mathbb{F}_p$ можемо реализовати и као количнички прстен

$$\mathbb{F}_p = \left(\mathbb{Z}/p\mathbb{Z}, +_p, \cdot_p\right).$$

Стављајући у $\mathbb{F}_q$ да је $q = p^n$, при чему је p прост, а n природан број, добијамо коначно поље $\mathbb{F}_{p^n}$. Тада, за сваки прост број p и природан број n постоји поље са $q = p^n$ елемената. Важи и обратно, ако је карактеристика коначног поља $\mathbb{F}_q$ неки прост број p, тада то поље има p^n елемената. Заиста, ако је карактеристика од $\mathbb{F}_q = p$ и p прост број, тада $\mathbb{F}_q$ садржи просто потпоље $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ са тачно p елемената и $\mathbb{F}_q$ је један коначно димензионалан векторски простор над пољем $\mathbb{F}_p$. Нека је n његова димензија и $[e_1, \ldots, e_n]$ једна његова база. Тада се сваки елемент $a \in \mathbb{F}_q$ може на једнозначан начин приказати у облику линеарне комбинације

$$a = \lambda_1 e_1 + \cdots + \lambda_n e_n,$$

при чему је λ_i из $\mathbb{Z}_p$. На тај начин је сваком елементу a из $\mathbb{F}_q$ придружена уређена n-торка $(\lambda_1, \ldots, \lambda_n)$ из $(\mathbb{Z}_p)^n$. Због тога је $q = p^n$, то јест поље $\mathbb{F}_q$ има p^n елемената.

Једна од реализација поља $\mathbb{F}_{p^n}$ за $n > 1$ је количнички прстен $\mathbb{Z}_p[x]/(f(x))$, где је f неки полином степена $d^\circ f = n$ који је нерастављив над $\mathbb{Z}_p$, а $(f(x))$ главни идеал генерисан са $f(x)$[4]. Тај прстен је и поље, јер је f нерастављив полином. Елементе поља $\mathbb{Z}_p[x]/(f(x))$ можемо приказати као полиноме над $\mathbb{Z}_p$ степена мањег или једнаког од $n-1$. Таквих полинома има тачно p^n. Операције сабирање и множење у пољу $\mathbb{F}_{p^n}$ су операције наслеђене из $\mathbb{Z}_p[x]$, с тим да се након множења полинома рачуна остатак при дељењу са полиномом f.

Пример 7.1. [**Конструкција поља** $\mathbb{F}_9$] Посматрајмо полином $f(x) = x^2 + 1$ над $\mathbb{Z}_3 = \{0, 1, 2\}$. Он је нерастављив над $\mathbb{Z}_3$, јер нема корен у $\mathbb{Z}_3$. Због тога, поље $\mathbb{F}_9 = \mathbb{F}_{3^2}$ можемо представити као поље $\mathbb{Z}_3[x]/(f(x))$. Одавде закључујемо да су елементи од $\mathbb{F}_9$:

$$0, 1, 2, x, x+1, x+2, 2x, 2x+1 \text{ и } 2x+2,$$

то јест

$$\mathbb{F}_{3^2} = \{a + b\eta : a, b \in \mathbb{F}_3\}$$

уз услов да је $\eta^2 = -1$, де је η класа елемента x у количничком прстену. То поље има тачно 9 елемената. Израчунајмо, на пример, $(\eta + 1)^2$ у пољу $\mathbb{F}_9$. Имамо:

$$(\eta + 1)^2 = \eta^2 + 2\eta + 1 = 2\eta,$$

јер се при дељењу полинома $\eta^2 + 2\eta + 1$ са $\eta^2 + 1$ добија остатак 2η. △

[4] *Главни идеал* комутативног прстена $(K, +, \cdot)$ је идеал[5] прстена $(K, +, \cdot)$ који је генерисан једним елементом, то јест идеал облика $\langle a \rangle = aK = \{ap : p \in K\}$ за a из K.

[5] *Идеал* уоченог прстена $(K, +, \cdot)$ је сваки од скупова I, у ознаци $I \lhd K$, за који важе услови: $\langle 1 \rangle$ I је подгрупа групе $(K, +)$, $\langle 2 \rangle$ $a \in K, x \in I \Rightarrow ax, xa \in I$.

• Мултипликативна група коначног поља

Нека је $\mathbb{F}_q$ коначно поље. Елементи поља $\mathbb{F}_q$ различити од нуле чине Абелову групу у односу на множење. Називамо је *мултипликативна*[6] *група* поља $\mathbb{F}_q$ и означавамо са $\mathbb{F}_q^*$. Она је циклична, па постоји елемент $g \in \mathbb{F}_q$ такав да се сваки елемент из $\mathbb{F}_q^*$ може написати као степен од g.

• Поље $\mathbb{F}_{2^m}$. Оптимална нормална база

Видели смо да је поље $\mathbb{F}_{2^m}$ векторски простор над пољем $\mathbb{F}_2$ димензије m. Постоји много различитих база тог векторског простора. Ми ћемо споменути два типа таквих база: триномне и нормалне.

Нека је f полином нерастављив над $\mathbb{F}_2$ степена $d^\circ p = m$. Тада се поље $\mathbb{F}_{2^m}$ може представити као скуп свих полинома над пољем $\mathbb{F}_2$ степена $d^\circ p < m$ са операцијама по модулу полинома f. За такво представљање кажемо да је представљање помоћу *полиномне базе*.

Представљање помоћу *триномне базе* је специјални случај представљања помоћу полиномне базе у којем полином f има облик

$$f(x) = x^m + x^k + 1.$$

Предност таквог представљања је ефикасност спровођења редукције по модулу полинома f. За неке m-ове, на пример $m \equiv 0 \pmod 8$, триномна база и не постоји. Експериментално је показано да триномна база постоји за нешто више од пола m-ова мањих од 1000.

Нормална база векторског простора $\mathbb{F}_{2^m}$ над пољем $\mathbb{F}_2$ је облика

$$[b, b^2, \ldots, b^{2m-1}],$$

при чему је b из $\mathbb{F}_{2^m}$. Таква база, за разлику од полиномне, увек постоји. Приликом представљања помоћу нормалне базе, квадрирање у пољу постаје тривијално: ако је

$$a = (a_0, a_1, \ldots, a_{m-1}),$$

онда је

$$a^2 = (a_{m-1}, a_0, a_1, \ldots, a_{m-2}),$$

то јест квадрирање није ништа друго него циклично померање удесно.

Међутим, за уопштену нормалну базу множење у пољу је знатно компликованије. Због тога су од интереса оне нормалне базе код којих је множење што једноставније. Такве базе називамо *оптималне нормалне базе*. Оптимална нормална база не мора да постоји. Један од неопходних услова за постојање такве базе је да је бар један од бројева $n + 1$, $2n + 1$ прост.

[6] Реч *мултипликативан* потиче од латинске речи *multiplicatio* што у преводу значи *множење, умножавање*.

7.2 Елиптичке криве над пољем $\mathbb{F}_p$

• Редукција по модулу p

Редукција по модулу p, то јест остатак при дељењу са p је хомоморфизам $\mathbb{Z} \to \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ задат са

$$m \mapsto m \,(\mathrm{mod}\, p). \tag{7.1}$$

То је један од *основних алата* у теорији бројева. Надаље, ради краткоће, уместо $m \,(\mathrm{mod}\, p)$ писаћемо $\overline{m}$.

У вези са редукцијом по модулу p, напоменимо и да се цео пројективни простор $\mathbb{P}^n(\mathbb{Q})$, односно $\mathbb{P}^n(\mathbb{Z})$ може редуковати у пројективни простор $\mathbb{P}^n(\mathbb{F}_p)$.

Елиптичку криву редукујемо по модулу p тако што њене коефицијенте, то јест коефицијенте полинома којим је она дефинисана редукујемо по модулу p.

Нека је $E/\mathbb{Q}$ елиптичка крива. Да би ту криву редуковали по модулу p, прво је требамо свести на погодан облик. Подсетимо се да је свака елиптичка крива над пољем $\mathbb{Q}$ изоморфна некој елиптичкој кривој облика

$$E : y^2 = x^3 + ax + b,$$

где су a и b цели бројеви. Њеном редукцијом по модулу p добијамо кубну криву $\overline{E}/\mathbb{F}_p$ чија је једначина

$$\overline{E} : y^2 \equiv x^3 + ax + b \,(\mathrm{mod}\, p),$$

односно

$$\overline{E} : y^2 = x^3 + \overline{a}x + \overline{b},$$

где су $\overline{a}$ и $\overline{b}$ из $\mathbb{Z}_p$. Она, у општем случају, не мора бити елиптичка, јер не мора бити глатка.

С друге стране, постоје и изоморфне елиптичке криве $E/\mathbb{Q}$ над пољем $\mathbb{Q}$ чије редукције по неком модулу p нису исте, што је илустровано следећим примером.

Пример 7.2. Елиптичке криве

$$E_1/\mathbb{Q} : y^2 = x^3 + x + 1 \quad \text{и} \quad E_2/\mathbb{Q} : y^2 = x^3 + 81x + 729$$

су изоморфне над пољем $\mathbb{Q}$, јер је

$$j(E_1) = j(E_2) = 222\frac{30}{31}.$$

Њихове редукције по модулу 3

$$\overline{E_1} : y^2 = x^3 + x + 1 \quad \text{и} \quad \overline{E_2} : y^2 = x^3$$

нису исте. Заиста, са $\overline{E_1}$ је задата елиптичка крива, а са $\overline{E_2}$ то није, јер је

$$\Delta(E_1) = -2^4 \cdot 31 \equiv 1 \,(\mathrm{mod}\, 3), \text{ а } \Delta(E_2) = 2^4 \cdot 3^{12} \cdot 31 \equiv 0 \,(\mathrm{mod}\, 3). \qquad \triangle$$

• Минималан модел елиптичке криве. p-адична валуација броја

Редукција $\overline{E}/\mathbb{F}_p$ елиптичке криве $E/\mathbb{Q}$ ће имати смисла, ако изаберемо *минималан модел* у класи изоморфизма елиптичке криве над пољем $\mathbb{Q}$. Да бисмо обухватили редукције елиптичких кривих $E/\mathbb{Q}$ по модулу p за свако p, посматраћемо елиптичку криву у Вајерштрасовом општем облику. Према [33, страна 31] имамо

Дефиниција 7.1. Кажемо да је

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{7.2}$$

при чему су a_i из $\mathbb{Z}$, *минималан модел* елиптичке криве $E/\mathbb{Q}$ ако је $|\Delta(E)|$ минималан у класи изоморфизма од $E/\mathbb{Q}$.

Једначину (7.2) називамо *минимална Вајерштарсова једначина* од $E/\mathbb{Q}$.

Да бисмо практично испитали да ли је неки модел елиптичке криве $E/\mathbb{Q}$ минималан, потребна нам је p-адична валуација броја, [33, страна 31].

Дефиниција 7.2. Нека је n цео број записан у облику $n = p^k \cdot m$, при чему је (p, m)[7] $= 1$[8] и $k \geq 0$. Тада је *p-адична валуација* $\nu_p(n)$ броја n највећи степен од p који дели n, то јест

$$\nu_p(n) = \nu_p(p^k \cdot m) = k.$$

У вези са претходним, за поједине вредности од p, користимо следећи став, [33, страна 31].

Став 7.1. Нека је $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, за a_i из $\mathbb{Z}$, Вајерштрасова форма елиптичке криве $E/\mathbb{Q}$ и $\Delta(E)$ њена дискриминанта. Ако је

$$0 \leq \nu_p(\Delta(E)) < 12,$$

за све просте бројеве p, тада је E минималан модел. □

За p различито од 2 и 3 важи и обрат овог става.

Пример 7.3. Видели смо у примеру (7.2) да су елптичке криве $E_1/\mathbb{Q} : y^2 = x^3 + x + 1$ и $E_2/\mathbb{Q} : y^2 = x^3 + 81x + 729$ изоморфне. Модел $E_1 : y^2 = x^3 + x + 1$ је минималан, јер је

$$\Delta(E_1) = 2^4 \cdot 31 \text{ и } \nu_2(\Delta(E_1)) = 4 < 12, \nu_{31}(\Delta(E_1)) = 1 < 12,$$

[7] Са (p, m) смо традиционално означили *највећи заједнички делилац* целих бројева p и m. Употребљавају се, поготово у школској математици, још и ознаке НЗД(p, m) или $D(p, m)$. Традиционална ознака за *најмањи заједнички садржалац* целих бројева a и b је $[a, b]$, а од других могућих ознака поменимо НЗС(a, b) или $S(a, b)$.

[8] Пошто је, у овом случају, p прост број, могли смо да напишемо и само $p \nmid m$.

док $E_2 : y^2 = x^3 + 81x + 729$ није минималан модел, јер је

$$\Delta(E_2) = 2^4 \cdot 3^{12} \cdot 31 \text{ и } \nu_2(\Delta(E_2)) = 4 < 12, \nu_3(\Delta(E_2)) = 12. \qquad \triangle$$

• Елиптичка крива над пољем $\mathbb{F}_p$

На основу [33, страна 31] имамо

Дефиниција 7.3. Нека је $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, при чему су a_i из $\mathbb{Z}$, минималан модел елиптичке криве $E/\mathbb{Q}$. Тада је са

$$\overline{E} : y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6,$$

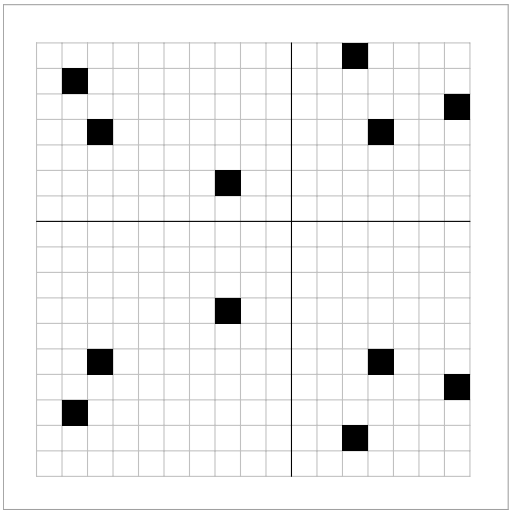
где је $\overline{a}_i$ слика од a_i при хомоморфизму $\mathbb{Z} \to \mathbb{F}_p$ редукција по модулу p, дефинисана елиптичка крива $\overline{E}/\mathbb{F}_p$ над пољем $\mathbb{F}_p$. Називамо је *редукцијом елиптичке криве* $E/\mathbb{Q}$ по модулу p.

Приметимо да важи следеће:

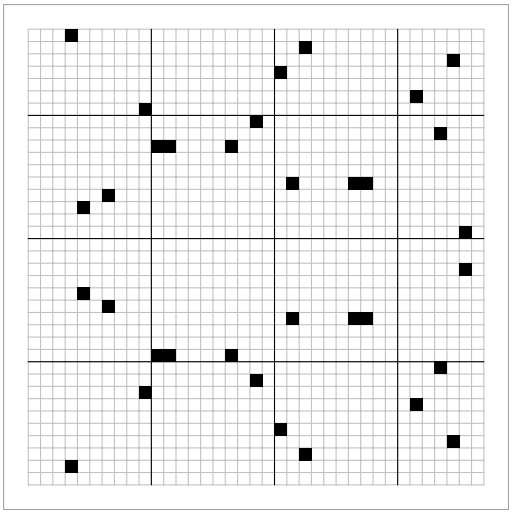
Кубна крива $\overline{E}$ над пољем $\mathbb{F}_p$ је елиптичка ако и само ако је $\Delta(\overline{E}) \neq 0$ у пољу $\mathbb{F}_p$, то јест $\Delta(\overline{E}) \not\equiv 0 \pmod p$, односно $p \nmid \Delta(E)$.

На следећем цртежу приказане су неке елиптичке криве над пољима $\mathbb{F}_p$.

$\overline{E}/\mathbb{F}_{17} : y^2 = x^3 + 5x - 2$



$\overline{E}/\mathbb{F}_{37} : y^2 = x^3 + 2x + 5$



• Добра и лоша редукција по модулу p

На основу [33, страна 31] имамо

Дефиниција 7.4. Ако $p \nmid \Delta(E)$, тада елиптичка крива $E/\mathbb{Q}$ има *добру редукцију* по модулу p. У супротном, она има *лошу редукцију* по модулу p.

Другим речима, ако је редукција $\overline{E}$ по модулу p елиптичка крива над $\mathbb{F}_p$, тада $E/\mathbb{Q}$ има добру редукцију по модулу p, иначе има лошу.

Уместо да кажемо елиптичка крива има редукцију *по модулу* p казаћемо краће да елиптичка крива има редукцију *у* p.

С обзиром на чињеницу да дискриминанта елиптичке криве има само коначно много простих фактора, можемо закључити да свака елиптичка крива има лошу редукцију у само коначно много p-ова.

Пример 7.4. Елиптичка крива

$$E_1/\mathbb{Q} : y^2 = x^3 - x$$

има добру редукцију у свим $p \neq 2$, јер је

$$\Delta(E_1) = 2^6.$$

Елиптичка крива

$$E_2/\mathbb{Q} : y^2 = x^3 - x^2 - 86x + 240$$

има добру редукцију свугде осим можда у $p = 2, 3, 5, 13$, јер је

$$\Delta(E_2) = -2^6 \cdot 3^4 \cdot 5^2 \cdot 13^2. \qquad \triangle$$

• Квадратни остатак по модулу p

Да бисмо наставили проучавање елиптичких кривих над пољем $\mathbb{F}_p$ и детаљније упознали лоше редукције, посебно мултипликативну, морамо се подсетити дефиниције квадратног остатка по моулу p, [32, страна 67].

Дефиниција 7.5. За цео број a кажемо да је *квадратни остатак по модулу* p, где је p прост број и $p \nmid a$, ако постоји цео број x такав да је

$$x^2 \equiv a \pmod{p}.$$

Другим речима, a је квадратни остатак по модулу p ако постоји потпун квадрат који даје исти остатак при дељењу са p као и a. У супротном кажемо да је *а квадратни неостатак по модулу* p. Скуп свих квадратних остатака, односно неостатака по модулу p означавамо са Q_p, односно са $\overline{Q}_p$.

Пример 7.5. За $p = 17$ је

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$x^2 \pmod{17}$	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1

па је $Q_{17} = \{1, 2, 4, 8, 9, 13, 15, 16\}$, односно $\overline{Q}_{17} = \{3, 5, 6, 7, 10, 11, 12, 14\}$. $\triangle$

Према [32, страна 67] важи наредна теорема.

Теорема 7.1. За дати непаран прост број p и цео број a, при чему $p \nmid a$, једначина $x^2 \equiv a \pmod{p}$ или нема решења или има тачно два решења. □

Из ове једноставне теореме, према [32, страна 67], следи

Теорема 7.2. За сваки непаран прост број p, међу бројевима $1, \ldots, p-1$ има тачно $\frac{p-1}{2}$ квадратних остатака [и исто толико квадратних неостатака]. □

• **Адитивна и мултипликативна редукција у p**

Нека је елиптичка крива $E/\mathbb{Q}$ задата моделом $E : y^2 = f(x)$, при чему је f полином степена $d^\circ f = 3$, и нека је $\overline{E} : y^2 = \overline{f}(x)$, где је $\overline{f} \in \mathbb{F}_p[x]$ полином по модулу p, то јест полином чији су коефицијенти добијени од коефицијената полинома f редукцијом по модулу p. Тада, према [33, страна 32], важи

Став 7.2. Елиптичка крива $E/\mathbb{Q}$ има *лошу редукцију* у p ако и само ако полином $\overline{f}$ у моделу $\overline{E} : y^2 = \overline{f}(x)$ има *вишеструки корен.* □

Постоји више врста лоше редукције у p. Прва од њих је адитивна[9] редукција, [33, страна 32].

Дефиниција 7.6. Ако полином $\overline{f}$ у моделу $\overline{E} : y^2 = \overline{f}(x)$ има троструки корен, тада елиптичка крива $E/\mathbb{Q}$ има *адитивну редукцију* у p.

У овом случају, кубна крива $\overline{E}$ има касп, а то је еквивалентно са $p \mid \Delta(E)$ и $p \mid ((4a_2 + a_1^2)^2 - 24(2a_4 + a_1a_3))$, при чему су a_1, a_2, a_3 и a_4 коефицијенти у Вајерштрасовој форми елиптичке криве $E/\mathbb{Q}$.

Друга лоша редукција је мултипликативна, [33, страна 32].

Дефиниција 7.7. Ако полином $\overline{f}$ у моделу $\overline{E} : y^2 = \overline{f}(x)$ има двоструки корен, тада елиптичка крива $E/\mathbb{Q}$ има *мултипликативну редукцију* у p и њен модел је облика

$$E : y^2 = x^2(x + a).$$

У овом случају, кубна крива $\overline{E}$ има тачку самопресека, а то је еквивалентно са $p \mid \Delta(E)$ и $p \nmid ((4a_2 + a_1^2)^2 - 24(2a_4 + a_1a_3))$.

Постоје, такође, расцепива и нерасцепива мултипликативна редукција у p, о чему говори наредна дефиниција, [33, страна 32].

Дефиниција 7.8. Ако је број a квадратни остатак по модулу p у моделу

$$E : y^2 = x^2(x + a)$$

[9] Реч *адитиван* потиче од латинске речи *additivus* што у преводу значи *додат*, *који има да се дода.*

елиптичке криве $E/\mathbb{Q}$ са мултипликативном редукцијом у p, тада та елиптичка крива има *расцепиву мултипликативну редукцију* у p, иначе је мултипликативна редукција у p *нерасцепива*.

• Кондуктор елиптичке криве. Полустабилна елиптичка крива

Поред дискриминанте $\Delta(E)$ и j-инваријанте $j(E)$ елиптичке криве E, дефинисаћемо још једну важну величину коју придружујемо свакој елиптичкој кривој E, а која је, такође, повезана са том дискриминантом, [15, страна 470].

Дефиниција 7.9. *Кондуктор елиптичке криве* $E/\mathbb{Q}$ је број

$$N = \prod_{p \text{ прост}} p^{f_p(E)},$$

при чему је

$$f_p(E) = \begin{cases} 0, & \text{ако } E/\mathbb{Q} \text{ има добру редукцију у } p \\ 1, & \text{ако } E/\mathbb{Q} \text{ има мултипликативну редукцију у } p \\ 2, & \text{ако } E/\mathbb{Q} \text{ има адитивну редукцију у } p \text{ и } p \notin \{2,3\}^{10)}. \end{cases}$$

Кондуктор елиптичке криве нам говори о њеној *врсти редукције*. Према [33, страна 126] имамо

Дефиниција 7.10. Елиптичку криву која нема адитивну редукцију ни у једнном простом броју p, то јест има мултипликативну или добру редукцију у сваком простом броју p називамо *полустабилном елиптичком кривом*.

Све полустабилне елиптичке криве имају кондуктор који није потпун квадрат.

7.3 Група $E/\mathbb{F}_p$

• Скуп $\overline{E}(\mathbb{F}_p)$

Видели смо да је $\overline{E}/\mathbb{F}_p$ редукција елиптичке криве $E/\mathbb{Q}$ по модулу p, то јест елиптичка крива E над пољем $\mathbb{F}_p$. Са $\overline{E}(\mathbb{F}_p)$ означићемо скуп

$$\overline{E}(\mathbb{F}_p) = \Big\{(x,y) \in \mathbb{F}_p^2 \mid y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \,(\mathrm{mod}\, p) \\ \text{и } \Delta(\overline{E}) \not\equiv 0 \,(\mathrm{mod}\, p)\Big\} \cup \{\infty\}.$$

[10)] За $p \in \{2,3\}$, дефиниција од $f_p(E)$ је компликованија, али у општем случају је $f_p(E) \geq 2$ ако елиптичка крива E има адитивну редукцију у p.

Називамо га *скуп тачака редукција по модулу* p елиптичке криве $E/\mathbb{Q}$.

• Група тачака редукција по модулу p

Сабирање тачака на $\overline{E}/\mathbb{F}_p$ за $p > 3$ уводимо тако што користимо исте формуле (5.4) - (5.7) којима смо увели сабирање тачака на $E/\mathbb{R}$ само што рачунање вршимо по модулу p, уз напомену да рачунање инверза на $\overline{E}/\mathbb{F}_p$ вршимо помоћу Еуклидовог алгоритма. Сабирање на $\overline{E}/\mathbb{F}_2$ или $\overline{E}/\mathbb{F}_3$ је такође исто као сабирање на $E/\mathbb{R}$ само су формуле (5.4) - (5.7) другачије јер, приликом њиховог формирања, уместо кратке Вајерштрасове форме користимо Вајерштрасову форму од E.

Теорема 7.3. Структура $(\overline{E}/\mathbb{F}_p, +)$ је Абелова група у односу на операцију $+$ сабирање тачака на $\overline{E}/\mathbb{F}_p$. □

Према теореми (5.3) и на скупу $\overline{E}(\mathbb{F}_p)$ можемо успоставити структуру Абелове групе. Отуда и

Теорема 7.4. Структура $(\overline{E}(\mathbb{F}_p), +)$ је Абелова група у односу на операцију $+$ сабирање тачака на $\overline{E}/\mathbb{F}_p$. □

Абелову групу $(\overline{E}(\mathbb{F}_p), +)$ називамо *група тачака редукција по модулу* p елиптичке криве $E(\mathbb{Q})$.

• Уопштење Лежандровог симбола на поље $\mathbb{F}_p$

Да бисмо наставили проучавање елиптичких кривих над пољем $\mathbb{F}_p$, морамо уопштити Лежандров симбол на $\mathbb{F}_p$. Пре тога, подсетимо се Лежандровог симбола и основних својстава у вези са њим, [32, страна 68].

Дефиниција 7.11. За дати непаран прост број p и цео број a, *Лежандров симбол* $\left(\frac{a}{p}\right)$ дефинишемо као

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ако } p \nmid a \text{ и } a \text{ је квадратни остатак по модулу } p \\ -1, & \text{ако } p \nmid a \text{ и } a \text{ је квадратни неостатак по модулу } p \\ 0, & \text{ако } p \mid a. \end{cases} \tag{7.3}$$

Лежандров симбол можемо видети као аритметичку функцију[11)]

$$a \mapsto \left(\frac{a}{p}\right) \qquad \mathbb{Z} \to \{-1, 0, 1\}$$

[11)] *Аритметичка функција* је свака комплексна функција дефинисана на скупу природних бројева $\mathbb{N}$ са вредностима у скупу $\mathbb{R}$ реалних или $\mathbb{C}$ комплексних бројева. Другим речима, аритметичке функције су низови реалних или комплексних бројева.

дефинисану помоћу (7.3). Штавише, та аритметичка функција је и мултипликативна[12)].

Важна својства Лежандровог симбола следе директно из *Ојлеровог критеријума* кога уводимо на основу *Фермаове теореме*[13)]. Зато се прво подсетимо Фермаове теореме, [22, стране 109 и 110].

Теорема 7.5. [Фермаова теорема] За сваки цео број a и прост број p важи $a^p \equiv a \pmod p$, као и томе еквивалентна импликација

$$p \nmid a \quad \Rightarrow \quad a^{p-1} \equiv 1 \pmod p. \qquad \square$$

Сада, на основу [32, страна 68], можемо формулисати Ојлеров критеријум.

Теорема 7.6. [Ојлеров критеријум] За сваки цео број a и непаран прост број p важи

$$p \nmid a \quad \Rightarrow \quad a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p. \qquad \square$$

Својства Лежандровог симбола, дата су следећим тврђењем, [32, стране 68, 69, 70, 72 и 75] и [19, стране 168, 169, 170 и 172].

Тврђење 7.1. Нека су p и q различити непарни прости бројеви и a, b цели бројеви. Тада важи:

1° ако је $a \equiv b \not\equiv 0 \pmod p$, онда је $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

2° ако $p \nmid a, b$, онда је $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ (мултипликативност);

3° ако је $p \geq 3$, онда је $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{за } p \equiv 1 \pmod 4 \\ -1, & \text{за } p \equiv 3 \pmod 4; \end{cases}$

4° ако је $p \geq 3$, онда је $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \begin{cases} 1, & \text{за } p \equiv \pm 1 \pmod 8 \\ -1, & \text{за } p \equiv \pm 3 \pmod 8; \end{cases}$

5° $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, то јест $\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right), & \text{за } p \equiv q \equiv -1 \pmod 4 \\ \left(\frac{p}{q}\right), & \text{иначе.} \end{cases}$

При том, само тврђење под 5° називамо *Гаусов закон квадратног реципроцитета*. $\square$

[12)] Аритметичка функција $f : \mathbb{N} \to \mathbb{C}$ је *мултипликативна* ако је $f(1) = 1$ и $f(mn) = f(m) \cdot f(n)$, за све $(m, n) = 1$, то јест ако она поштује мултипликативну структуру природних бројева

[13)] Ову Фермаову теорему често називамо и *мала Фермаова теорема* да би је разликовали од другог Фермаовог тврђења званог Велика Фермаова теорема.

Пример 7.6. На основу својстава из тврђења (7.1) и чињенице да је 2311 прост број, можемо показати да је $\left(\frac{2013}{2311}\right) = -1$. Заиста,

$$\left(\frac{2013}{2311}\right) = \left(\frac{3\cdot 11\cdot 61}{2311}\right) = \left(\frac{3}{2311}\right)\left(\frac{11}{2311}\right)\left(\frac{61}{2311}\right)$$
$$\left(\frac{3}{2311}\right) = -\left(\frac{2311}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$
$$\left(\frac{11}{2311}\right) = -\left(\frac{2311}{11}\right) = -\left(\frac{210\cdot 11+1}{11}\right) = -\left(\frac{1}{11}\right) = -1,$$
$$\left(\frac{61}{2311}\right) = (-1)^{\frac{61-1}{2}\frac{2311-1}{2}}\left(\frac{2311}{61}\right) = \left(\frac{2311}{61}\right) = \left(\frac{37\cdot 61+54}{61}\right) = \left(\frac{2\cdot 3^3}{61}\right) =$$
$$= \left(\frac{2}{61}\right)\left(\frac{3}{61}\right)^3 = (-1)^{\frac{61^2-1}{8}}\left(\frac{61}{3}\right)^3 = (-1)^{465}\left(\frac{1}{3}\right)^3 = -1,$$
$$\left(\frac{2013}{2311}\right) = (-1)(-1)(-1) = -1. \qquad \triangle$$

Дефинишимо сада уопштење Лежандровог симбола на поље $\mathbb{F}_p$.

Дефиниција 7.12. Нека је x из $\mathbb{F}_p$ и $\mathbb{F}_p^*$ мултипликативна група поља $\mathbb{F}_p$. Тада је

$$\left(\frac{x}{\mathbb{F}_p}\right) = \begin{cases} 1, & \text{ако једначина } t^2 = x \text{ има решење } t \in \mathbb{F}_p^* \\ -1, & \text{ако једначина } t^2 = x \text{ нема решење } t \in \mathbb{F}_p \\ 0, & \text{ако је } x = 0. \end{cases}$$

• Ред групе $E(\mathbb{F}_p)$

Нека је $P[X : Y : Z]$ произвољна тачка пројективног простора $\mathbb{P}^2(\mathbb{Z})$ таква да су X, Y и Z цели бројеви који нису дељиви са p и од којих је бар један различит од нуле. Видели смо да се цео пројективни простор $\mathbb{P}^n(\mathbb{Q})$, односно $\mathbb{P}^n(\mathbb{Z})$ може редуковати у пројективни простор $\mathbb{P}^n(\mathbb{F}_p)$. Према [33, страна 32] важи

Став 7.3. Нека је $E/\mathbb{Q}$ елиптичка крива са добром редукцијом у p. Тада је редукција по модулу p

$$E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$$

дефинисана са

$$\mathbb{P}^2(\mathbb{Z}) \ni P[X : Y : Z] \mapsto [\overline{X} : \overline{Y} : \overline{Z}] \in \overline{E}(\mathbb{F}_p)$$

хомоморфизам група. Он пресликава $\mathcal{O}$ из $E(\mathbb{Q})$ у $\mathcal{O}$ из $E(\mathbb{F}_p)$. $\square$

Надаље, због једноставности, групу $\overline{E}(\mathbb{F}_p)$ тачака редукција по модулу p елиптичке криве $E/\mathbb{Q}$ ћемо означавати са $E(\mathbb{F}_p)$, односно уместо $\overline{E}$ писаћемо E.

Број $|E(\mathbb{F}_p|$ елемената групе $E(\mathbb{F}_p)$, то јест ред групе $E(\mathbb{F}_p)$, односно број тачака на елиптичкој кривој $E(\mathbb{F}_p)$ означаваћемо са $\#E(\mathbb{F}_p)$.

Пример 7.7. Нека је $E : y^2 = x^3 + x + 3$ крива над пољем $\mathbb{F}_7$. Она је и елиптичка јер је

$$\Delta(E) = -2^4 \cdot 13 \cdot 19 \quad \text{и} \quad 7 \nmid 2^4 \cdot 13 \cdot 19.$$

Заменом $x = 0$, $x = 1$, $x = 2$, $x = 3$, $x = 4$, $x = 5$ и $x = 6$ у једначину елиптичке криве E добијамо, редом, $y^2 = 3$, $y^2 = 5$, $y^2 = 6$, $y^2 = 5$, $y^2 = 1$, $y^2 = 0$ и $y^2 = 1$ у $\mathbb{F}_7$. С обзиром да су бројеви 0, 1, 2 и 4 једини квадрати у пољу $\mathbb{F}_7$, само за $x = 4$, $x = 5$ и $x = 6$ можемо наћи одговарајуће y. Како је

$$y^2 \equiv 1 \,(\mathrm{mod}\, 7) \Leftrightarrow y \equiv \pm 1 \,(\mathrm{mod}\, 7) \Leftrightarrow y \equiv 1 \,(\mathrm{mod}\, 7) \vee y \equiv 6 \,(\mathrm{mod}\, 7),$$
$$y^2 \equiv 0 \,(\mathrm{mod}\, 7) \Leftrightarrow y \equiv 0 \,(\mathrm{mod}\, 7),$$

можемо закључити да је

$$E(\mathbb{F}_7) = \{\mathcal{O}, (4,1), (4,6), (5,0), (6,1), (6,6)\},$$

па је $\#E(\mathbb{F}_7) = 6$. Све ово можемо представити и помоћу табеле.

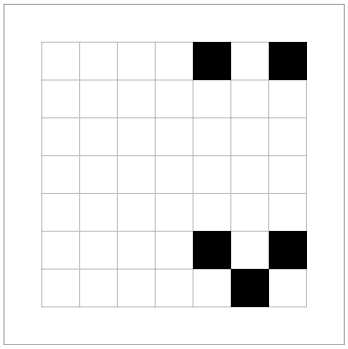
$E/\mathbb{F}_7 : y^2 = x^3 + x + 3$							
x или y	0	1	2	3	**4**	**5**	**6**
$x^3 + x + 3 \,(\mathrm{mod}\, 7)$	3	5	6	5	**1**	**0**	**1**
$y^2 \,(\mathrm{mod}\, 7)$	0	1	4	2	2	4	1

Означимо тачку $(4,1)$ са P, и рачунајмо nP за $n = 2, 3, \ldots$ Добијамо:

$$2P = (6,6),\ 3P = (5,0),\ 4P = (6,1),\ 5P = (4,6) \quad \text{и} \quad 6P = \mathcal{O},$$

одакле закључујемо да је $E(\mathbb{F}_7)$ циклична група реда 6 чији је генератор тачка $(4,1)$. Све тачке елиптичке криве $E/\mathbb{F}_7 : y^2 = x^3 + x + 3$ осим тачке $\mathcal{O}$ приказане су на следећем цртежу. △

$E/\mathbb{F}_7 : y^2 = x^3 + x + 3$



Пример 7.8. Нека је $E : y^2 = x^3 + 2x + 1$ елиптичка крива над пољем $\mathbb{F}_5$.

$E/\mathbb{F}_5 : y^2 = x^3 + 2x + 1$					
x или y	**0**	**1**	2	**3**	4
$x^3 + 2x + 1 \pmod 5$	**1**	**4**	3	**4**	3
$y^2 \pmod 5$	0	1	4	4	1

На основу података из табеле, видимо да је

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0,1), (0,4), (1,2), (1,3), (3,2), (3,3)\},$$

па је $\#E(\mathbb{F}_5) = 7$. Како је ред ове групе прост број, она је циклична и свака њена тачка, осим тачке $\mathcal{O}$ у бесконачности, је њен генератор, то јест ред сваке њене тачке, осим тачке $\mathcal{O}$ је једнак реду групе, односно

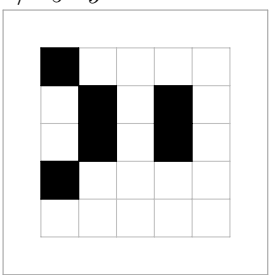
$$|(0,1)| = |(0,4)| = |(1,2)| = |(1,3)| = |(3,2)| = |(3,3)| = 7.$$

Означимо $P = (0,4)$, и покажимо да је она заиста један од генератора. Рачуном добијамо да је

$$2P = P + P = (1,2), \quad 3P = 2P + P = (3,2), \quad 4P = 3P + P = (3,3),$$
$$5P = 4P + P = (1,3), \quad 6P = 5P + P = (0,1), \quad 7P = 6P + P = \mathcal{O},$$

па је тачка $(0,4)$ заиста један од генератора циклične групе $E(\mathbb{F}_5)$ и, у том случају је $E(\mathbb{F}_5) = \{k(0,4) \mid k = 0,1,2,3,4,5,6\}$. Све тачке елиптичке криве $E/\mathbb{F}_5 : y^2 = x^3 + 2x + 1$ осим тачке $\mathcal{O}$ приказане су на следећем цртежу. △

$E/\mathbb{F}_5 : y^2 = x^3 + 2x + 1$



Пример 7.9. Нека је $E : y^2 = x^3 + 5x + 3$ елиптичка крива над пољем $\mathbb{F}_7$.

$E/\mathbb{F}_7 : y^2 = x^3 + 5x + 3$							
x или y	0	**1**	**2**	3	4	5	**6**
$x^3 + 5x + 3 \pmod 7$	3	**2**	**0**	3	3	6	**4**
$y^2 \pmod 7$	0	1	4	2	2	4	1

На основу података из табеле, видимо да је

$$E(\mathbb{F}_7) = \{\mathcal{O}, (1,3), (1,4), (2,0), (6,2), (6,5)\},$$

то јест $\#E(\mathbb{F}_7) = 6$. Како је и

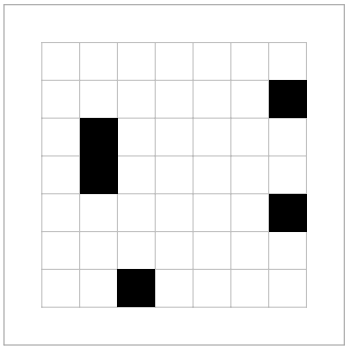
P	$2P$	$3P$	$4P$	$5P$	$6P$
(1,3)	$(6,2)$	$(2,0)$	$(6,5)$	$(1,4)$	$\mathcal{O}$
(1,4)	$(6,5)$	$(2,0)$	$(6,2)$	$(1,3)$	$\mathcal{O}$
$(2,0)$	$\mathcal{O}$				
$(6,2)$	$(6,5)$	$\mathcal{O}$			
$(6,5)$	$(6,2)$	$\mathcal{O}$			

видимо да је

$$|(1,3)| = 6, |(1,4)| = 6, |(2,0)| = 2, |(6,2)| = 3, |(6,5)| = 3,$$

одакле закључујемо да је група $E(\mathbb{F}_7)$ циклична и да су тачке $(1,3)$ и $(1,4)$ њени генератори. Све тачке елиптичке криве $E/\mathbb{F}_7 : y^2 = x^3 + 5x + 3$ осим тачке $\mathcal{O}$ приказане су на следећем цртежу. △

$E/\mathbb{F}_7 : y^2 = x^3 + 5x + 3$



Пример 7.10. Нека је $E : y^2 = x^3 + 3x$ елиптичка крива над пољем $\mathbb{F}_5$.

$E/\mathbb{F}_5 : y^2 = x^3 + 3x$					
x или y	**0**	1	**2**	**3**	4
$x^3 + 3x \pmod 5$	**0**	2	**0**	**0**	3
$y^2 \pmod 5$	0	1	4	4	1

На основу података из табеле, видимо да је

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0,0), (2,0), (3,0)\},$$

то јест $\#E(\mathbb{F}_5) = 4$. Како је и

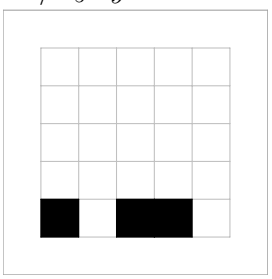
P	$2P$	$3P$	$4P$
$(0,0)$	$\mathcal{O}$		
$(2,0)$	$\mathcal{O}$		
$(3,0)$	$\mathcal{O}$		

видимо да је

$$|(0,0)|= |(2,0)|= |(3,0)|= 2,$$

то јест не постоји тачка чији је ред једнак реду групе, па закључујемо да група $E(\mathbb{F}_5)$ није циклична. Она је пример Клајнове[14)] четворне групе[15)] $V = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Све тачке елиптичке криве $E/\mathbb{F}_5 : y^2 = x^3 + 3x$ осим тачке $\mathcal{O}$ приказане су на следећем цртежу. △

$E/\mathbb{F}_5 : y^2 = x^3 + 3x$



Ако је $E : y^2 = x^3 + ax + b$, тада за свако $x \in \mathbb{F}_p$ имамо 0 тачака ако $x^3 + ax + b$ није квадратни остатак по модулу p, 1 тачку ако је $x^3 + ax + b$ дељиво са p, и 2 тачке ако је $x^3 + ax + b$ квадратни остатак по модулу p и није дељиво са p. То све можемо записати помоћу Лежандровог симбола

$$1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + ax + b}{\mathbb{F}_p} \right) \right) = 1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{\mathbb{F}_p} \right),$$

при чему смо број 1 испред знака за суму додали због тачке $\mathcal{O}$. Отуда, према [33, страна 34] и следеће

Тврђење 7.2. Ред $\#E(\mathbb{F}_p)$ групе $E(\mathbb{F}_p)$ елиптичке криве $E : y^2 = x^3 + ax + b$ дат је са

$$\#E(\mathbb{F}_p) = 1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{\mathbb{F}_p} \right). \square \tag{7.4}$$

Рачунање реда $\#E(\mathbb{F}_p)$ за велике p-ове није једноставан проблем. Међутим, у применама су p-ови врло мали јер бирамо најмање непарне p-ове који не

[14)] Феликс Кристијан Клајн (Felix Christian Klein, 1849–1925), немачки математичар

[15)] *Клајнова четворна група* V_4 је Абелова група у којој је сваки елемент инверзан самом себи дефинисана над скупом $\{0, a, b, c\}$ на следећи начин: 0 је неутрал, док за преостала три елемента важи $2a = 2b = 2c = 0$, $a + b = b + a = c$, $b + c = c + b = a$ и $c + a = a + c = b$.

деле дискриминанту Δ, тако да је за рачунање $\#E(\mathbb{F}_p)$ сасвим задовољавајућа формула (7.4).

Пример 7.11. Одредимо ред групе $E(\mathbb{F}_5)$ елиптичке криве $y^2 = x^3+4x+2$. Како је $\mathbb{F}_5 = \{0,1,2,3,4\}$, биће

$$\left(\frac{0^3+4\cdot 0+2}{\mathbb{F}_5}\right) = \left(\frac{2}{\mathbb{F}_5}\right) = -1, \qquad \left(\frac{1^3+4\cdot 1+2}{\mathbb{F}_5}\right) = \left(\frac{7}{\mathbb{F}_5}\right) = -1,$$
$$\left(\frac{2^3+4\cdot 2+2}{\mathbb{F}_5}\right) = \left(\frac{18}{\mathbb{F}_5}\right) = -1, \qquad \left(\frac{3^3+4\cdot 3+2}{\mathbb{F}_5}\right) = \left(\frac{41}{\mathbb{F}_5}\right) = 1,$$
$$\left(\frac{4^3+4\cdot 4+2}{\mathbb{F}_5}\right) = \left(\frac{82}{\mathbb{F}_5}\right) = -1,$$

па је

$$\#E(\mathbb{F}_5) = 1+5+\sum_{x\in\mathbb{F}_5}\left(\frac{x^3+4x+2}{\mathbb{F}_5}\right) = 1+5-1-1-1+1-1 = 3.$$

Дакле, елиптичка крива $E/\mathbb{F}_5 : y^2 = x^3+4x+2$ има три тачке, од којих је једна тачка $\mathcal{O}$. △

• Процена реда групе $E(\mathbb{F}_p)$

Видели смо да је формула (7.4) ефикасна за врло мале p-ове. За $p > 10^4$ она је практично неприменљива. Због тога не можемо увек одредити ред $\#E(\mathbb{F}_p)$, па зато вршимо његову процену.

Како ће за половину x-ева x^3+ax+b бити квадратни остатак по модулу p, а за другу половину неће, очекујемо да ће у просеку бити

$$\#E(\mathbb{F}_p) = 2\cdot\frac{p}{2}+0\cdot\frac{p}{2}+1 = p+1,$$

то јест

$$\#E(\mathbb{F}_p) \approx p+1,$$

односно $\#E(\mathbb{F}_p)$ не може бити превише далеко од $p+1$. Због тога је

$$p+1-\varepsilon \le \#E(\mathbb{F}_p) \le p+1+\varepsilon$$

за неку грешку ε, то јест

$$|\#E(\mathbb{F}_p) - p - 1| \le \varepsilon.$$

Показује се да је $\varepsilon = 2\sqrt{p}$. Отуда и следећа теорема позната под називом Хасеова теорема. Она нам даје процену реда $\#E(\mathbb{F}_p)$ групе $E(\mathbb{F}_p)$, [33, страна 34].

Теорема 7.7. [**Хасе**] За елиптичку криву $E/\mathbb{F}_p$ важи

$$|\#E(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}. \ \square \tag{7.5}$$

Релација (7.5) позната је и као *Хасеова оцена*.

Пример 7.12. Испитајмо да ли постоје елиптичке криве $E/\mathbb{F}_{41}$ такве да је $\#E(\mathbb{F}_{41}) = 25$ или $\#E(\mathbb{F}_{41}) = 55$. У овом случају је $p = 41$ и важи

$$\#E(\mathbb{F}_{41}) = 1 + p + \varepsilon = 1 + 41 + \varepsilon = 42 + \varepsilon,$$

где је

$$|\varepsilon| \leq 2\sqrt{p} = 2\sqrt{41} = \sqrt{164}.$$

Како је $12 < \sqrt{164} < 13$, то је $-12 \leq \varepsilon \leq 12$, па је

$$42 - 12 = 30 \leq \#E(\mathbb{F}_{41}) \leq 54 = 42 + 12.$$

Дакле, не постоје такве елиптичке криве, јер $\#E(\mathbb{F}_{41}) = 25$ и $\#E(\mathbb{F}_{41}) = 55$ не припадају сегменту $[30, 54]$. $\triangle$

За елиптичке криве над пољем $\mathbb{F}_p$ Хасеова оцена је најбоља могућа, у смислу да за сваки природан број

$$n \in (p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$$

постоји елиптичка крива над $\mathbb{F}_p$ реда $\#E(\mathbb{F}_p) = n$. Ова чињеница, која је својеврстан обрат Хасеове теореме, је позната и као Дојрингова[16] теорема. Пре него што формулишемо ту теорему, дефинишимо Хасеов интервал, [15, страна 511].

Дефиниција 7.13. Интервал $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ називамо *Хасеов интервал* и означавамо са $\mathcal{H}(p)$, то јест

$$\mathcal{H}(p) = (p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}) = ((\sqrt{p} - 1)^2, (\sqrt{p} + 1)^2).$$

На основу [15, страна 511], важи

Теорема 7.8. [**Дојринг**] За сваки природан број n из $\mathcal{H}(p)$ постоји елиптичка крива $E/\mathbb{F}_p$ таква да је $\#E(\mathbb{F}_p) = n$. $\square$

У применама, често бирамо елиптичке криве E чији ред $\#E(\mathbb{F}_p)$ има неко задато аритметичко својство – прост је, има само мале просте факторе, и слично. Притом је јако важна чињеница, [15, страна 511], коју је доказао Ленстра[17], а која каже да ће редови $\#E(\mathbb{F}_p)$ елиптичких кривих E над коначним пољем $\mathbb{F}_p$, за (a, b) из $\mathbb{F}_p \times \mathbb{F}_p$, имати «скоро униформну» расподелу унутар интерва-

[16] Макс Дојринг (Max Deuring, 1907–1984), немачки математичар

[17] Хендрик Вилем Ленстра (Hendrik Willem Lenstra, 1949), немачки математичар

ла $(p+1-\sqrt{p}, p+1+\sqrt{p})$. То значи да ће ред случајно одабране елиптичке криве E над $\mathbb{F}_p$ имати задато својство са приближно истом вероватноћом као и случајно одабран природан број реда величине као p.

Иако у релацији (7.5) једнакост никад не наступи, тај облик се традиционално пише јер важи и за свако коначно поље са $q = p^n$ елемената, то јест важи

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

На крају напоменимо да важи и уопштење Хасеове теореме (7.7). Први њен доказ је дао Вej. Због тога, она је позната под именом Хасе–Вејова теорема, [33, страна 35].

Теорема 7.9. [Хасе-Вej] Нека је C глатка алгебарска крива рода g над пољем $\mathbb{F}_p$. Тада је

$$|\#E(\mathbb{F}_p) - p - 1| \leq 2g\sqrt{p}. \qquad \square$$

• Фробенијусов траг елиптичке криве

Према [15, страна 511] имамо

Дефиниција 7.14. Величину $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$ називамо *Фробенијусов*[18] *траг елиптичке криве* $E/\mathbb{F}_p$.

Ако је јасно о којој елиптичкој кривој E је реч, често ћемо уместо $a_p(E)$ писати само a_p. На основу Хасеове теореме (7.7) важи

$$|a_p| \leq 2\sqrt{p}.$$

Лако можемо закључити, на основу дефиниције (7.14), да је проблем израчунавања реда $\#E(\mathbb{F}_p)$ еквивалентан проблему израчунавања Фробенијусовог трага a_p елиптичке криве $E/\mathbb{F}_p$, што се најбоље види приликом одређивања реда $\#E(\mathbb{F}_p)$ у случају када је $q = p^n$. О томе нам управо говори следећа теорема, [17, страна 205].

Теорема 7.10. Нека је $q = p^n$. Тада постоји елиптичка крива $E/\mathbb{F}_q$ таква да је $\#E(\mathbb{F}_q) = q + 1 - a_p$ ако и само ако је $|a_p| \leq 2\sqrt{q}$ и a_p задовољава један од следећих услова:

1° $(a_p, p) = 1$;

2° n је паран и $a_p = \pm 2\sqrt{q}$ или $(a_p = \pm\sqrt{q}$ и $p \not\equiv 1 \pmod 3)$ или $(a_p = 0)$ и $p \not\equiv 1 \pmod 4)$;

3° n је непаран и $a_p = 0$ или $(a_p = \pm\sqrt{2q}$ и $p = 2)$ или $(a_p = \pm\sqrt{3q}$ и $p = 3)$. $\square$

[18] Фердинанд Георг Фробенијус (Ferdinand Georg Frobenius, 1849–1917), немачки математичар

• **Аномалне и суперсингуларне елиптичке криве**

На основу Фробенијусовог трага дефинисаћемо још два типа елиптичких кривих, [17, страна 207].

Дефиниција 7.15. Елиптичка крива $E/\mathbb{F}_p$ је *аномална* ако је њен Фробенијусов траг $a_p = 1$, то јест ако је $\#E(\mathbb{F}_p) = p$.

Дефиниција 7.16. Елиптичка крива $E/\mathbb{F}_p$, где је $q = p^k$, је *суперсингуларна* ако карактеристика p поља $\mathbb{F}_q$ дели њен Фробениусов траг a_q.

• **Структура групе $E(\mathbb{F}_p)$**

О структури групе $E(\mathbb{F}_p)$ говори нам следећа теорема, [15, страна 512].

Теорема 7.11. Нека је $E/\mathbb{F}_p$ елиптичка крива. Тада је

$$E(\mathbb{F}_p) = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

где су n_1 и n_2 природни бројеви, $n_1 \mid n_2$ и $n_1 \mid p-1$. □

Ако је $n_1 = 1$, онда је група $E(\mathbb{F}_p)$ циклична. Из услова да $n_1 \mid (n_2, p-1)$ закључујемо да се може очекивати да ће, у општем случају, n_1 бити мали природан број , а група $E(\mathbb{F}_p)$ «скоро циклична».

• **Торзија елиптичке криве и редукција по модулу p**

Проблем са применом Луц-Нагелове теореме (6.7) може се јавити ако је тешко факторисати дискриминанту Δ или ако она има пуно квадратних фактора. Следећи став нам показује како помоћу редукције по модулу p можемо наћи торзију $\mathcal{T}or(E)$ елиптичке криве $E/\mathbb{Q}$ и одредити ред $\#\mathcal{T}or(E)$, уз напомену да тај поступак није алгоритам као што нам даје Луц-Нагелова теорема (6.7), [33, страна 32].

Став 7.4. Нека је $E/\mathbb{Q}$ елиптичка крива и p прост број. Ако $E/\mathbb{Q}$ има добру редукцију у p, тада је рестрикција редукције по модулу p на торзиону подгрупу

$$\rho_p : \mathcal{T}or(E) \to E(\mathbb{F}_p)$$

инјективни хомоморфизам. □

Како је ρ_p инјективни хомоморфизам, његово језгро[19] $\operatorname{Ker}\rho_p$ је тривијално, па је $\mathcal{T}or(E)$ изоморфна слици $\operatorname{Im}\rho_p$ тог хомоморфизма, а то је подгрупа од

[19] то јест скуп свих елемената из $\mathcal{T}or(E)$ који се пресликају у неутрални елемент $\mathcal{O}$ из $E(\mathbb{F}_p)$

$E(\mathbb{F}_p)$. Одавде закључујемо да

$$\#\mathcal{T}or(E) \mid \#E(\mathbb{F}_p),$$

јер ред подгрупе дели ред групе. Ово својство ћемо искористити приликом израчунавања $\#\mathcal{T}or(E)$. Узећемо неколико вредности за p, и тада највећи заједнички делилац тако добијених $\#E(\mathbb{F}_p)$ мора бити садржалац од $\#\mathcal{T}or(E)$.

Пример 7.13. Одредимо торзију елиптичке криве $E/\mathbb{Q} : y^2 = x^3+18x+72$. Како је $4a^3+27b^2 = 4\cdot 18^3+27\cdot 72^2 = 163\,296 = 2^5\cdot 3^6\cdot 7$, према Луц-Нагеловој теореми (6.7) требамо проверити све делиоце $y \mid 108$. Уместо тога, можемо проверити да је $\#E(\mathbb{F}_5) = 5$ и $\#E(\mathbb{F}_{11}) = 8$. С обзиром да је $(5, 8) = 1$, можемо закључити да је торзија $\mathcal{T}or(E)$ дате елиптичке криве тривијална, то јест $\mathcal{T}or(E) = \{\mathcal{O}\}$. △

7.4 L-функције и елиптичке криве

• Дефиниција L-функције

Елиптичке криве можемо проучавати и помоћу L-функција, зато што свакој елиптичкој кривој можемо придружити неку L функцију. На основу [44, страна 14] и [15, страна 500] имамо

Дефиниција 7.17. Нека је $E/\mathbb{Q}$ елиптичка крива. Тада је њена L-функција дефинисана са

$$L(E; s) = \prod_p \left(1 - \frac{a_p}{p^s} + p^{1-2s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{7.6}$$

при чему је s комплексан број, $a_p = p+1-N_p$ за p-ове у којима E има добру редукцију, $a_p = 0$ у случају адитивне редукције, $a_p = 1$ у случају мултипликативне расцепиве, а $a_p = -1$ у случају мултипликативне нерасцепиве редукције.

Фробенијусов траг a_p користили смо у облику $a_p = p + 1 - N_p$[20], при чему је $N_p = \#E(\mathbb{F}_p)$ број решења једначине $y^2 \equiv x^3+ax+b \pmod p$, за $x = 0, \ldots, p-1$.

L-функцију елиптичке криве E можемо схватити као аналогон Риманове ζ функције, ако се подсетимо Ојлерове формуле

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - p^{-s}\right)^{-1}.$$

Производ (7.6) конвергира за $\Re(s) > \frac{3}{2}$. Ако формално уврстимо $s = 1$ у (7.6),

[20] Уместо a_p, односно N_p користе се и ознаке $a(p)$, односно $A(p)$.

добићемо

$$L(E;1)=\prod_p\left(1-\frac{a_p}{p}+\frac{1}{p}\right)^{-1}=\prod_p\left(\frac{p-a_p+1}{p}\right)^{-1}=\prod_p\left(\frac{N_p}{p}\right)^{-1}$$

то јест

$$L(E;1)=\prod_p\frac{p}{N_p}. \tag{7.7}$$

На основу (7.7) можемо закључити да ако је, у просеку, N_p веће од p тада ће производ (7.7) конвергирати.

• Бирч и Свинертон-Дајерова хипотеза

Нека је $E/\mathbb{Q}$ елиптичка крива са добром редукцијом у p. Видели смо, према ставу (7.3), да редукција по модулу p индукује хомоморфизам група

$$E(\mathbb{Q})\to E(\mathbb{F}_p).$$

Бирч и Свинертон-Дајер су уочили да ако је већа група $E(\mathbb{Q})$ и групе $E(\mathbb{F}_p)$ биће у просеку веће. Другим речима, ако елиптичка крива $E/\mathbb{Q}$ има «много» рационалних тачака, то јест већи ранг, она ће имати и «много» тачака при редукцији по модулу p, то јест број N_p ће бити велик за «већину» p-ова. То их је 1965. године довело до формулације следећег проблема, [5, страна 12].

Хипотеза. [Бирч и Свинертон-Дајер] Нека је $f(P)=\prod_{p\le P}\frac{N_p}{p}$. Тада је

$$f(P)\sim C(\log P)^r,$$

када $P\to\infty$, где је r ранг елиптичке криве $E/\mathbb{Q}$ и C константа која зависи од те елиптичке криве.

С друге стране, функција $L(E;s)$ има аналитичко продужење на неку околину тачке $s=1$, што су 1995. године доказали Вајлс и Тејлор[21)]. То нам омогућава да Бирч и Свинертон-Дајерову хипотезу искажемо и помоћу L-функције, [44, страна 15].

Хипотеза. [Бирч и Свинертон-Дајер] Тејлоров развој од $L(E;s)$ у $s=1$ има облик

$$L(E;s)=c(s-1)^r+\text{чланови вишег реда},$$

при чему је $c\neq 0$ константа, а r ранг елиптичке криве $E/\mathbb{Q}$.

Из ове хипотезе, према [60, страна 2], за $s=1$, можемо закључити да је $L(E;1)=0$ ако и само ако елиптичка крива $E/\mathbb{Q}$ има бесконачно много рационалних тачака.

[21)] Ричард Лоренс Тејлор (Richard Lawrence Taylor, 1962), британски и амерички математичар

Решење овог проблема – који је и један од најизазовнијих проблема – водило би решењу многих проблема везаних за Диофантове једначине. Од 2017. године доказани су само специјани случајеви ове хипотезе.

Бирч и Свинертон-Дајерова хипотеза[22)] је један од *седам миленијумских проблема* који су познати и под називом *проблеми за миленијумску награду*. То су проблеми постављени пре више стотина година, али и они постављени последњих деценија. Сви они се сврставају међу најтеже математичке проблеме на свету. За решење сваког од припремљених проблема, Клејов институт је понудио награду од чак милион долара. Зато математичари, у шали, кажу да је најтежи начин да се заради милион долара управо тај да се реши неки од ових проблема, то јест докаже нека од постављених хипотеза!

До сада, само један од седам миленијумских проблема је решен! Перељман[23)], добитник Филдсове медаље, решио је Поенкареову хипотезу[24)] – један од највећих и централних проблема геометријске топологије, који се, најкраће речено, своди на описивање тродимензионалних површи у четвородимензионалном простору. Клејов институт је 18. марта 2010. године објавио да су испуњени услови за доделу прве миленијумске награде од милион долара.

Награда ипак није додељена, јер је Перељман одбио и признање и новац за решење тог проблема[25)]. Он је тада изјавио да није у реду да награду не добије и Хамилтон[26)] чије је идеје искористио и модификовао. Тако Перељман испред свега ставља науку и њене резултате, а не материјална добра[27)].

[22)] Birch and Swinnerton-Dyer Conjecture

[23)] Григорије Перељман (Григо́рий Перельма́н, 1966), руски математичар

[24)] Poincaré Conjecture

[25)] Занимљиво је да је Перељман овај доказ написао на крајње оригиналан начин. Колико је доказ био језгровит сведочи и чињеница да је врхунским математичарима било потребно четири године да на око 500 страна разраде оно што је Перељман написао на 58 страна.

[26)] Ричард Хамилтон (Richard Hamilton, 1943), амерички математичар

[27)] Перељман је 2006. године, иако је добио Филдсову медаљу, одбио да прими и ту награду. Она се састојала од 15 000 канадских долара и златне медаље. Није се ни појавио на Међународном конгресу математичара у Мадриду, на свечаној додели те награде, где је и званично објављено: *Доказ је тачан, Поенкареов проблем је решен!*

8

Доказ Морделове теореме

Видели смо, према Мазуру, да је торзија елиптичке криве $E/\mathbb{Q}$, то јест групе $E(\mathbb{Q})$ коначно генерисана – циклична или производ две цикличне групе. Морделова теорема тврди да је цела структура $(E(\mathbb{Q}), +)$ коначно генерисана Абелова група. У овом поглављу даћемо идеју доказа Морделове теореме. За више детаља погледати [57], [33], [16] и [15].

Проучавање групе $E(\mathbb{Q})$, као и методи, технике и концепти које је увео Вej приликом уопштења Морделове теореме на Абелове многострукости[1)] над пољима алгебарских бројева[2)], створили су *аритметичку алгебарску геометрију*, која је изазвала револуцију у теорији бројева, али и математици уопште.

Морделова теорема је једна од *четири фундаменталне теореме* коначности Диофантове геометрије. Остале три су: *Зигелова*[3)] *теорема*[4)], *Фалтингсова теорема* и *Ротова*[5)] *теорема*[6)].

Два основна корака у доказу Морделове теореме су:

- ▷ коришћење чињенице да је индекс $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ коначан, то јест да је група $E(\mathbb{Q})/2E(\mathbb{Q})$ коначна, о чему нам говори такозвана *слаба Морделова теорема*;
- ▷ доказ да коначност групе $E(\mathbb{Q})/2E(\mathbb{Q})$ повлачи да је $E(\mathbb{Q})$ коначно генерисана група. Кључна идеја у овом доказу ће бити да множење са

[1)] *Абелове многострукости* су алгебарске многострукости које су уједно и Абелове групе.

[2)] Тако је настала *Мордел – Вејова теорема*: Нека је E елиптичка крива над пољем алгебарских бројева $\mathbb{K}$. Тада је $E(\mathbb{K})$ коначно генерисана Абелова група, [33, страна 13].

[3)] Карл Лудвиг Зигел (Carl Ludwig Siegel, 1896–1981), немачки математичар

[4)] Свака афина крива рода $g \geq 1$ има коначно много тачака са целобројним координатама, [19, страна 283].

[5)] Клаус Рот (Klaus Roth, 1925), британски математичар немачког порекла

[6)] За сваки ирационалан алгебарски број α и свако $\varepsilon > 0$, постоји коначно много рационалних бројева $\frac{p}{q}$ таквих да је $|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\varepsilon}}$, [19, страна 283].

2 «повећава» координате тачака на елиптичкој кривој, и да постоји коначно много тачака «мањих» од неке, унапред задате, величине. За то ће нам бити потребно да, на неки начин, измеримо «величину» тачке, у чему ће нам помоћи *функција висине*. О свему томе нам говори *теорема о спусту*.

8.1 Слаба Морделова теорема

• Формулација

На основу [16, 11. лекција, страна 1] важи

Теорема 8.1. Нека је $E/\mathbb{Q}$ елиптичка крива. Тада је индекс $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ подгрупе $2E(\mathbb{Q})$ у групи $E(\mathbb{Q})$ коначан.

• Множење са 2

Ради једноставности, групу $E(\mathbb{Q})$ означимо са Г. Њена подгрупа $2E(\mathbb{Q}) = 2\Gamma$ се састоји од свих рационалних тачака које су, слободније речено, два пута нека рационална тачка из Г.

С друге стране, операција *множење са* 2

$$P \mapsto 2P = P + P \qquad E \to E \tag{8.1}$$

је један хомоморфизам групе $(E, +)$ који свакој тачки P на E додељује тачку $2P$ на E.

Да бисмо избегли прелазак у поље алгебарских бројева, доказ слабе Морделове теореме извешћемо за елиптичку криву $E/\mathbb{Q}$ која има рационалну тачку реда 2, то јест

$$E/\mathbb{Q} : y^2 = (x - e)(x^2 + ax + b), \tag{8.2}$$

при чему су a, b и e цели бројеви. Ако уведемо смену координата тако да ту тачку померимо у координатни почетак, тада је $T = (0, 0)$ њена рационална тачка реда 2 и (8.2) постаје

$$E/\mathbb{Q} : y^2 = x(x^2 + ax + b),$$

односно

$$E/\mathbb{Q} : y^2 = x^3 + ax^2 + bx. \tag{8.3}$$

Дискриминанта те елиптичке криве износи

$$\Delta = b^2(a^2 - 4b),$$

па како она није сингуларна, важиће и $b \neq 0$ и $a^2 \neq 4b$. Пре него што докажемо слабу Морделову теорему, упознајмо хомоморфизме које ћемо користити приликом извођења тог доказа.

• Изогеније елиптичких кривих

Посматрајући формуле (5.6) и (5.7) – за које кажемо да су и *формуле за дуплирање тачке* – уочавамо да оне нису једноставне. Због тога, операцију множење са 2 ћемо поделити на две мање и једноставније операције.

Нека је $\overline{E}$ елиптичка крива дефинисана са

$$\overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x,$$

при чему је $\overline{a} = -2a$ и $\overline{b} = a^2 - 4b$. Она је повезана са елиптичком кривом (8.3), иако на први поглед оне немају ништа заједничко. Разлог због ког нам је она значајна увиђамо када применимо исту процедуру на $\overline{E}$. Тако добијемо

$$\overline{\overline{E}} : y^2 = x^3 + \overline{\overline{a}}x^2 + \overline{\overline{b}}x,$$

при чему је $\overline{\overline{a}} = -2\overline{a} = 4a$ и $\overline{\overline{b}} = \overline{a}^2 - 4\overline{b} = 16b$. Дакле, елиптичка крива $\overline{\overline{E}}$ је дата једначином

$$\overline{\overline{E}} : y^2 = x^3 + 4ax^2 + 16bx,$$

и готово је иста као и полазна крива (8.3). Штавише, тада су и групе Γ и $\overline{\overline{\Gamma}}$ изоморфне.

Одредимо хомоморфизме са E на $\overline{E}$ и са $\overline{E}$ на $\overline{\overline{E}}$ тако да њихова композиција буде операција множење са 2. Ту ће нам помоћи следеће тврђење, [16, 11. лекција, страна 1]:

Тврђење 8.1. Нека су E и $\overline{E}$ елиптичке криве задате са

$$E : y^2 = x^3 + ax^2 + bx,$$
$$\overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x, \quad \overline{a} = -2a, \quad \overline{b} = a^2 - 4b,$$

и нека је $T = (0, 0)$ тачка на E. Тада:

1° Постоји хомоморфизам $\phi : E \to \overline{E}$ дефинисан са

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right), & \text{ако је } P = (x, y) \neq \mathcal{O}, T \\ \overline{\mathcal{O}}, & \text{ако је } P \in \{\mathcal{O}, T\}, \end{cases} \tag{8.4}$$

и његово језгро је $\operatorname{Ker}\phi = \{\mathcal{O}, T\}$.

2° Постоји хомоморфизам $\psi : \overline{E} \to E$ дефинисан са

$$\psi(\overline{P}) = \begin{cases} \left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}\right), & \text{ако је } \overline{P} = (\overline{x}, \overline{y}) \neq \overline{\mathcal{O}}, \overline{T} \\ \mathcal{O}, & \text{ако је } \overline{P} \in \{\overline{\mathcal{O}}, \overline{T}\}, \end{cases} \tag{8.5}$$

3° Композиција $\psi \circ \phi : E \to E$, односно $\phi \circ \psi : \overline{E} \to \overline{E}$ је множење са 2, то јест $(\psi \circ \phi)(P) = 2P$, односно $(\phi \circ \psi)(\overline{P}) = 2\overline{P}$, за све P са E, односно $\overline{P}$ са $\overline{E}$. □

Хомоморфизми (8.1), (8.4) и (8.5) су и примери изогенија елиптичких кривих, прецизније то су 2-изогеније. Уопште, према [33, страна 21], имамо

Дефиниција 8.1. Нека су $(E_1, \mathcal{O}_1)$ и $(E_2, \mathcal{O}_2)$ елиптичке криве. *Изогенија* између E_1 и E_2 је хомоморфизам

$$\phi : E_1 \to E_2$$

за који важи $\phi(\mathcal{O}_1) = \mathcal{O}_2$.

За елиптичке криве E_1 и E_2 кажемо да су *изогене* ако постоји изогенија из E_1 у E_2, односно, еквивалентно, из E_2 у E_1. Изогеније су хомоморфизми задати помоћу рационалних функција.

Скуп свих изогенија између елиптичких кривих E_1 и E_2 означавамо са $\mathrm{Hom}(E_1, E_2)$. На том скупу можемо задати операцију сабирања стандардно са

$$(\phi + \psi)(P) = \phi(P) + \psi(P), \tag{8.6}$$

за све изогеније ϕ и ψ из $\mathrm{Hom}(E_1, E_2)$ и сваку тачку P на елиптичкој кривој E. Уколико је $E_1 = E_2$ можемо вршити и композицију изогенија. Прецизније, за елиптичку криву E, $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ је *прстен ендоморфизама елиптичке криве* E на коме је сабирање дефинисано помоћу (8.6), а множење као композиција изогенија

$$(\phi \circ \psi)(P) = \phi(\psi(P)),$$

за све изогеније ϕ и ψ из $\mathrm{End}(E)$ и сваку тачку P на елиптичкој кривој E.

• Доказ

На почетку напоменимо да ћемо дати само скицу доказа за слабу Морделову теорему, односно показаћемо којим путем бисмо дошли до њеног доказа, и притом ћемо истакнути његове кључне кораке.

Рационалне тачке са елиптичке криве E се помоћу изогеније ϕ сликају у рационалне тачке на елиптичкој кривој $\overline{E}$, али произвољна тачка са $\overline{E}$ не мора бити слика рационалне тачке са E при тој изогенији.

С друге стране, слике рационалних тачака из Γ, при изогенији ϕ, чине подгрупу рационалних тачака од $\overline{\Gamma}$. Означавамо је са $\phi(\Gamma)$. О томе како она изгледа, говори нам следеће тврђење, [16, 11. лекција, стране 2 и 3].

Тврђење 8.2. За подгрупу $\phi(\Gamma)$ групе Γ важи:

1° $\overline{\mathcal{O}}$ припада $\phi(\Gamma)$;

2° $\overline{T} = (0, 0)$ припада $\phi(\Gamma)$ ако и само ако је $\overline{b} = a^2 - 4b$ потпун квадрат;

3° $\overline{P} = (\overline{x}, \overline{y})$ из $\overline{\Gamma}$, при чему је $\overline{x} \neq 0$, припада $\phi(\Gamma)$ ако и само ако је $\overline{x}$ квадрат неког рационалног броја. □

Аналогно тврђење важи и за подгрупу $\psi(\overline{\Gamma})$ групе Γ, јер, као што смо видели, ψ се дефинише аналогно као и ϕ, то јест ψ је композиција ϕ и изоморфизма $(x, y) \mapsto (\frac{x}{4}, \frac{y}{8})$.

Покажимо да су индекси $[\Gamma : \psi(\overline{\Gamma})]$ и $[\overline{\Gamma} : \phi(\Gamma)]$ коначни, то јест

$$[\Gamma : \psi(\overline{\Gamma})] < +\infty \quad \text{и} \quad [\overline{\Gamma} : \phi(\Gamma)] < +\infty,$$

јер ће тада бити и

$$[\psi(\overline{\Gamma}) : \psi(\phi(\Gamma))] < +\infty,$$

односно

$$[\Gamma : 2\Gamma] = [\Gamma : \psi(\overline{\Gamma})] \cdot [\psi(\overline{\Gamma}) : \psi(\phi(\Gamma))] \leq [\Gamma : \psi(\overline{\Gamma})] \cdot [\overline{\Gamma} : \phi(\Gamma)] < +\infty,$$

при чему је $2\Gamma = \psi(\phi(\Gamma))$.

Како су индекси $[\Gamma : \psi(\overline{\Gamma})]$ и $[\overline{\Gamma} : \phi(\Gamma)]$ симетрични, довољно је доказати да је један од њих коначан. Показаћемо да је то, на пример, индекс $[\Gamma : \psi(\overline{\Gamma})]$.

Нека је $\mathbb{Q}^*$ мултипликативна група $(\mathbb{Q}\backslash\{0\}, \cdot)$ не-нула рационалних бројева, $\mathbb{Q}^{*2} = \{u^2 \mid u \in \mathbb{Q}^*\}$ њена подгрупа која се састоји од квадрата рационалних бројева који нису нула и $\mathbb{Q}^*/\mathbb{Q}^{*2}$ количничка група чији су представници -1 и 1, и природни бројеви који у свом растављању немају виших степена. Класе у $\mathbb{Q}^*/\mathbb{Q}^{*2}$ означаваћемо помоћу симбола $\widetilde{\ }$. Тада је $(\widetilde{t})^2 = \widetilde{1}$ за свако t из $\mathbb{Q}$.

Дефинишимо пресликавање $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ као

$$\begin{aligned} &\alpha(\mathcal{O}) = \widetilde{1} \\ &\alpha(T) = \widetilde{b} = b \,(\mathrm{mod}\, \mathbb{Q}^{*2}) \\ &\alpha(P) = \alpha(x, y) = \widetilde{x} = x \,(\mathrm{mod}\, \mathbb{Q}^{*2}). \end{aligned} \tag{8.7}$$

У вези са њим важи следеће, [16, 11. лекција, стране 3 и 4].

Тврђење 8.3.

1° Пресликавање α дефинисано са (8.7) је хомоморфизам.

2° Језгро $\operatorname{Ker}\alpha$ је $\psi(\overline{\Gamma})$. Због тога постоји утапање или мономорфизам

$$\Gamma/\psi(\overline{\Gamma}) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}.$$

3° Нека су $p_1, \ldots, p_k$ различити прости бројеви који деле b. Тада је $\alpha(\Gamma)$ подгрупа подгрупе од $\mathbb{Q}^*/\mathbb{Q}^{*2}$ која се састоји од елемената облика

$$\pm p_1^{\epsilon_1} \cdot p_2^{\epsilon_2} \cdot \ \cdots \ \cdot p_k^{\epsilon_k},$$

при чему ϵ_i припада скупу $\{0, 1\}$ за свако $i = 1, \ldots, k$.

4° Индекс $[\Gamma : \psi(\overline{\Gamma})] \leq 2^{k+1}$. □

Дакле, индекс $[\Gamma : 2\Gamma] = [E(\mathbb{Q}) : 2E(\mathbb{Q})]$ је коначан, па је и група $E(\mathbb{Q})/2E(\mathbb{Q})$ коначна. □

8.2 Висина тачке елиптичке криве

У доказу Морделове теореме користимо појам висине, који потиче од Фермаа. На почетку, прво ћемо дефинисати висину рационалног броја.

• Висина рационалног броја

На основу, [16, 10. лекција, страна 2] имамо

Дефиниција 8.2. За рационалан број $t = \frac{m}{n}$, при чему су m и n узајамно прости[7)], дефинишемо његову *висину* као

$$H(t) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\}.$$

Понекад висину H називамо и «наивна» висина рационалног броја. Она нам, на неки начин, говори о томе колико је дати рационалан број компликован.

• Логаритамска висина

Ако је $P = (x, y)$ афина рационална тачка која припада елиптичкој кривој $E/\mathbb{Q}$, тада њену висину дефинишемо као висину њене прве координате, [16, 10. лекција, страна 2].

Дефиниција 8.3. Нека је $P = (x, y) \in E/\mathbb{Q}$. Тада је

$$H(P) = H(x).$$

Дефинишемо и висину H бесконачно далеке тачке $\mathcal{O}$ са $H(\mathcal{O}) = 1$, [16, 10. лекција, страна 2]. На основу истог извора имамо и

Дефиниција 8.4. *Логаритамска висина* на $E(\mathbb{Q})$ је функција

$$h : E(\mathbb{Q}) \to \mathbb{R}$$

дефинисана са

$$h(P) = \begin{cases} \ln H(P), & \text{ако је } P \neq \mathcal{O} \\ 0, & \text{ако је } P = \mathcal{O}. \end{cases}$$

Приметимо да је вредност $h(P)$ увек ненегативна.

Из формула (5.4) и (5.6) за сабирање тачака на елиптичкој кривој можемо видети каква је веза између висина тачака P и $2P$, то јест колико пута се повећа број цифара у приказу тачке $2P$ у односу на приказ тачке P. Нека је $E/\mathbb{Q} : y^2 = x^3 + ax + b$ елиптичка крива, $P = (x, y)$ тачка и P_0 фиксирана

[7)] то јест разломак $\frac{m}{n}$ је «максимално» скраћен

тачка из $E(\mathbb{Q})$. Тада је

$$h(2P) \approx 4h(P) \quad \text{и} \quad h(P+P_0) \approx h(2P).$$

8.3 Три леме

Претходна разматрања ћемо прецизирати у оквиру наредне три леме. Оне представљају својства висине h.

• Формулација

Прво ћемо формулисати све три леме, [16, 10. лекција, страна 3], а затим ћемо доказати једну по једну, [16, 10. лекција, стране 3, 4 и 5].

Лема 8.1. За сваки реалан број K, скуп

$$\{P \in E(\mathbb{Q}) \mid h(P) \leq K\}$$

свих рационалних тачака на елиптичкој кривој E чија је висина мања од неког, унапред задатог, броја K је коначан, и нема више од $2(2e^K+1)^2$ елемената.

Лема 8.2. Нека је $E/\mathbb{Q} : y^2 = x^3 + ax + b$ и P_0 из $E(\mathbb{Q})$ фиксирана тачка. Тада постоји константа k_0 која зависи од P_0, a и b таква да за сваку тачку P из $E(\mathbb{Q})$ важи

$$h(P+P_0) \leq 2h(P) + k_0.$$

Лема 8.3. Нека је $E/\mathbb{Q} : y^2 = x^3 + ax + b$. Тада постоји константа k која зависи од a и b таква да за сваку тачку P из $E(\mathbb{Q})$ важи

$$h(2P) \geq 4h(P) - k.$$

• Доказ прве леме

За сваки реалан број C, скуп

$$\{t \in \mathbb{Q} \mid H(t) \leq C\}$$

је очигледно коначан. Заправо, има највише $(2C+1)^2$ елемената, јер бројилац и именилац разломка t морају бити цели бројеви између $-C$ и C. Даље, за свако x постоје највише две вредности за y такве да је $P = (x, y)$ рационална тачка елиптичке криве E. Зато је и скуп

$$\{P \in E(\mathbb{Q}) \mid h(P) \leq K\}$$

коначан. □

• Доказ друге леме

Нека је $P = (x, y)$ рационална тачка на елиптичкој кривој $E/\mathbb{Q}$. Тада су обе њене координате x и y рационални бројеви, па постоје цели бројеви m, M, n и N, такви да је

$$x = \frac{m}{M} \quad \text{и} \quad y = \frac{n}{N}, \tag{8.8}$$

при чему је $(m, M) = 1$, $(n, N) = 1$ и $M, N > 0$. Када (8.8) заменимо у једначину $y^2 = x^3 + ax + b$ елиптичке криве $E/\mathbb{Q}$, добијамо

$$\left(\frac{n}{N}\right)^2 = \left(\frac{m}{M}\right)^3 + a\left(\frac{m}{M}\right) + b,$$

то јест

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m}{M} + b,$$

односно, наком множења са N^2M^3

$$n^2M^3 = m^3N^2 + amN^2M^2 + bN^2M^3. \tag{8.9}$$

Како N^2 дели десну страну једнакости (8.9) мора да дели и њену леву страну, то јест $N^2 \mid n^2M^3$. Како је и $(n, N) = 1$ можемо закључити да $N^2 \mid M^3$.

С друге стране, из једнакости (8.9) такође следи да $M \mid N^2$. Сви сабирци на десној страни једнакости (8.9) осим m^3N^2 су дељиви са M^2, па $M^2 \mid N^2$, то јест $M \mid N$. Међутим, сада су сви сабирци осим m^3N^2 дељиви са M^3, па можемо закључити да $M^3 \mid N^2$.

Дакле, $N^2 \mid M^3$ и $M^3 \mid N^2$, одакле следи да је $N^2 = M^3$. Због тога је

$$P = (x, y) = \left(\frac{m}{M}, \frac{n}{N}\right) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right).$$

Висина тачке P је

$$H(P) = H(x) = H(\frac{m}{e^2}) = \max\{|m|, |e^2|\},$$

па је

$$|m| \leq H(P) \quad \text{и} \quad e^2 \leq H(P). \tag{8.10}$$

Сада ћемо покушати да ограничимо висину y, то јест $\frac{n}{e^3}$, односно n, јер је e већ ограничено. Заменом координата тачке $P = (\frac{m}{e^2}, \frac{n}{e^3})$ у једначину $y^2 = x^3+ax+b$ елиптичке криве $E/\mathbb{Q}$, добијамо

$$\left(\frac{n}{e^3}\right)^2 = \left(\frac{m}{e^2}\right)^3 + a\frac{m}{e^2} + b,$$

то јест

$$\frac{n^2}{e^6} = \frac{m^3}{e^6} + a\frac{m}{e^2} + b,$$

односно наком множења са e^6

$$n^2 = m^3 + ame^4 + be^6.$$

Сада је и

$$|n^2| \leq |m^3| + |a||m||e^4| + |b||e^6|,$$

односно, примењујући (8.10)

$$|n^2| \leq H(P)^3 + |a|H(P) \cdot H(P)^2 + |b|H(P)^3,$$

па је

$$|n^2| \leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3.$$

Дакле,

$$|n|^2 \leq H(P)^3(1 + |a| + |b|),$$

па смо тако ограничили n, то јест добили оцену за њега:

$$|n| \leq RH(P)^{\frac{3}{2}}, \quad R = \sqrt{1 + |a| + |b|}.$$

Нека је $P_0 = (x_0, y_0)$ фиксирана, а $P = (x, y)$ произвољна тачка из $E(\mathbb{Q})$. Нека је и $P + P_0 = (W, \Omega)$. Тада је, према формули (5.4)

$$W = \left(\frac{y_0 - y}{x_0 - x}\right)^2 - (x + x_0),$$

то јест

$$W = \frac{(y_0 - y)^2 - (x + x_0)(x_0 - x)^2}{(x_0 - x)^2}.$$

Када ово измножимо и заменимо $y^2 - x^3$ са $ax + b$[8)] добијамо

$$W = \frac{-2y_0y + x_0x^2 + (a + x_0^3)x + y_0 - x_0^3 + b}{x_0^2 - 2x_0x + x^2},$$

то јест

$$W = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}, \tag{8.11}$$

при чему су коефицијенти A, B, C, D, E, F и G цели бројеви, јер бројилац и именилац последњег израза можемо множити све док они то не постану. Након замене $x = \frac{m}{e^2}$ и $y = \frac{n}{e^3}$ у (8.11), добијамо

$$W = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

Сада је и

$$H(W) = H(P + P_0) \leq \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\},$$

[8)] јер је $y^2 = x^3 + ax + b$

па ако на то применимо већ добијене оцене

$$e \leq H(P)^{\frac{1}{2}}, \quad n \leq RH(P)^{\frac{3}{2}} \quad \text{и} \quad m \leq H(P)$$

биће

$$\begin{aligned} |Ane + Bm^2 + Cme^2 + De^4| &\leq |Ane| + |Bm^2| + |Cme^2| + |De^4| \\ &\leq (|AR| + |B| + |C| + |D|)H(P)^2, \end{aligned}$$

односно

$$\begin{aligned} |Em^2 + Fme^2 + Ge^4| &\leq |Em^2| + |Fme^2| + |Ge^4| \\ &\leq (|E| + |F| + |G|)H(P)^2. \end{aligned}$$

Дакле,

$$H(P + P_0) \leq \max\{|AR| + |B| + |C| + |D|, |E| + |F| + |G|\}H(P)^2. \tag{8.12}$$

Након логаритмовања (8.12) видимо да заиста постоји константа k_0 за коју важи

$$h(P + P_0) \leq 2h(p) + k_0. \qquad \square$$

• Доказ треће леме

Нека је $P = (x, y)$ произвољна тачка из $E(\mathbb{Q})$. Нека је и $2P = (U, V)$. Тада је према формули (5.6)

$$U = \frac{(3x^2 + a)^2}{4(x^3 + ax + b)} - 2x,$$

то јест

$$U = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}. \tag{8.13}$$

Ако у (8.13) заменимо $x = \frac{u}{v}$, уз претпоставку да је разломак $\frac{u}{v}$ «максимално» скраћен, добијамо

$$U = \frac{u^4 - 2au^2v^2 - 8buv^3 + a^2v^4}{4u^3v + 4auv^3 + 4bv^4}.$$

Означимо $u^4 - 2au^2v^2 - 8buv^3 + a^2v^4$ са $\Phi(u, v)$, а $4u^3v + 4auv^3 + 4bv^4$ са $\Psi(u, v)$. Тада је

$$U = \frac{\Phi(u, v)}{\Psi(u, v)}.$$

За разлику од доказа друге леме, где смо тражили горњу границу, сада тражимо доње ограничење за $H(U) = H(2P)$, па нам је важно да ли $\Phi(u, v)$ и $\Psi(u, v)$ имају заједничке чиниоце. За наставак доказа, биће нам потребна следећа помоћна лема, [48, страна 222]:

Лема 8.4. Нека је $D = 4A^3 + 27B^2$, и дефинишемо полиноме

$$\begin{aligned}
F(X,Y) &= X^4 - 2AX^2Y^2 - 8BXY^3 + A^2Y^4,\\
G(X,Y) &= 4X^3Y + 4AXY^3 + 4BY^4,\\
f_1(X,Y) &= 12X^2Y + 16AY^3,\\
g_1(X,Y) &= 3X^3 - 5AXY^2 - 27BY^3,\\
f_2(X,Y) &= 4(4A^3 + 27B^2)X^3 - 4A^2BX^2Y\\
&\quad + 4A(3A^3 + 22B^2)XY^2 + 12B(A^3 + 8B^2)Y^3,\\
g_2(X,Y) &= A^2BX^2 + A(5A^3 + 32B^2)X^2Y\\
&\quad + 2B(13A^3 + 96B^2)XY^2 - 3A^2(A^3 + 8B^2)Y^3.
\end{aligned}$$

Тада у $\mathbb{Z}[A,B,X,Y]$ важи

$$\begin{aligned}
f_1(X,Y)F(X,Y) - g_1(X,Y)G(X,Y) &= 4DY^7,\\
f_2(X,Y)F(X,Y) - g_2(X,Y)G(X,Y) &= 4DX^7.
\end{aligned}$$ □

Нека је $\delta = [\Phi(u,v), \Psi(u,v)]$. Тада је, на основу помоћне леме

$$\begin{aligned}
f_1(u,v)\Phi(u,v) - g_1(u,v)\Psi(u,v) &= 4Dv^7,\\
f_2(u,v)\Phi(u,v) - g_2(u,v)\Psi(u,v) &= 4Du^7,
\end{aligned}$$

па можемо закључити да $\delta \mid 4D$, то јест да важи

$$|\delta| \leq |4D|,$$

па је зато и

$$H(U) = H(2P) \geq \frac{\max\{|\Phi(u,v)|, |\Psi(u,v)|\}}{|4D|}.$$

С друге стране, на основу помоћне леме имамо и следеће процене

$$|4Dv^7| \leq 2\max\{|f_1(u,v)|, |g_1(u,v)|\}\max\{|\Phi(u,v)|, |\Psi(u,v)|\}, \tag{8.14}$$
$$|4Du^7| \leq 2\max\{|f_2(u,v)|, |g_2(u,v)|\}\max\{|\Phi(u,v)|, |\Psi(u,v)|\}. \tag{8.15}$$

Посматрајући f_1,f_2, g_1 и g_2 можемо закључити да је

$$\max\{|f_1(u,v)|, |g_1(u,v)|, |f_2(u,v)|, |g_2(u,v)|\} \leq C\max\{|u|^3, |v|^3\}, \tag{8.16}$$

при чему је C нека константа која зависи само од u и v. Комбиновањем неједнакости (8.14), (8.15) и (8.16), добијамо

$$\max\{|4Du^7|, |4Dv^7|\} \leq 2C\max\{|u|^3, |v|^3\}\max\{|\Phi(u,v)|, |\Psi(u,v)|\}. \tag{8.17}$$

Након скраћивања обе стране неједнакости (8.17) са $\max\{|u|^3, |v|^3\}$ биће

$$\frac{\max\{|\Phi(u,v)|, |\Psi(u,v)|\}}{|4D|} \geq \frac{1}{2C}\max\{|u|^4, |v|^4\}.$$

Користећи чињеницу да је $\max\{|u|,|v|\} = H(P)$ добијамо

$$H(2P) \geq \frac{1}{2C} H(P)^4. \tag{8.18}$$

Након логаритмовања(8.18) видимо да заиста постоји константа k за коју важи

$$h(2P) \geq 4h(P) - k. \qquad \square$$

8.4 Теорема о спусту

• **Формулација**

Према [48, страна 218], важи

Теорема 8.2. Нека је Γ Абелова група таква да је група $\Gamma/2\Gamma$ коначна и нека је $h : \Gamma \to [0, +\infty)$ функција висине која задовољава следећа својства:

1° за сваки реалан број K, скуп $\{P \in \Gamma \mid h(P) \leq K\}$ је коначан,

2° постоји константа k_0 таква да за сваку тачку P из Γ важи

$$h(P + P_0) \leq 2h(P) + k_0,$$

3° постоји константа k таква да за сваку тачку P из Γ важи

$$h(2P) \geq 4h(P) - k.$$

Тада је Абелова група Γ коначно генерисана. $\square$

• **Доказ**

Како је $\Gamma/2\Gamma$ коначна група, тада је и скуп

$$A = \{Q_1, \ldots, Q_n\}$$

представника из групе Γ с обзиром на њену подгрупу 2Γ коначан. То значи да је

$$(Q_1 + 2\Gamma) \cup \cdots \cup (Q_n + 2\Gamma) = \Gamma. \tag{8.19}$$

Нека су k_i, за $i = 1, \ldots, n$ константе које постоје према својству 2°, стављајући $-Q_i$ уместо P_0, и нека је k' највећа од њих. Дефинишимо скуп

$$B = \{R \in \Gamma \mid h(R) \leq k + k'\}.$$

Он је према својству 1° коначан.

Покажимо да скуп $A \cup B$ генерише групу Γ, посебно да је Γ коначно генерисана.

Нека је P произвољан елемент групе Г. Тада према (8.19) постоји елемент Q_{i1} из скупа A такав да је $P - Q_{i1}$ из 2Г, што можемо записати као

$$P - Q_{i1} = 2P_1 \tag{8.20}$$

за неки елемент P_1 из Г. Исто важи и за елемент P_1, па је

$$P_1 - Q_{i2} = 2P_2 \tag{8.21}$$

за неки елемент P_2 из Г. Ако наставимо поступак, добијамо низ једнакости

$$P_2 - Q_{i3} = 2P_3, \tag{8.22}$$
$$P_3 - Q_{i4} = 2P_4, \tag{8.23}$$
$$\vdots$$
$$P_{m-1} - Q_{im} = 2P_m, \tag{8.24}$$

које важе за неке елементе $P_3, \ldots, P_m$ из Г. Ако једнакост (8.21) помножимо са 2, једнакост (8.22) са 4, једнакост (8.23) са 8, и тако даље, па све тако добијене једнакости саберемо, добићемо

$$P = Q_{i1} + 2Q_{i2} + 4Q_{i3} + \cdots + 2^{m-1}Q_{im} + 2^m P_m. \tag{8.25}$$

Покажимо да је, без обзира на избор елемента P, за довољно велико m, елемент P_m из скупа B, то јест да је $h(P_m) \leq k + k'$ за довољно велико m.

Нека је P_j произвољан елемент из Г. Тада, на основу својстава 2° и 3° и уведених константи k_i и k' важи

$$\begin{aligned} 4h(P_j) &\leq h(2P_j) + k = h(P_{j-1} - Q_{ij}) + k \\ &\leq 2h(P_{j-1}) + k' + k, \end{aligned}$$

па је

$$h(P_j) \leq \frac{2}{4}h(P_{j-1}) + \frac{1}{4}(k' + k).$$

Сада је и

$$h(P_j) \leq \frac{2}{4}h(P_{j-1}) + \frac{1}{4}h(P_{j-1}) - \frac{1}{4}h(P_{j-1}) + \frac{1}{4}(k' + k),$$

то јест

$$h(P_j) \leq \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (k' + k)). \tag{8.26}$$

На основу (8.26) можемо закључити да у низу елемената $P_1, P_2, P_3, \ldots, P_i, \ldots$, докле год је $h(P_i) - (k' + k) \geq 0$, то јест $h(P_i) \geq k' + k$, следећи елемент P_{i+1} има висину $h(P_{i+1})$ бар 75% мању од висине $h(P_i)$, па једном, то јест за неко m висина $h(P_m)$ мора пасти испод $k' + k$. Дакле, важи $h(P_m) \leq k + k'$, па је P_m из скупа B.

Сада, на основу једнакости (8.25) и произвољности елемента P из групе Γ, можемо закључити да је група Γ генерисана са

$$A \cup B = \{Q_1, \ldots, Q_n\} \cup \{R \in \Gamma \mid h(R) \leq k + k'\}$$

што је коначно као унија два коначна скупа.

Дакле, Абелова група Γ је коначно генерисана, то јесте Γ је коначно генерисана Абелова група. □

На основу слабе Морделове теореме, својстава висине h које су дате у три леме, и теореме о спусту можемо тврдити да је скуп $E(\mathbb{Q})$ свих рационалних тачака елиптичке криве $E/\mathbb{Q}$, то јест структура $(E(\mathbb{Q}), +)$ коначно генерисана Абелова група, што је први доказао Мордел 1922. године. □

9

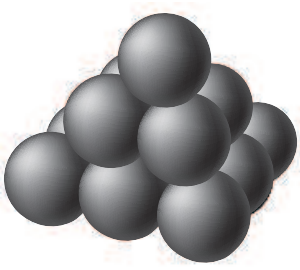
Неке примене елиптичких кривих

Елиптичке криве – као један од најзначајнијих и најизучаванијих објеката, како у теорији бројева, тако и у модерној математици уопште – имају и велику примену. У овом поглављу, приказаћемо само неке од њих, са посебним освртом на једну од њених најважнијих примена – доказ последње Фермаове теореме. Опширније, о неким деловима овог поглавља, потражити у [59], [13], [15], [34] и [55].

9.1 Пирамида топовских кугли

• Поставка проблема

Нека је скуп топовских кугли сложен у облику правилне четворостране пирамиде тако да је једна кугла на врху – кажемо и у првом реду, четири у другом, девет кугли у трећем реду и тако даље.



Ако се тако сложена гомила топовских кугли уруши, да ли их можемо поново пресложити тако да од њих добијемо квадрат?

Ако пирамида има три реда – кажемо да је висине 3 – онда није могуће кугле од којих је она састављена пресложити тако да добијемо квадрат с обзиром да је $1 + 4 + 9 = 14$, а 14 није потпун квадрат неког природног броја. Ако посматрамо само једну куглу, тада је она и пирамида висине 1, али и јединични квадрат. У случају да немамо кугле, помињање пирамиде и квадрата нема смисла.

Поред ова два последња, кажемо и тривијална, случаја, користећи методу

која потиче још од Диофанта, пронаћи ћемо и још неке случајеве.

• Формирање елиптичке криве

Нека је x висина пирамиде. Тада у пирамиди имамо укупно

$$1^2 + 2^2 + \cdots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

кугли. С обзиром да желимо да овај број кугли буде потпун квадрат неког природног броја, на пример y, тражимо решење једначине

$$y^2 = \frac{x(x+1)(2x+1)}{6} \tag{9.1}$$

у скупу природних бројева, то јест позитивних целих бројева. Њеним упрошћавањем добијамо једначину

$$y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x. \tag{9.2}$$

Погодним трансформацијама једначину (9.2) можемо свести на облик

$$y^2 = x^3 + ax + b,$$

а као што знамо оваквим једначинама су описане елиптичке криве.

• Диофантова метода

Да бисмо пронашли још неке случајеве, тражимо решења једначине (9.1) у скупу позитивних целих бројева, то јест тражимо тачке (x, y) чије су обе координате позитивни цели бројеви, а које припадају елиптичкој кривој чија је једначина (9.1).

Диофантова метода проналажења нових тачака полази од чињенице да одредимо тачке (x, y) за које знамо да сигурно припадају елиптичкој кривој. У нашем случају, лако уочавамо да су то тачке $(0, 0)$ и $(1, 1)$. Права која пролази кроз ове две тачке има једначину

$$y = x$$

и њеним пресеком са елиптичком кривом добијамо једначину

$$x^2 = \frac{x(x+1)(2x+1)}{6} = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x. \tag{9.3}$$

Сређивањем једначине (9.3) добијамо

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0.$$

Знамо да су решења ове једначине $x = 0$ и $x = 1$. Да бисмо пронашли и треће њено решење, можемо факторисати полином

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x.$$

Међутим, постоји бољи начин да дођемо до трећег решења. Наиме, знамо да за било које a, b и c важи

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+ac+bc)x^2 - abc. \tag{9.4}$$

Како је коефицијент уз x^3 једнак 1, негативна вредност коефицијента уз x^2 је збир решења једначине. У нашем случају то значи да је

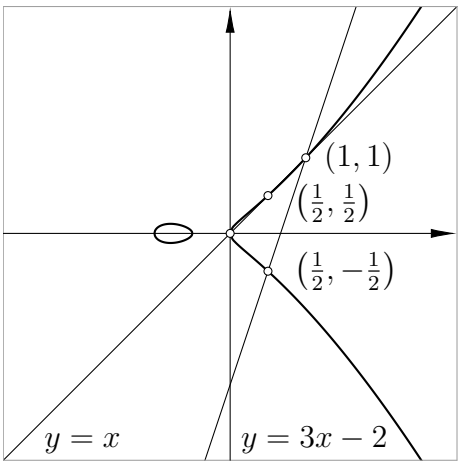
$$0 + 1 + x = \frac{3}{2},$$

одакле рачунањем добијамо да је $x = \frac{1}{2}$. Како тачка $(\frac{1}{2}, y)$ припада и правој $y = x$, лако добијамо да је и $y = \frac{1}{2}$. У смислу топовских кугли ово не сматрамо решењем, али смо бар пронашли још једну нетривијалну и рационалну тачку на елиптичкој кривој. Због симетричности елиптичке криве у односу на x-осу, одмах добијамо да и тачка $(\frac{1}{2}, -\frac{1}{2})$ припада елиптичкој кривој. С обзиром да тражимо тачку која припада првом квадранту, можемо поновити претходно описану процедуру, али полазећи од тачака $(1, 1)$ и $(\frac{1}{2}, -\frac{1}{2})$. Права која пролази кроз ове две тачке има једначину

$$y = 3x - 2$$

и њеним пресеком са елиптичком кривом добијамо једначину

$$(3x-2)^2 = \frac{x(x+1)(2x+1)}{6} = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x. \tag{9.5}$$



Сређивањем једначине (9.5) добијамо

$$2x^3 - 51x^2 + 73x - 24 = 0,$$

па на основу (9.4) важи

$$1 + \frac{1}{2} + x = \frac{51}{2},$$

јер знамо да су решења једначине $x = 1$ и $x = \frac{1}{2}$. Рачунањем добијамо да је $x = 24$, а како тачка $(24, y)$ припада и правој $y = 3x - 2$ лако добијамо да је и $y = 70$. То значи да је

$$1^2 + 2^2 + \cdots + 24^2 = 70^2.$$

Дакле, $70^2 = 4900$ топовских кугли можемо расподелити у пирамиду висине 24 или у квадрат чија једна страница садржи 70 топовских кугли.

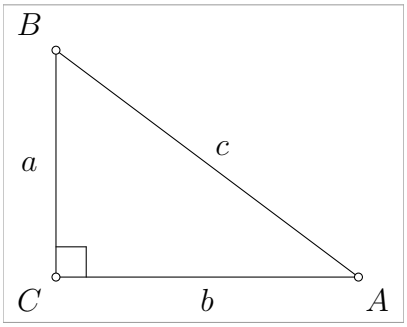
Ако наставимо са горе наведеним поступком, користећи, на пример, управо добијене тачке, добићемо бесконачно много рационалних решења једначине (9.1).

9.2 Правоугли троугао

• Поставка проблема

Већ је Ферма знао да не постоји правоугли троугао са целобројним дужинама страница чија је површина квадрат неког целог броја. Другим речима, не постоји правоугли троугао чије су дужине страница рационални бројеви, а површина једнака 1. С друге стране, јасно је да постоји такав троугао с површином једнаком 6. То је троугао чије су дужине страница $a = 3$, $b = 4$ и $c = 5$.

Нека је ABC правоугли троугао са правим углом код темена C, чије су дужине катета a и b и хипотенузе c рационални бројеви.



Одредимо дужине тих страница ако је површина тог троугла 5.

• Формирање елиптичке криве

Како је површина правоуглог троугла

$$P = \frac{ab}{2} = 5,$$

тражимо рационалне бројеве a, b и c за које важи

$$a^2 + b^2 = c^2 \quad \text{и} \quad ab = 10. \tag{9.6}$$

Ако пођемо од $(\frac{a+b}{2})^2$ и $(\frac{a-b}{2})^2$ добијамо да је

$$\left(\frac{a+b}{2}\right)^2 = \frac{a^2+2ab+b^2}{4} = \frac{a^2+b^2+2ab}{4} = \frac{c^2+20}{4} = \frac{c^2}{4}+5 = \left(\frac{c}{2}\right)^2+5,$$

и

$$\left(\frac{a-b}{2}\right)^2 = \frac{a^2-2ab+b^2}{4} = \frac{a^2+b^2-2ab}{4} = \frac{c^2-20}{4} = \frac{c^2}{4}-5 = \left(\frac{c}{2}\right)^2-5.$$

Сменом $x = \left(\frac{c}{2}\right)^2$ претходне две једнакости постају

$$\left(\frac{a+b}{2}\right)^2 = x+5, \quad \left(\frac{a-b}{2}\right)^2 = x-5,$$

па се проблем одређивања рационалних бројева a, b и c за које важи (9.6) своди на одређивање рационалног броја x таквог да су бројеви x, $x+5$ и $x-5$ истовремено квадрати рационалних бројева. Ако такав рационалан број x постоји, тада мора и производ

$$(x-5)x(x+5) = x^3-25x$$

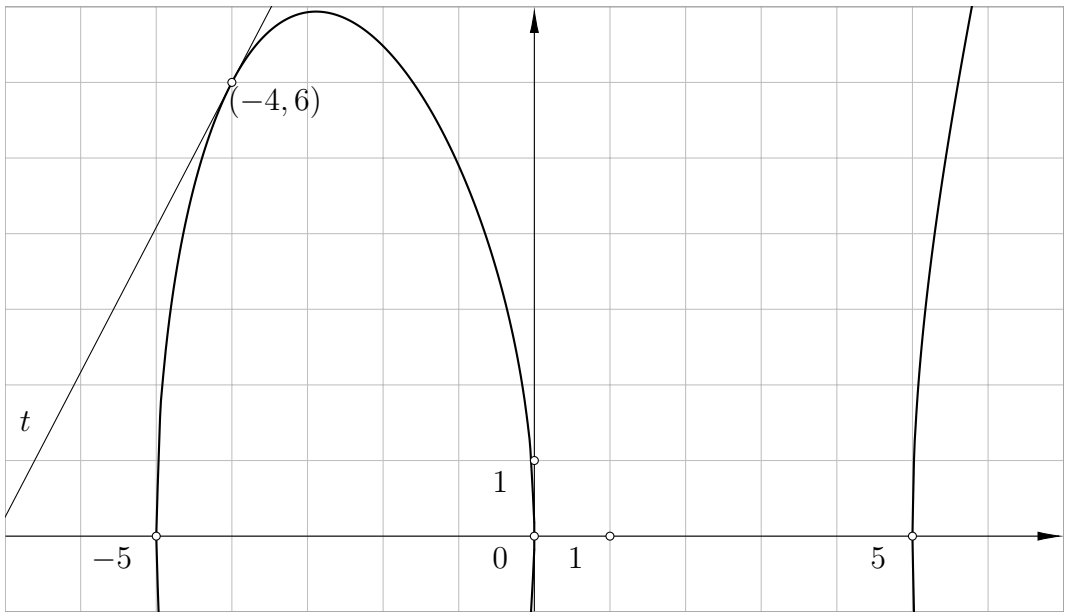
бити квадрат рационалног броја, на пример y, па тражимо рационално решење једначине

$$y^2 = x^3-25x. \tag{9.7}$$

Као што знамо, оваквим једначинама су описане елиптичке криве.

• Диофантова метода

Очигледно је да тачке $(-5,0)$, $(0,0)$ и $(5,0)$ припадају елиптичкој кривој. Међутим, све три тачке су и колинеарне, то јест не граде троугао, па нам та чињеница не може помоћи.



Посматрањем графика елиптичке криве уочавамо, а затим и заменом њених координата у њену једначину, проверавамо, да тачка $(-4, 6)$ припада елиптичкој кривој. Диференцирањем имплицитно задате функције

$$x^3 - 25x - y^2 = 0$$

коју добијамо из (9.7) можемо одредити једначину тангенте t на елиптичкој кривој $y^2 = x^3 - 25x$ која садржи тачку $(-4, 6)$. Наиме, из

$$3x^2 - 25 - 2yy' = 0$$

закључујемо да је

$$y' = \frac{3x^2 - 25}{2y}, \tag{9.8}$$

па увршћавањем $x = -4$ и $y = 6$ у (9.8) лако одређујемо једначину тангенте

$$t : y = \frac{23}{12}x + \frac{41}{3}.$$

Одређивањем пресека елиптичке криве $y^2 = x^3 - 25x$ и тангенте t добијамо једначину $\left(\frac{23}{12}x + \frac{41}{3}\right)^2 = x^3 - 25x$, то јест

$$144x^3 - 529x^2 - 11144x - 26896 = 0$$

Како је права тангента на елиптичкој кривој $y^2 = x^3 - 25x$ у тачки $(-4, 6)$, $x = -4$ је двоструко решење, па на основу (9.4) је $-4 - 4 + x = \left(\frac{23}{12}\right)^2$, одакле закључујемо да је

$$x = \frac{1681}{144} = \left(\frac{41}{12}\right)^2. \tag{9.9}$$

Како тачка $\left(\left(\frac{41}{12}\right)^2, y\right)$ припада и тангенти t, одмах израчунавамо да је и

$$y = \frac{62279}{1728}.$$

Враћањем смене $x = \left(\frac{c}{2}\right)^2$ у (9.9) добијамо да је

$$c = \frac{41}{6}.$$

Како је $y^2 = x^3 - 25x$, то је

$$\begin{aligned} y =& \sqrt{x^3 - 25x} = \sqrt{(x-5)x(x+5)} = \sqrt{\left(\frac{a-b}{2}\right)^2 \left(\frac{c}{2}\right)^2 \left(\frac{a+b}{2}\right)^2} \\ =& \frac{(a-b)c(a+b)}{2 \cdot 2 \cdot 2} = \frac{(a^2 - b^2)c}{8}, \end{aligned}$$

па је

$$\frac{62279}{1728} = \frac{(a^2 - b^2)c}{8} = \frac{41(a^2 - b^2)}{48},$$

то јест

$$a^2 - b^2 = \frac{1519}{36}. \tag{9.10}$$

С обзиром да је троугао ABC правоугли, важи и $a^2 + b^2 = c^2$, па је

$$a^2 + b^2 = \left(\frac{41}{6}\right)^2. \tag{9.11}$$

Решавањем система једначина (9.10) и (9.11) добијамо да је

$$a^2 = \frac{400}{9} \quad \text{и} \quad b^2 = \frac{9}{4}.$$

Узимајући само позитивне вредности за a и b, јер су то катете правоуглог троугла, решење постављеног проблема је

$$a = \frac{20}{3}, b = \frac{3}{2}, \text{ и } c = \frac{41}{6},$$

то јест то су дужине страница правоуглог троугла ABC чија је површина једнака 5. Како је $\frac{20}{3} = \frac{40}{6}$ и $\frac{3}{2} = \frac{9}{6}$ лако уочавамо да странице a, b и c чине Питагорину тројку

$$(40, 9, 41)$$

умањену шест пута.

Ако наставимо са горе наведеним поступком, користећи, на пример, управо добијене тачке, добићемо бесконачно много рационалних решења једначине (9.7).

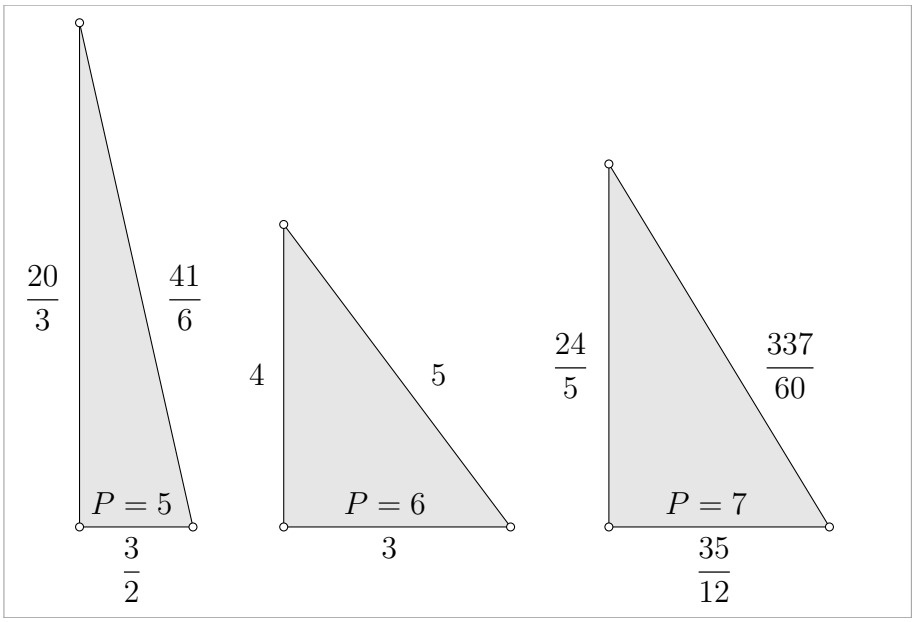
9.3 Конгруентни бројеви

• Дефиниција конгруентног броја

На основу [15, страна 539], имамо

Дефиниција 9.1. За природан број n кажемо да је *конгруентан* ако је он једнак површини неког правоуглог троугла чије су дужине страница рационални бројеви.

Из претходне секције видимо да је број 5 конгруентан, јер је једнак површини троугла са страницама $(a, b, c) = (\frac{20}{3}, \frac{3}{2}, \frac{41}{6})$. Лако уочавамо да је и број 6 конгруентан, јер је он једнак површини троугла са страницама $(a, b, c) = (3, 4, 5)$. Број 7 је, такође, конгруентан, јер је он једнак површини троугла са страницама $(a, b, c) = (\frac{24}{5}, \frac{35}{12}, \frac{337}{60})$.



С друге стране, познато је да бројеви 1, 2, 3, 4, 8, 9 и 10 нису конгруентни.

• Конгруентни бројеви и елиптичке криве

Одређивање да ли је неки број конгруентан, повезано је са елиптичким кривама, [15, страна 539].

Став 9.1. Природан број n је конгруентан ако и само ако постоји рационалан број x са својством да су x, $x-n$ и $x+n$ квадрати рационалних бројева.

Доказ. Нека је n конгруентан број. Тада, према дефиницији (9.1), постоје рационални бројеви a, b и c који су дужине катета и хипотенузе правоуглог троугла чија је површина $\frac{ab}{2} = n$. Ставимо да је $x = \frac{c^2}{4} = \left(\frac{c}{2}\right)^2$. Тада је

$$x - n = \frac{c^2}{4} - \frac{ab}{2} = \frac{c^2 - 2ab}{4} = \frac{a^2 + b^2 - 2ab}{4} = \frac{(a-b)^2}{4} = \left(\frac{a-b}{2}\right)^2,$$
$$x + n = \frac{c^2}{4} + \frac{ab}{2} = \frac{c^2 + 2ab}{4} = \frac{a^2 + b^2 + 2ab}{4} = \frac{(a+b)^2}{4} = \left(\frac{a+b}{2}\right)^2,$$

па су x, $x-n$ и $x+n$ квадрати рационалних бројева.

Обратно, нека су x, $x-n$ и $x+n$ квадрати рационалних бројева. Тада постоје рационални бројеви, на пример, u, v и w, такви да је $x = u^2$, $x - n = v^2$ и $x + n = w^2$. Ако ставимо да је

$$a = w + v = \sqrt{x+n} + \sqrt{x-n},$$
$$b = w - v = \sqrt{x+n} - \sqrt{x-n},$$
$$c = 2u = 2\sqrt{x}$$

добијамо да је

$$\begin{aligned} a^2+b^2 &= (w+v)^2+(w-v)^2 = (\sqrt{x+n}+\sqrt{x-n})^2+(\sqrt{x+n}-\sqrt{x-n})^2 \\ &= x+n+2\sqrt{(x+n)(x-n)}+x-n+x+n-2\sqrt{(x+n)(x-n)}+x-n \\ &= 4x = (2\sqrt{x})^2 = (2u)^2 \\ &= c^2, \end{aligned}$$

па је троугао са страницама (a,b,c) правоугли и његова површина је

$$\frac{ab}{2} = \frac{(\sqrt{x+n}+\sqrt{x-n})(\sqrt{x+n}-\sqrt{x-n})}{2} = \frac{x+n-x+n}{2} = \frac{2n}{2} = n$$

Дакле, n је конгруентан број. □

Ако су бројеви x, $x-n$ и $x+n$ квадрати рационалних бројева, онда је и њихов производ

$$x(x-n)(x+n) = x(x^2-n^2) = x^3-n^2x$$

квадрат неког рационалног броја. То значи да ако је n конгруентан број, онда на придруженој елиптичкој кривој

$$E_n : y^2 = x^3-n^2x \tag{9.12}$$

осим 2-торзионих тачака $(0,0)$, $(n,0)$ и $(-n,0)$ постоји бар још једна рационална тачка. Отуда и следећа теорема, [15, страна 540].

Теорема 9.1. Природан број n је конгруентан ако и само ако елиптичка крива $E_n : y^2 = x^3-n^2x$ садржи бар једну рационалну тачку (x,y) за коју је $y \neq 0$.

Доказ. Ако је n конгруентан број, видели смо да елиптичка крива $E_n : y^2 = x^3-n^2x$ садржи бар још једну рационалну тачку. Зато докажимо да важи и обратно.

Нека је $P(x,y), y \neq 0$ нека рационална тачка на елиптичкој кривој E. Тада знамо да је производ бројева x, $x-n$ и $x+n$ квадрат рационалног броја, али то не значи да је и сваки од тих бројева такође квадрат рационалног броја. Показаћемо међутим да је овај јачи захтев испуњен за тачке облика $2P$. Заиста, стављајући у једнакост (5.6) да је $a=-n^2$ и $b=0$, након упрошћавања добијамо

$$x(2P) = \left(\frac{x^2+n^2}{2y}\right)^2, \quad x(2P)+n = \left(\frac{x^2+2xn-n^2}{2y}\right)^2,$$
$$x(2P)-n = \left(\frac{x^2-2xn-n^2}{2y}\right)^2.$$ □

Можемо показати да елиптичка крива (9.12), осим 2-торзионих тачака, нема других тачака коначног реда. Отуда и, [15, страна 540]

Теорема 9.2. Природан број n је конгруентан ако и само ако елиптичка крива $E_n : y^2 = x^3 - n^2x$ садржи бесконачно много рационалних тачака, то јест ако је њен ранг позитиван. □

• Квадратно слободни бројеви. Танелова теорема

Резултат који је најближи одговору на питање како за дати природан број n утврдити да ли је конгруентан, дат је Танеловом[1)] теоремом.

Пре тога, подсетимо се када је природан број квадратно слободан, [15, страна 32].

Дефиниција 9.2. За природан број n кажемо да је *квадратно слободан* ако је 1 највећи потпун квадрат који га дели, то јест ако важи

$$(\forall m \in \mathbb{N})(m^2 \mid n \Rightarrow m = 1).$$

Пример 9.1. Бројеви 6 и 15 су квадратно слободни, а бројеви 12 и 100 нису, јер $4 = 2^2 \mid 12$, односно $4 = 2^2 \mid 100$ и $25 = 5^2 \mid 100$. Такође, сваки прост број је квадратно слободан. △

На основу [15, страна 540] важи

Теорема 9.3. [**Танел**] Нека је природан број n квадратно слободан, и нека је $d = 1$ ако је n непаран, а $d = 2$ ако је n паран број. Ако је n конгруентан, онда једначина

$$x^2 + 2dy^2 + 8z^2 = \frac{n}{d}$$

има тачно два пута више целобројних решења (x, y, z) од једначине

$$x^2 + 2dy^2 + 32z^2 = \frac{n}{d}.$$ □

Уз претпоставку да важи Бирч и Свинертон-Дајерова хипотеза, важи и обрат Танелове теореме.

Пример 9.2. Нека је $n = 3$, па самим тим и $d = 1$. Свака од једначина $x^2 + 2y^2 + 8z^2 = 3$ и $x^2 + 2y^2 + 32z^2 = 3$ има по 4 решења: $(1, 1, 0)$, $(1, 1, 0)$, $(1, 1, 0)$ и $(1, 1, 0)$, па на основу обрата Танелове теореме закључујемо да број 3 није конгруентан. △

Пример 9.3. Нека је $n = 34$, па самим тим и $d = 2$. Једначина $x^2 + 4y^2 + 8z^2 = 17$ има 8 решења $(1, 2, 0)$, $(1, 2, 0)$, $(1, 2, 0)$, $(1, 2, 0)$, $(3, 0, 1)$, $(3, 0, 1)$, $(3, 0, 1)$, $(3, 0, 1)$, док једначинаа $x^2 + 4y^2 + 32z^2 = 17$ има 4 решења $(1, 2, 0)$,

[1)] Џеролд Беитс Танел (Jerrold Bates Tunnell, 1950), амерички математичар

$(1,2,0)$, $(1,2,0)$, $(1,2,0)$. Према томе, на основу обрата Танелове теореме, закључујемо да је број 34 конгруентан. Уверимо се у то тако што ћемо пронаћи правоугли троугао са рационалним дужинама страницама чија је површина једнака 34. Пођимо од елиптичке криве $y^2 = x^3 - 34^2 x$. На њој се налази рационална тачка $P = (-2, 48)$. Тада је

$$x(2P) = \left(\frac{(-2)^2 + 34^2}{2 \cdot 48}\right)^2 = \left(\frac{1160}{96}\right)^2 = \left(\frac{145}{12}\right)^2,$$

$$x(2P) + n = \left(\frac{(-2)^2 + 2 \cdot (-2) \cdot 34 - 34^2}{2 \cdot 48}\right)^2 = \left(\frac{-1288}{96}\right)^2 = \left(-\frac{161}{12}\right)^2,$$

$$x(2P) - n = \left(\frac{(-2)^2 - 2 \cdot (-2) \cdot 34 - 34^2}{2 \cdot 48}\right)^2 = \left(\frac{-1016}{96}\right)^2 = \left(-\frac{127}{12}\right)^2$$

па на основу доказа става (9.1), то јест релација

$$x(2P) = \left(\frac{c}{2}\right)^2, x(2P) - n = \left(\frac{a-b}{2}\right)^2 \text{ и } x(2P) + n = \left(\frac{a+b}{2}\right)^2$$

налазимо странице правоуглог троугла: $c = \frac{145}{6}$, $a = 24$ и $b = \frac{17}{6}$. △

9.4 Харди - Раманујанов проблем таксија

• Поставка проблема

Проблем таксија је добио име по једној анегдоти везаној за математичаре Хардија[2)] и Раманујана[3)].

Док је Раманујан био у болници у Лондону, у посету му је дошао Харди. Харди је споменуо да је стигао са таксијем број 1729, и додао да је тај број сасвим незанимљив. Међутим, Раманујан му је одмах одговорио да се са њим не слаже, јер је 1729 врло занимљив број. Као разлог је навео да је то најмањи природан број који се може приказати као збир кубова два природна броја на два различита начина. Заиста,

$$1729 = 9^3 + 10^3 = 1^3 + 12^3.$$

[2)] Годфри Харолд Харди (Godfrey Harold Hardy, 1877–1947), енглески математичар

[3)] Срениваса Ађангар Раманујан (Srinivasa Aiyangar Ramanujan, 1887–1920), индијски математичар

• Проблем таксија и елиптичке криве

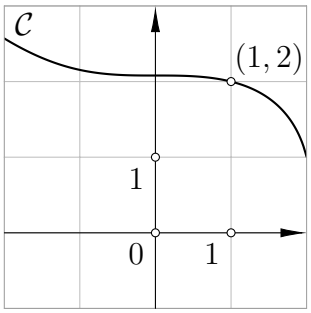
Сада се можемо питати да ли постоји природан број који се може приказати као збир кубова два природна броја на три различита начина, или уопштено на M различитих начина. Одговор на то питање је потврдан и дат је следећом теоремом, [13, Тема 2.2].

Теорема 9.4. За сваки природан број M постоји природан број m такав да једначина $x^3 + y^3 = m$ има бар M целобројних решења.

Доказ. На почетку, посматрајмо, криву

$$\mathcal{C} : x^3 + y^3 = 9.$$

Тврдимо да она има бесконачно много рационалних тачака. Једна очигледна рационална тачка је $(1, 2)$.



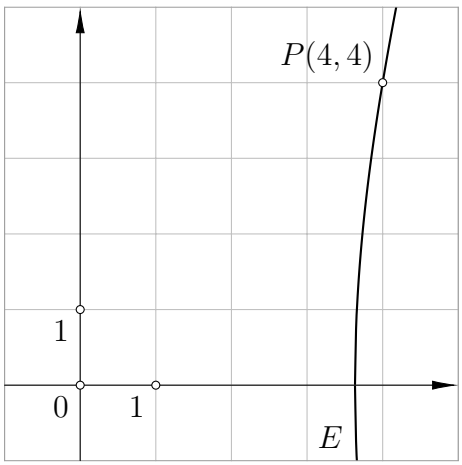
Помоћу бирационалне трансформације

$$s = \frac{12}{x+y} \quad t = \frac{12(x-y)}{(x+y)}$$

добијамо да је крива $\mathcal{C}$ бирационално еквивалентна елиптичкој кривој

$$E : t^2 = s^3 - 48.$$

Притом тачки $(1, 2)$ са $\mathcal{C}$ одговара тачка $P(4, 4)$ са E.



Поставља се питање да ли је тачка P бесконачног реда или је она торзиона. Рачунајмо nP за $n = 2, 3, \ldots$ Добијамо:

$$2P = (28, 148), \quad 3P = 2P + P = (\frac{73}{9}, \frac{595}{27}).$$

Ово је довољно да бисмо, према Луц – Нагеловој теореми (6.7), закључили да је тачка P бесконачног реда, јер да би нека тачка била торзиона, она мора имати целобројне координате. Одавде закључујемо да крива $\mathcal{C}$ и елиптичка крива E имају бар једну, а тиме и бесконачно много рационалних тачака.

Нека је сада M задати природни број. Према претходном, на кривој $\mathcal{C}$ можемо изабрати неких M рационалних тачака

$$Q_1, \ldots, Q_M.$$

Лако се види да прва и друга координата тих тачака имају једнаке имениоце, то јест тачке Q_i су облика

$$Q_i = (\frac{a_i}{d_i}, \frac{b_i}{d_i}).$$

Да бисмо из рационалних тачака на кривој $\mathcal{C}$ добили целобројна решења на некој кривој $x^3 + y^3 = m$, довољно је узети да је

$$m = 9(d_1 \cdots d_M)^3.$$

Сада, на кривој $x^3 + y^3 = m$ лежи M целобројних тачака чије се координате добијају множењем координата тачака Q_i, за $i = 1, \ldots, M$ са производом $d_1 \cdots d_M$. □

• Такси број

Од свих природних бројева који се могу приказати као збир кубова два природна броја на M различитих начина посебно издвајамо најмањи такав, [13, Тема 2.2].

Дефиниција 9.3. Најмањи природан број који се може приказати као збир кубова два природна броја на M различитих начина називамо *M-ти такси број* и означавамо га са $Ta(M)$.

Тривијално је

$$Ta(1) = 2 = 1^3 + 1^3.$$

Видели смо да је

$$Ta(2) = 1729 = 9^3 + 10^3 = 1^3 + 12^3.$$

Познато је још да важи

$$Ta(3) = 87539319 = 167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3.$$

9.5 Диофантове m-торке бројева

• Рационална Диофантова m-торка

На основу [13, Тема 2.3] имамо

Дефиниција 9.4. Скуп $\{a_1, \ldots, a_m\}$ од m природних бројева $a_1, \ldots, a_m$ називамо *Диофантова m-торка* ако је $a_i a_j + 1$ потпун квадрат за свако $1 \leq i < j \leq m$.

Другим речима, *Диофантова m-торка* је скуп од m природних бројева са својством да је производ свака два његова различита елемента увећан за 1 потпун квадрат.

Проблем конструкције Диофантових m-торки има корене у далекој прошлости. Сваким даном је познато све више нових резултата из овог подручија, али и даље постоје многи отворени проблеми и недоказане хипотезе.

Ако посматрамо m рационалних бројева различитих од нуле са истим својством, добијамо рационалну Диофантову m-торку. Прецизније, [13, Тема 2.3]

Дефиниција 9.5. Скуп $\{a_1, \ldots, a_m\}$ од m рационалних бројева $a_1, \ldots, a_m$ различитих од нуле називамо *рационална Диофантова m-торка* ако је $a_i a_j + 1$ потпун квадрат за свако $1 \leq i < j \leq m$.

Прву Диофантову четворку, то јест скуп

$$\{1, 3, 8, 120\}$$

пронашао је Ферма. Уверимо се да је овај скуп заиста Диофантова четворка:

$$\begin{aligned} 1 \cdot 3 + 1 &= 2^2, \quad 1 \cdot 120 + 1 = 11^2, \\ 1 \cdot 8 + 1 &= 3^2, \quad 3 \cdot 120 + 1 = 19^2, \\ 3 \cdot 8 + 1 &= 5^2, \quad 8 \cdot 120 + 1 = 31^2. \end{aligned}$$

Прву рационалну Диофантову четворку пронашао је Диофант, по коме су овакви скупови и добили име. То је четворка

$$\left\{ \frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16} \right\}.$$

• Допуна Диофантове m-торке

Познато је да се свака Диофантова тројка може допунити до Диофантове четворке, као и да се свака Диофантова четворка може допунити до рационалне Диофантове петорке. Ојлер је успео допунити Фермаов скуп са петим рационалним бројем $\frac{777480}{8288641}$. Прва рационална Диофантова шесторка пронађена је тек 1999. године. То је скуп

$$\left\{ \frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16} \right\},$$

који је пронашао Гибс[4)]. Он је пронашао 45 примера рационалних Диофантових шесторки, а још неколико их је 2009. године пронашао Дујела[5)]. Користећи се *теоријом Диофантових апроксимација*[6)], Дујела је доказао следеће две теореме, [13, Тема 2.3].

Теорема 9.5. Не постоји Диофантова шесторка. □

Теорема 9.6. Постоји само коначно много Диофантових петорки. □

Уопште, није познато да ли постоји горње ограничење за величину рационалних Диофантових m-торки.

• Диофантове m-торке и елиптичке криве

Нека је $\{a, b, c\}$ Диофантова тројка или рационална Диофантова тројка, свеједно. Претпоставимо да ту тројку треба допунити до Диофантове четворке. То значи да треба наћи број d такав да су бројеви

$$ad + 1,\ bd + 1 \text{ и } cd + 1$$

потпуни квадрати. Овом проблему на природан начин можемо придружити елиптичку криву

$$E : y^2 = (x + ab)(x + ac)(x + bc).$$

Наиме, ако је d решење нашег проблема, онда је тачка са првом координатом $x = abcd$ рационална тачка на елиптичкој кривој E. Крива E има три рационалне тачке реда 2:

$$(ab, 0),\ (ac, 0),\ (bc, 0),$$

а такође и тривијалну рационалну тачку $P(0, abc)$ за коју није тешко показати да је бесконачног реда. Дакле, на елиптичкој кривој E постоји бар једна, а тиме и бесконачно много рационалних тачака (x, y). Поставља се питање за које ће од тих тачака број $d = \frac{x}{abc}$ представљати решење полазног проблема, то јест имати својство да је $\{a, b, c, d\}$ рационална Диофантова четворка. Одговор је да су то све тачке облика $P + 2U$, при чему је U произвољна рационална тачка на E. На елиптичкој кривој E се налази још једна занимљива рационална тачка. То је тачка са првом координатом једнаком 1. Прецизније, ако је

$$ab + 1 = r^2,\ ac + 1 = s^2,\ bc + 1 = t^2,$$

[4)] Филип Едвард Гибс (Philip Edward Gibbs, 1960), британски математичар и физичар

[5)] Андреј Дујела (Andrej Dujella, 1966), хрватски математичар

[6)] *Теорија Диофантових апроксимација* је грана теорије бројева у којој се проучавају апроксимације реалних бројева рационалним. Као што је познато, сваки реалан број се може произвољно добро апроксимирати рационалним; међутим, ако се при том за бројеве којима се врши апроксимација захтевају неки додатни услови, на пример, ограничава им се на одређени начин именилац, тада се захтевана тачност не може увек постићи.

онда тачка $S(1, rst)$ припада елиптичкој кривој E. Штавише, важи да је $S = 2R$, где је

$$R = ((rs + rt + st + 1), (r + s)(r + t)(s + t)).$$

Директан рачун показује да су прве координате тачака $P - S$ и $P + S$ једнаке

$$a + b + c \pm 2abc + 2rst,$$

што представља доказ чињенице да се свака Диофантова тројка може допунити до Диофантове четворке. Ако применимо ову конструкцију, на пример, на Диофантову тројку $\{1, 3, 120\}$, добићемо Диофантове четворке $\{1, 3, 8, 120\}$ и $\{1, 3, 120, 1680\}$. У вези са тим, споменимо да су Дујела и Петхо[7)] доказали 1998. године да се свака Диофантова тројка облика $\{1, 3, c\}$, где је $c \neq 8$, може на тачно два начина проширити до Диофантове четворке.

У доказу да се свака Диофантова четворка може допунити до рационалне Диофантове петорке, поново користимо сабирање и одузимање тачком S. Нека је $T(x, y)$ тачка на елиптичкој кривој E таква да број $d = \frac{x}{abc}$ задовољава услов да су $ad + 1, bd + 1$ и $cd + 1$ потпуни квадрати. Посматрајмо тачку $T \pm S = (x', y')$. Тада и број $d' = \frac{x'}{abc}$ задовољава исти услов као и d. Међутим, важи и више, $dd' + 1$ је такође потпун квадрат. Другим речима, $\{a, b, c, d, d'\}$ је рационална Диофантова петорка. Применом ове конструкције на Фермаов скуп $\{a, b, c, d\} = \{1, 3, 8, 120\}$, добијамо управо Ојлерово решење $d' = \frac{777480}{8288641}$.

9.6 Последња Фермаова теорема

• Ферма и почетак модерне теорије бројева

Диофантов рад је знатно утицао на арапске и европске математичаре, нарочито на Ферма. Проучавајући Башеов превод Диофантове *Аритметике* на латински језик из 1621. године, у којој Диофант приказује партикуларна решења једначина, Ферма је почео да тражи општа решења тих једначина. Ово се сматра почетком *модерне теорије бројева*. Тако је Ферма дошао до низа значајних резултата из теорије бројева, али није оставио скоро ниједан доказ[8)]. Током живота, Ферма није објављивао радове из математике. То је учинио његов син, који је 1679. године издао књигу његових радова *Varia opera mathematica – Разни математички радови*.

• Осми проблем и два коментара

Ферма је на маргинама Башеовог превода *Аритметике* написао 48 коментара. На 61. страни друге књиге налази се 8. проблем, [34]:

[7)] Отило Пећу (Attila Pethő, 1950), мађарски математичар

[8)] Неки математичари сматрају да је Ферма из теорије бројева оставио само један доказ, и то доказ тврђења да не постоји правоугли троугао са целобројним дужинама страница чија је површина квадрат неког целог броја

Квадрат[9] поделити на два квадрата.[10]

Диофант у решењу овог проблема показује како се број 16 – који је квадрат броја 4 – приказује као збир квадрата два друга броја: $\frac{256}{25}$ и $\frac{144}{25}$. Тако он решава конкретан проблем и на том решењу показује општи метод.

Дати проблем је, у суштини, *питагорејски проблем* представљен *Питагориним једначином*

$$x^2 + y^2 = z^2$$

чије је решење било познато Вавилонцима две хиљаде година раније. Уз тај проблем, Ферма је 1637. године написао свој најзначајнији коментар, [34]:

Куб у два куба, или биквадрат[11] у два биквадрата или уопште било који, од бесконачно много степена већих од квадрата, не може се разложити у два степена исте врсте.[12]

Изгледало је да се не зна зашто бар један скуп решења не би могао бити пронађен међу свим могућим бројевима, па ипак, Ферма је тврдио да се нигде у бесконачном универзуму бројева не може наћи таква тројка бројева. Била је то врло необична тврдња, али Ферма је веровао да је може доказати.

После првог коментара на маргини, Ферма је забележио и додатни коментар, који ће прогањати генерације математичара, [34]:

Нашао сам диван доказ за то, али он не може да стане на малу маргину.[13]

Без обзира на то, ниједан коректан доказ, који је морао бити изведен средствима математике XVII века, није пронађен наредних 357 година.

• Формулација последње Фермаове теореме

Коментарима, које је Ферма оставио, практично је формулисана једна од најпознатијих теорема[14] у историји математике. Она је свом аутору донела славу далеко изван граница математике. То је *последња Фермаова теорема*[15] позната и као *велика Фермаова теорема*, односно *последњи Фермаов проблем*. У савременим ознакама та теорема гласи, [34]:

[9] Мисли се на број који је квадрат неког другог броја.

[10] У оригиналу, на латинском језику: *Quadratum dividere in duos quadratos.*

[11] четврти степен неке величине

[12] У оригиналу, на латинском језику: *Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullom in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere.*

[13] У оригиналу, на латинском језику: *Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet.*

[14] Она је вековима погрешно називана теоремом уместо хипотезом, јер је Ферма тврдио да је њу доказао.

[15] Тај назив се користи од почетка деветнаестог века, јер су до тада све остале Фермаове теореме биле или потврђене или оповргнуте.

Теорема 9.7. Ако је n ма који природан број већи од 2, онда не постоје позитивни цели бројеви[16)] a, b и c такви да је

$$a^n + b^n = c^n.$$

Другим речима, једначина

$$x^n + y^n = z^n, \tag{9.13}$$

за $n > 2$ и $n \in \mathbb{N}$ нема решења у скупу позитивних целих бројева. □

Једначина (9.13) је једна од најпознатијих Диофантових једначина. Последњу Фермаову теорему можемо исказати и у терминима теорије скупова, [52, страна 12]:

$$\{n \mid n \in \mathbb{N} \wedge (\exists\, a, b, c \in \mathbb{Z}^+)\, a^n + b^n = c^n\} = \{1, 2\}.$$

Она је и генерализација Питагорине једначине $x^2 + y^2 = z^2$ која је повезана са Питагорином теоремом. Због тога кажемо да се Питагорина теорема може посматрати као једначина над рационалним или реалним бројевима.

Док последња Фермаова теорема сама по себи нема директну употребу – не користи се као доказ ни у једној другој теореми – показано је да је она повезана са другим математичким темама, због чега је и данас веома популарна. Њен доказ је једини математички доказ о коме је писано на насловној страни Њујорк Тајмса[17)].

• Разни покушаји доказа последње Фермаове теореме

Што се тиче покушаја доказа последње Фермаове теореме, познато је Фермаово решење само за $n = 4$, то јест за

$$x^4 + y^4 = z^4.$$

Ојлер, кога је Голдбах[18)] заинтересовао за теорију бројева, је доказао низ Фермаових тврђења, а 1753. године је написао да зна да докаже случај $n = 3$, то јест

$$x^3 + y^3 = z^3.$$

Доказ је објављен у његовој *Алгебри* 1770. године. У том доказу има пропуст, тако да он није коректан. Међутим, Ојлер је у другим радовима из теорије бројева користио чињенице којима се овај пропуст заобилази, тако да се може рећи да је Ојлер знао све потребне чињенице да напише коректан доказ. Око 1823. године Жермен[19)] је доказала да једначина

$$x^p + y^p = z^p$$

[16)] У теорији бројева радије се каже *позитиван цео* него *природан* број.

[17)] Њујорк Тајмс (на енглеском језику: The New York Times) су Њујоршке дневне новине

[18)] Кристиајн Голдбах (Christian Goldbach, 1690–1764), пруски математичар, који је као и Ферма студирао права

[19)] Марија-Софија Жермен (Marie-Sophie Germain, 1776–1831), француски математичар, физичар и филозоф

нема решење ако су p и $2p+1$ прости бројеви и $xyz \not\equiv 0 \pmod p$. Дирихле и Лежандр су доказали да једначина

$$x^5 + y^5 = z^5$$

нема решења око 1825. године. Дирихле је 1832. године решио и случај $n = 14$, то јест

$$x^{14} + y^{14} = z^{14},$$

а Ламе[20)] је 1839. године решио случај $p = 7$, то јест

$$x^7 + y^7 = z^7.$$

Ламе је 1847. године у француској академији наука изложио и скицу доказа последње Фермаове теореме, која је била уопштење Ојлеровог доказа за $n = 3$. После његовог излагања, Лиувил је приметио недостатак у изложеном доказу. Кумер[21)] је 1947. године доказао да једначина

$$x^p + y^p = z^p$$

нема решење када је p непаран прост број и p не дели бројиоце Бернулијевих бројева $b_2, b_4, \ldots, b_{p-3}$, при чему за бројеве b_i важи рекурентна формула

$$\begin{aligned} b_0 &= 1, \\ b_k &= \frac{-1}{k+1} \sum_{j=0}^{k-1} \binom{k+1}{j} b_j, \end{aligned}$$

где је $k > 0$. Кумер је 1857. године доказао последњу Фермаову теорему за све $n < 101$. У његовом доказу је било неких пропуста које је уочио и исправио Вандивер[22)] тек 1920. године. Вандиверов доказ је омогућио да се од 1928. до 1936. године последња Фермаова теорема провери помоћу стоних калкулатора за све $p < 619$. Вандивер је 1954. године, заједно са Лемером[23)], извршио њену проверу помоћу рачунара SWAC за све $p < 2\,003$. Селфриџ[24)] је 1967. године проверио да последња Фермаова теорема важи за све $p < 25\,000$. Вагстаф[25)] је 1978. године на рачунарима IBM 360/65 и IBM 370 извршио проверу за све $p < 125\,000$. И на крају, 1993. године је показано да последња Фермаова теорема важи за све $p < 4\,000\,000$.

Француска академија наука је два пута расписивала награду за доказ последње Фермаове теореме, 1816. и 1850. године. Награда није додељена, али је 1856. додељена медаља Кумеру.

[20)] Габријел Ламе (Gabriel Lamé, 1795–1870), француски математичар
[21)] Ернст Едуард Кумер (Ernst Eduard Kummer, 1810–1893), немачки математичар
[22)] Хари Шулц Вандивер (Harry Schultz Vandiver, 1882–1973), амерички математичар
[23)] Дерик Хенри Лемер (Derrick Henry Lehmer, 1905–1991), амерички математичар
[24)] Џон Левис Селфриџ (John Lewis Selfridge, 1927–2010), амерички математичар
[25)] Семјул Стендфилд Вагстаф, јуниор (Samuel Standfield Wagstaff, Jr, 1945), амерички математичар

Последња Фермаова теорема је први математички проблем, за чије решење је расписана награда приватне особе. Волфскел[26)] је својим тестаментом завештао 100 000 марака њеном решавачу – да је докаже или оповргне. Услов је да проблем буде решен у наредних 100 година од момента расписивања, то јест до 13. септембра 2007. године.

• Вајлс и прича о доказу последње Фермаове теореме

Са овом теоремом Вајлс се сусрео у локалној библиотеци када је имао само 10 година. Читајући Белову[27)] књигу *Последњи проблем* потпуно га је одушевило сазнање да постоји нерешен проблем чија формулација, на први поглед, делује толико јасно да о њему може да размишља чак и десетогодишњак.

Након што је постао професор на Универзитету Принстон, Вајлс, на тавану своје канцеларије, покушава у потпуној тајности, повучен у себе – све због тога да неко од његових колега не би сазнао чиме се он бави, а затим га још и предухитри са решењем – да дође до решења. После седам година напорног и усамљеничког рада – иако је све време подучавао студенте и похађао разне семинаре – у среду 23. јуна 1993. године на Институту математичких наука сер Исак Њутн[28)]у Кембрицу, у оквиру мале математичке конференције под називом *p-адичне Галоаове репрезентације, Ивасавина*[29)] *теорија*[30)] *и Тамагавини*[31)] *бројеви мотива*[32)], Вајлс је објавио свој доказ последње Фермаове теореме тако што је предавање на тему *Модуларне форме, елиптичке криве и Галоаове репрезентације* завршио речима, [3, страна 16]:

> ... и ово доказује последњу Фермаову теорему. Мислим да ћу овде стати.[33)]

Занимљиво је да је доказ последње Фермаове теореме у потпуности разумело можда свега двадесет математичара на свету, иако је њена формулација прилично једноставна, јер сам доказ представља бриљантни врх једне веома високе теоријске грађевине.

Одмах пошто је предавање у Кембрицу завршено, 200 страна Вајлсовог рада, који је он предао часопису *Inventiones mathematicae*, морало је бити проверено од стране шест рецензената које је одредио главни уредник тог

[26)] Паул Волфскел (Paul Wolfskehl, 1856–1906), немачки индустријалац који је и сам студирао математику

[27)] Ерик Темпл Бел (Eric Temple Bell, 1883 – 1960), шкотски математичар и писац научне фантастике

[28)] Isaac Newton Institute for Mathematical Sciences

[29)] Кенкичи Ивасава (Kenkichi Iwasawa, 1917–1998), јапански математичар

[30)] Ивасавина теорија је део теорије бројева на које се односила Вајлсова докторска дисертација, и у коју је он био јако добро упућен.

[31)] Тсунео Тамагава (Tsuneo Tamagawa, 1925–2017), математичар рођен у Јапану

[32)] У оригиналу, на енглеском језику: *P-adic Galois Representations, Iwasawa Theory and the Tamagawa Numbers of Motives*

[33)] У оригиналу, на енглеском језику: *... and this proves Fermat's Last Theorem. I think, I'll stop here.*

часописа.

Један од делова доказа дат је на проверу Нику Кацу[34)], који је 23. августа 1993. године пронашао грешку у доказу. Та грешка није значила да су Вајлсов труд и рад били узалудни, али јесте значила да ће он морати да ојача свој доказ. Вајлс се потрудио да исправи ту грешку, али се показало да она задире у саме темеље доказа.

Након шестомесечне изолације он одлучује да позове Тејлора свог бившег докторанда и једног од рецензената рада да ради заједно са њим и помогне му у отклањању те грешке. Тек годину дана касније Вајлс је успео решити проблем «заобилазним путем».

Џон Коутс[35)], Вајлсов ментор при изради докторске дисертације је тада објавио, [51, страна 285]:

> „Са математичког гледишта, финални доказ представља еквивалент открићу цепања атома или структуре ДНК."

На његов позив, Вајлс је крајем јуна 1993. године, у оквиру семинара о Ивасавиној теорији, одржао трочасовно поменуто предавање, које је он распоредио на три дела. Сваки дан је одржао по један део у трајању од једног часа.

Занимљиво је да је првог дана Вајлса слушало двадесетак математичара, другог дана је сала била попуњена до последњег места, а трећег дана, док је прилазио сали, Вајлс је морао себи да крчи пут кроз окупљене слушаоце. Људи су стајали и у ходнику, а сала је била препуна. Док је Вајлс поново исписивао наизглед бескрајне формуле и теореме на табли, атмосфера је постајала све напетија. Многи су понели и фотографске апарате, јер су наслућивали да ће се, на крају Вајлсовог предавања, догодити нешто заиста величанствено, што су касније и потврдили неки математичари. Присутнима је већ после другог дана било јасно да је прави циљ тродневног предавања био доказивање хипотезе Танијама[36)]-Шимура[37)].

• Хипотеза Танијама-Шимура. Модуларне форме

Сам Вајлсов рад не представља директан доказ последње Фермаове теореме, већ, као што смо видели, хипотезе Танијама-Шимура. Та хипотеза – коју су они поставили 1950. проучавајући елиптичке криве – повезује две потпуно различите области математике, и омогућава да се појмови везани за елиптичке криве преведу на језик модуларних форми.

Пре него што формулишемо хипотезу Танијама-Шимура, подсетимо се модуларних форми, као и Хекеовог[38)] оператора, [34].

[34)] Николас Мајкл Кац (Nicholas Michael Katz, 1943), амерички математичар
[35)] Џон Хенри Коутс (John Henry Coates, 1945), аустралијски математичар
[36)] Јутака Танијама (Yutaka Taniyama, 1927–1958), јапански математичар
[37)] Горо Шимура (Goro Shimura, 1930), јапански математичар
[38)] Ерих Хеке (Erich Hecke, 1887–1947), немачки математичар

Дефиниција 9.6. *Модуларна форма* тежине k је холоморфна комплексна функција дефинисана на $\mathbb{H} = \{z \mid z \in \mathbb{C}, \mathrm{Im}(z > 0)\} \cup \{i\infty\}$ горњој комплексној полуравни са бесконачном тачком за коју важи

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \tag{9.14}$$

при чему су a, b, c и d из $\mathbb{Z}$, k из $\mathbb{N}_0$, $ad - bc = 1$ и f је ограничена када z тежи $i\infty$.

Скуп свих модуларних форми тежине k означавамо са M_k.

Функција $f(z)$ из (9.14) има Фуријеов развој

$$f(z) = \sum_{n=-m}^{\infty} a_n q^n, \quad q = e^{2\pi i z}.$$

На основу [2, страна 121], имамо

Дефиниција 9.7. За фиксирани цео број k и било који позитиван број n Хекеов оператор T_n дефинишемо на скупу M_k са

$$(T_n f)(\tau) = n^{k-1} \sum_{d|n} d^{-k} \sum_{b=0}^{d-1} f\left(\frac{n\tau + bd}{d^2}\right).$$

Према [55, страна 225],

Хипотеза. [**Танијама-Шимура**] Нека је E елиптичка крива са целобројним коефицијентима. Ако је N њен кондуктор и ако је a_n низ бројева који се појављују у L-функцији елиптичке криве E, онда постоји нова модуларна форма тежине 2, нивоа N, која је карактеристична форма Хекеовог оператора са Фуријеовим развојем облика

$$\sum_{n=1}^{\infty} a_n q^n.$$

Другим речима, свака полустабилна елиптичка крива је модуларна.

• Фрејова крива и Рибетова теорема

Карику што спаја последњу Фермаову теорему са хипотезом Танијама–Шимура изнео је Фреј[39] на симпозијуму одржаном 1984. године у Немачкој који је имао за циљ да дискутује различите помаке у проучавању елиптичких кривих. Он полази од претпоставке да последња Фермаова теорема није истинита, то јест да постоји тројка (a, b, c) узајамно простих бројева која за прост број $p > 3$

[39] Герхард Фреј (Gerhard Frey, 1944), немачки математичар

задовољава једначину

$$x^p + y^p = z^p.$$

Пошто тада и тројка $(a, -c, -b)$ мора бити решење исте једначине можемо закључити да је b паран број и $a \equiv -1 \pmod 4$. Фрej тада посматра криву

$$y^2 = x(x - a^p)(x + b^p)$$

познату под називом и *Фрејова крива*, за коју је 1970. године Елгуарш[40)] уочио да има необичне особине, ако је

$$a^n + b^n = c^n,$$

за $n > 3$. Он износи и хипотезу да оваква крива јесте полустабилна елиптичка крива над пољем $\mathbb{Q}$, али да нема модуларну презентацију, то јест да није модуларна. Прецизне услове под којима то важи формулисао је Сер као ε-хипотезу. Да ти услови важе доказао је 1986. године Рибет[41)], након чега она постаје Рибетова теорема.

Дакле, ако последња Фермаова теорема није тачна, онда постоји елиптичка крива која није модуларна, а видели смо да свака елиптичка крива мора бити модуларна, па претпоставка да последња Фермаова теорема није тачна је погрешна, то јест последња Фермаова теорема је тачна. Одавде закључујемо да доказ последње Фермаове теореме следи из наредна два тврђења, [34].

Теорема 9.8. [**о модуларности**] Свака рационална, елиптичка крива

$$y^2 = ax^3 + bx^2 + cx + d$$

је модуларна. □

Теорема 9.9. [**Фрej, Сер, Рибет**] Нека је $a^n + b^n = c^n$. Тада елиптичка крива

$$y^2 = x(x - a^n)(x + b^n)$$

није модуларна. □

• Вајлсов коначни доказ

Вајлс 1993. године, након седам година проучавања разних елиптичких кривих и њихових модуларности, износи скицу доказа да је свака полустабилна елиптичка крива модуларна. Видели смо да пропусте који су тада уочени, он, заједно са Тејлором, успева да превазиђе. Тада настају два рада: *Модуларне елиптичке криве и последња Фермаова теорема*, аутора Ендруа Вајлса и *Теоријске особине прстена неких Хекеових алгебри*, аутора Ричарда Тејлора и

[40)] Ив Елгуарш (Yves Hellegouarch, 1936), француски математичар
[41)] Кен Рибет (Ken Ribet, 1948), амерички математичар

Ендруа Вајлса. Они су објављени 25. октобра 1994. године. Први рад је доказ последње Фермаове теореме и ослања се на други у битном кораку.

Оба та рада од 130 страна, најстроже прегледана у историји математике, објављена су и у 141. броју часописа *Annals of mathematics* на странама 443-551, у мају 1995. године.

Мада је Вајлс методама XX века доказао загонетку из XVII века, успео је да савлада Фермаов изазов по условима Волфскеловог комитета, и 27. јуна 1997. године добије награду у износу од 50 000 долара.

На крају напоменимо, иако је Вајлс доказао последњу Фермаову теорему, то јест хипотезу Танијама-Шимура, морамо приметити да доказ последње Фермаове теореме није дело само једног математичара. Иако је највећи део славе припао Вајлсу, на њу су подједнако право полагали и други математичари: Рибет, Мазур, Шимура, Танијама и Фрej. Њихова размишљања и теорије су помогле Вајлсу да докаже ту теорему.

Литература

[1] Д. Аднаћевић, З. Каделбург, *Математичка анализа II*, Математички факултет, Београд, 2008.

[2] T. Apostol, *The Hecke Operators*, Springer-Verlag, New York, 1997.

[3] A. Acel, *Poslednja Fermaova teorema – Odgonetanje drevne matematičke zagonetke*, Narodna knjiga-Alfa, Beograd, 2002.

[4] Ђ. Баралић, *О кривама другог реда – дијалог између геометрије и алгебре*, Државни семинар о настави математике и рачунарства у основној и средњој школи Друштва математичара Србије, Београд, 2018.

[5] M. Bertolini, *Report on the Birch and Swinnerton-Dyer conjecture*, 2010.

[6] N. Blažić, N. Bokan, Z. Lučić, Z. Rakić, *Analitička geometrija*, Matematički fakultet, Beograd, 2003.

[7] N. Bokan, S. Vukmirović, *Projektivna geometrija*, Matematički fakultet, Beograd, 2004.

[8] I. Vidav, *Eliptične krivulje in eliptične funkcije*, Društvo matematikov, fizikov in asronomov Slovenije, Ljubljana, 1991.

[9] *GeoGebra Centar Beograd*, http://geogebra.math.rs .

[10] K.Devlin, *The Millennium Problems – The Seven Greatest Unsolved Mathematical Puzzles of Our Time*, Granta Books, London, 2004.

[11] В. Драговић, Д. Милинковић, *Анализа на многострукостима: Примене у геометрији, механици, топологији*, Математички факултет, Београд, 2003.

[12] В. Драговић, М. Радновић, *Понселеови поризми, квадрике и билијари*, Завод за уџбенике, Београд, 2013.

[13] A. Dujela, *Eliptičke krivulje i njihova primjena u kriptografiji* – studentski seminar, PMF – MO, 2003.

[14] A. Dujela, *Eliptičke krivulje u kriptografiji*, PMF – MO, Sveučilište u Zagrebu, 2013.

[15] A. Dujela, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[16] A. Dujela, *Uvod u aritmetiku eliptichkih krivulja*, PMF – MO

[17] A. Dujela, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[18] G. Đanković, *Algebra 3* – dodatni materijal, Matematički fakultet, Beograd, 2018.

[19] G. Đanković, *Teorija brojeva*, Matematički fakultet, Beograd, 2013.

[20] D. Eisenbud, M. Green and J. Harris, *Cayley-Bacharach Theorems And Conjectures*, Bulletin (New Series) Of The American Mathematical Society, Volume 33, Number 3, July 1996.

[21] B. Ibrahimpašić, *Uvod u teoriju brojeva*, Pedagoški fakultet, Bihać, 2014.

[22] G. Kalajdžić, *Algebra*, Zavod za udžbenike, Beograd, 2011.

[23] G. Kalajdžić, *Linearna algebra*, Zavod za udžbenike, Beograd, 2011.

[24] Г. Калајџић, *Линеарна алгебра и геометрија*, Завод за уџбенике, Београд, 2011.

[25] G. Kalajdžić, M. Đorić, *Geometrija* – materijal za studente, Beograd, 2003.

[26] I. Connell, *Elliptic Curve Handbook*, Montreal, 1999.

[27] A. Lipkovski, *Algebraic Geometry (Selected Topics)*, Beograd.

[28] M. Mateljević, *Kompleksna analiza 1*, Zavod za udžbenike, Beograd, 2012.

[29] *Математика, физика, астрономија, рачунарство – школска енциклопедија*, Просвета, Београд, 1993.

[30] P. Miličić, *Kurs diferencijalne geometrije*, Gnosos, Beograd, 2005.

[31] Б. Милошевић, И. Мировић, Љ. Младеновић, *Прозор у свет математике – уџбеник из математике за пети разред основне школе*, Нова школа, Београд, 2015.

[32] В. Митић, З. Каделбург, Д. Ђукић, *Увод у теорију бројева*, Друштво математичара Србије, Београд, 2013.

[33] F. Najman, *Eliptičke krivulje nad poljima algebarskih brojeva*, Prirodoslovno matematički fakultet, Matematički odsjek, Zagreb, 2013.

[34] Ђ. Пауић, *Велика Фермаова теорема – 25 година од доказа* – предавање одржано 15. 03. 2019. године на Математичком факултету у Београду

[35] Đ. Paunić, *Funkcionalne jednačine klasičnih matematičkih funkcija*, Društvo matematičara Srbije, Beograd, 2020.

[36] M. Perović, *Istorija matematike • Tom III*, Crnogorska akademija nauka i umjetnosti, Podgorica, 2017.

[37] З. Петровић, *Алгебра 1* – Предавања за школску 2014/15 годину

[38] З. Петровић, *Алгебра 2* – Предавања за школску 2014/15 годину

[39] З. Петровић, Ж. Мијајловић, *Математичка логика: елементи теорије скупова*, Завод за уџбенике, Београд, 2012.

[40] М. Петровић, *Елиптичке функције • Интеграција помоћу редова*, Завод за уџбенике и наставна средства, Београд, 1997.

[41] Z. Rakić, *Materijali za predmet Geometrija 3*, Matematički fakultet, Beograd, 2013.

[42] Z. Rakić, *Materijali za predmet Linearna algebra i analitička geometrija*, Matematički fakultet, Beograd, 2015.

[43] Z. Rakić, *Materijali za predmet Matematika 1* – Fizička hemija, Beograd, 2010.

[44] Z. Rakić, *O rangu eliptičkih krivih* – Seminar za geometriju, obrazovanje i vizualizaciju sa primenama, Matematički institut SANU, Beograd, 2014.

[45] Z. Rakić, *Uvod u eliptičke krive* – Seminar za geometriju, obrazovanje i vizualizaciju sa primenama, Matematički institut SANU, Beograd, 2009.

[46] A. Samardžić, G. Nenadić, P. Janičić, LaTeX 2_ε *za autore*, Kompjuter biblioteka, Beograd, 2003.

[47] A. Savelov, *Ravninske krivulje*, Školska knjiga, Zagreb, 1979.

[48] J. Silverman, *The Arithmetic of Elliptic Curves, Second Edition*, Springer, New York, 2009.

[49] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

[50] *Eliptične funkcije*, http://sinbad.bplaced.net/dwnldir/elipt˙funkcije.pdf .

[51] S. Sing, *Fermaova poslednja teorema*, DN Centar, Beograd, 2004.

[52] З. Станић, *Дискретне структуре 2*, Математички факултет, Београд, 2018.

[53] J. Stedall, *Povijest matematike – kratki uvod*, Element, Zagreb, 2014.

[54] Z. Stojaković, M. Stojaković, *Vodič za LaTeX*, Univerzitet u Novom Sadu, Institut za metematiku i STYLOS, Novi Sad, 1996.

[55] S. Useinović, *Posljednja Fermaova teorema*, Vaspitanje i obrazovanje – Časopis za pedagošku teoriju i praksu 1, Podgorica, 2008.

[56] *Photo, image & design editor | Adobe Photoshop*, https://www.adobe.com/products/photoshop.html .

[57] D. Husemöller, *Elliptic Curves, Second Edition*, Springer-Verlag, New York, 2004.

[58] T. Šukilović, S. Vukmirović, *Geometrija za informatičare*, Matematički fakultet, Beograd, 2015.

[59] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography (2nd ed.)*, Chapman & Hall/CRC, Boca Raton London New York, 2008.

[60] A. Wiles, *The Birch And Swinnerton-Dyer Conjecture*

Индекс имена

Биографија

Бранислав Милошевић је рођен 28. новембра 1974. године у Београду. Детињство је провео на Дорћолу. Похађао је Основну школу „Перо Поповић Ага”– која сада носи назив „Михаило Петровић Алас”– и Електротехничку школу „Никола Тесла”у Београду.

Дипломирао је математику на Математичком факултету Универзитета у Београду и стекао звање дипломирани математичар – професор математике и рачунарства. Иако је завршио студије математике пре увођења «Болоње», ради даљег усавршавања, уписује мастер академске студије на истом факултету.

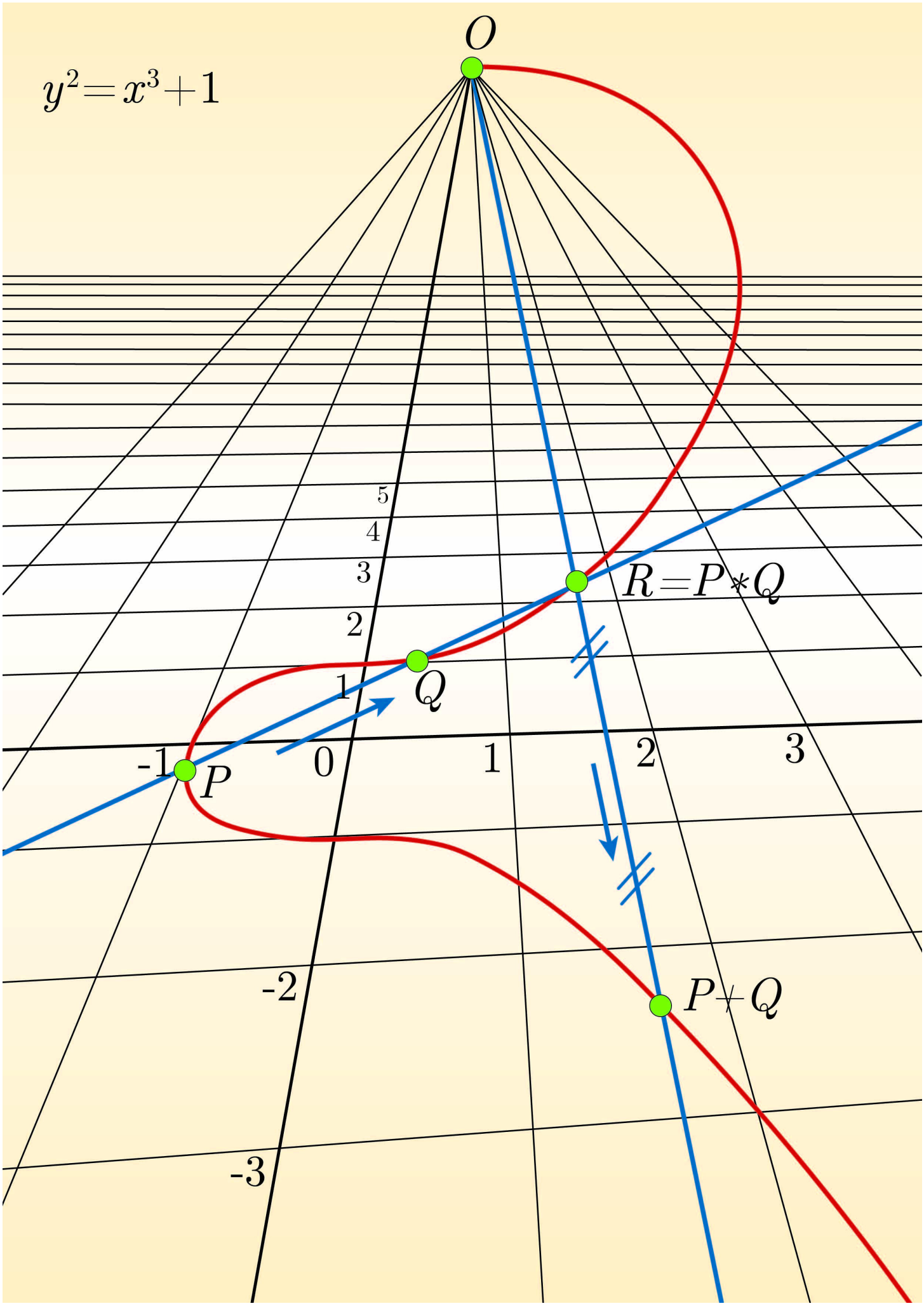
Предавао је Математику и Рачунарство и информатику и у основној и у средњој школи. Тренутно је запослен у ОШ „Горња Варош”у Земуну, где предаје математику.

Припремао је и водио ученике на многа такмичења. На јубиларном 50. Државном такмичењу из математике, одржаном 2017. године, у организацији Друштва математичара Србије, његов ученик је освојио похвалу, а њему је додељено признање за постугнуте резултате у раду са младим математичарима.

Коаутор је 37 публикација из математике – уџбеника, збирки задатака, радних листова и контролних вежби – у Издавачкој кући „Нова школа”из Београда. Писао је и популарне текстове из математике за часопис *Школарац*. Био је и аутор текстова за рубрику *Рачунам* у часопису *Наj*, у оквиру којих је настојао да деци дочара лепоту математике.

Поносан је и срећан што предаје математику. Воли да сарађује са децом и да их подучавајући уводи у необичан и чаробан свет математике.

Читање, писање, путовања, као и прављење занимљивих фотографија такође су поља његовог интересовања. Колекционар је већег броја књига – нарочито из математике – љубитељ је наливпера и калиграфије.


$y^2=x^3+1$
O
$R=P*Q$
Q
P
$P+Q$
5
4
3
2
1
-1
0
1
2
3
-2
-3