**Математички факултет у Београду**

МАСТЕР РАД

**СМЕР: ТЕОРИЈСКА МАТЕМАТИКА И ПРИМЕНЕ**

# Шаботи-Колеманов метод

Студент:
Стеван Гајовић
Број индекса: 1049/2015

Ментор:
др Горан Ђанковић

У Београду,
септембар 2016.

## Садржај

# 1 Увод

Диофантове једначине су од давнина окупирале пажњу и будиле радозналост код многих математичара. Почев од једноставних проблема које су постављали антички математичари долазимо данас до великих математичких резултата и области које су се развиле ради решавања разних Диофантових једначина, од којих је најпознатија *Велика Фермаова Теорема*. Као што можемо да приметимо и цела област носи име по једном античком математичару, *Диофанту*, тако да је већ то довољно да закључимо од када је ова област актуелна у математици. У својим чувеним књигама „*Аритметика*" оставио је велики број једначина које треба да се реше у скупу целих или рационалних бројева, због чега и цела област носи име по њему.

Колико су важне Диофантове једначине за математику, говори и то да је један од чувених 23 проблема које *Давид Хилберт* наводи на Међународном конгресу математичара у Паризу 1900. године као проблеме који би требало да окупирају математички свет у наредном веку баш проблем експлицитног решавања Диофантових једначина. Конкретно, овај проблем је *Хилбертов десети проблем* и гласи:

„За дату Диофантову једначину са рационалним коефицијентима и било којим бројем непознатих, одредити на који начин у коначном броју корака (савременим речником, алгоритам) можемо одредити да ли та једначина има решења у скупу рационалних бројева."

На основу Хилбертових ставова делује да је Хилберт веровао да тражени алгоритам постоји. Као и у свим осталим случајевима, био је убеђен да сваки математички проблем мора имати одлучиво решење.

Конкретно, проучавајући овај проблем, математичари су временом све више веровали да ипак не постоји тражени алгоритам. Треба узети у обзир да је Хилберт ово питање поставио и пре развоја *математичке логике* и свакако пре чувене *Геделове теореме о непотпуности математичког система*. Након развоја ове теорије, заједничким радом, математичари *Мартин Дејвис*, *Хилари*

*Патнам*, *Џулија Робинсон* и *Јуриј Матијашевич* су дали одговор на Хилбертово питање, који је негативан.

**Теорема 1.** Решивост Диофантових једначина је неодлучив проблем.

Дакле, не може се наћи алгоритам којим можемо решити сваку Диофантову једначину, чак је њихов резултат и прецизнији од ове наведене теореме. Наиме, они су доказали да постоји експлицитан полином $F(x_0, x_1, ..., x_n)$ такав да не постоји алгоритам који би за било које $a \in \mathbb{Z}$ као дати податак одредио да ли постоје целобројна решења једначине $F(a, x_1, ..., x_n) = 0$!

У пракси, најчешће није тешко одредити сва решења Диофантове једначине, најтежи део посла је доказивање да нема осталих решења. Тај део је и кључан у тексту теореме која каже да не постоји алгоритам којим можемо решити Диофантову једначину „до краја". Зато, математичари покушавају да пронађу разне начине како би нашли решење и, очекивано, пробали су да употребе разне гране математике у решавању овог проблема, од којих су се неке највише и развиле управо захваљујући Диофантовим једначинама.

Диофантове једначине се могу решавати уз помоћ многих области математике и управо је то била лепота ове области која ме је мотивисала да одаберем овакву тему за мастер. Остатак ове главе има намену да презентује примере како се разне математичке области користе у решавању Диофантових једначина и да пружи мотивацију како за конкретно оно што је предмет овог мастер рада, тако и за целокупну област.

**Препоручена литература:** Многи текстови Михаела Штола, као што су [РПК1-Ш], [РПК2-Ш], [55], [60], текст Самира Сиксека са конференције у Охриду [45] и Бјорна Пунена [38], су одлични као мотивациони текстови о Диофантовим једначинама, садрже разне примере и презентацију историјских и досадашњих важних резултата у овој области.

## 1.1 Одабрани примери Диофантових једначина

У наредном тексту се налази кратак преглед одређених Диофантових једначина са литературом одакле их прочитати. То су примери који илуструју како се разне математичке области примењују у решавању Диофантових проблема (Диофантових једначина и Диофантових апроксимација). За више интересантних примера погледати књигу велемајстора ове области [32].

### Позната анегдота и ирационалност

Добро је познато да су Стари Грци на почетку сматрали да су бројеви само (позитивни?) рационални бројеви. У то време је било шокантно откриће да дијагонала квадрата странице 1 није број, тј. није рационалан број. Једна од прича која се помиње јесте да је један Питагорин ученик убијен зато што је изнео тврдњу о том открићу.

Преласком на математику, поставља се питање да ли постоје природни бројеви $p$ и $q$ такви да $\frac{p}{q} = \sqrt{2}$, тј. $p^2 = 2q^2$. Ове две једначине су еквивалентне, зато што се ради о природним бројевима, али разликују се у чињеници да је ова друга једначина Диофантова, док прва то није. Бар у изворном облику, за Диофантове једначине сматрамо једначине које се састоје од рационалних или целих бројева и где се траже таква решења.

Међутим, ова Диофантова једначина није Диофантова једначина најједноставнијег типа, то су линеарне Диофантове једначине, које се рутински решавају, али се решава лако, можемо да претпоставимо да су $p$ и $q$ узајамно прости и онда докажемо да су дељиви са 2, што је контрадикција, тј. једначина нема решења.

Ово је само почетак, касније се може показати ирационалност многих бројева, $\sqrt{n}$, где је $n$ природан број који није квадрат, $\pi$, $e$, ... Докази да $\pi$ и $e$ садрже у себи *математичку анализу*, што је већ један пример како области морају да се удруже да бисмо добили неки резултат.

Међутим, сама ирационалност нема нешто пуно везе са Диофантовим једначинама, тако да ћемо се концентрисати на нешто што има везе, а то је има ли полиномна једначина по $x$ рационал-

но решење, ако су коефицијенти рационални бројеви

$$a_n x^n + ... + a_1 x + a_0 = 0.$$

Када помножимо једначину свим имениоцима разломака коефицијената, добијемо једначину истог оваквог типа, само са целобројним коефицијентима. Тада за решење $x = \frac{p}{q}$, са узајамно простим целим бројевима $p$ и $q$ важи да $p \mid a_0$ и $q \mid a_n$ (ово је посебно згодно кад је $a_n = 1$). Овако добијамо само коначно много рационалних кандидата за решење, па ако сви отпадну, ова једначина нема рационалних решења. На пример, на овај начин се може доказати да је $\sin 20^\circ$ ирационалан број. Све ово се може наћи у књизи [3].

**Питагорине тројке - теорија бројева, алгебра, геометрија, алгебарска геометрија**

Ово је још један познат историјски пример, али је интересантан јер се може решити на више начина. Траже се цели бројеви (или рационални) који могу бити странице правоуглог троугла. Другим речима, решавамо једначину $x^2 + y^2 = z^2$ у скупу целих (или рационалних бројева).

Врло једноставно се решења изводе алгебарски само уз помоћ пропорција, док слична идеја уз коришћење теорије бројева такође пролази, то се може наћи у многим књигама, нпр. у [3].

Следећи начин је лепши и више поучан, а зове се рационална параметризација круга, и може се наћи у [52]. Поделимо све са $z$ тако да добијемо рационално решење једначине $x^2 + y^2 = 1$. Ово је круг у равни, и треба одредити његове рационалне тачке.

То постижемо тако што фиксирамо једну рационалну тачку (обично се узима $(-1, 0)$) и вучемо линије рационалног нагиба. Када повучемо све могуће овакве линије, одредићемо и све рационалне тачке круга. Ово је пример где *геометрија* али и дух *алгебре* помаже решавању Диофантових једначина.

На крају, можемо посматрати једначину $x^2 + y^2 = z^2$ над било којим пољем $K$ као један алгебарски пројективни варијетет. Тада можемо проверити да је $[s, t] \mapsto [s^2 - t^2, 2st, s^2 + t^2]$ изоморфизам пројективне праве $\mathbb{P}^1(K)$ и овог варијетета, са инверзним $[x, y, z] \mapsto [x + z, y]$, а као што видимо овако се заиста описују сва

рационалне и целобројне Питагорине тројке. Ово се може наћи у [51].

**Диофантове апроксимације**

Као што је познато, у стварном свету су нам потребне „добре" апроксимације математичких вредности које не можемо прецизно да одредимо. Међутим, то је посао нумеричке математике, а не теорије бројева (иако $p$-адска анализа има важне теореме које су у духу нумеричке математике), тако да овде значење „добре" апроксимације није само да је број што ближи броју који желимо да апроксимирамо.

У теорији бројева нас интересују особине ирационалних бројева и алгебарских, односно трансцендентних бројева. Проценјиваћемо бројеве уз помоћ рационалних бројева. Мера „јачине" апроксимације је степен имениоца, тј. за реалан број $\alpha$ нас интересују неједнакости $\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^t}$, где је $c$ константа коју у пракси сами тражимо - намештамо у зависности од $\alpha$, са жељом да степен $t$ на десној страни буде што већи.

Можемо да кажемо, да за разлику од Диофантових једначина где решавамо једначине у скупу целих (рационалних) бројева, тако се Диофантове апроксимације баве решавањем неједнакости у целим (рационалним) бројевима.

Прво се уз помоћ Дирихеловог принципа доказује да постоје узајамно прости цели бројеви $p$ и $q$ тако да $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$, и то за ирационалне $\alpha$ оваквих парова има бесконачно много.

Даље се лако изводи критеријум када је број $\alpha$ рационалан или не: $\alpha$ је рационалан ако и само ако постоји константа $c > 0$ (која зависи од $\alpha$) тако да за све $\frac{p}{q} \neq \alpha$ важи $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q}$. Уз помоћ овог тврђења можемо да покажемо да је, на пример, следећи број ирационалан

$$\alpha = \sum_{n=0}^{\infty} \frac{(-1)^n}{2^{n^2}}.$$

Даље, постоји начин како да одредимо да су неки бројеви трансцендентни. Ако је $\alpha$ алгебарски број степена $d$, може се показати да постоји константа $c$ која зависи од $\alpha$ таква да $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^d}$,

одакле су једино трансцендентни бројеви они који могу да имају произвољно добру апроксимацију (што већи степен), а уз помоћ овог тврђења можемо да утврдимо да је трансцендентан, на пример, следећи број

$$\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}.$$

Постоји још једна теорема која карактерише трансцендентност - Линденманова теорема која каже да ако постоје алгебарски бројеви $\alpha_2$, ... , $\alpha_n$, $C_1$, ... , $C_n$, такви да је бар један од ових бројева $C_i \neq 0$, који задовољавају једначину

$$C_1 e^{\alpha_1} + C_2 e^{\alpha_2} + ... + C_n e^{\alpha_n} = 0$$

тада је $\alpha_1$ трансендентан број. Уз помоћ ове теореме се лако доказује да је $\pi$ трансцендентан број.

Вратимо се на последњу написану неједнакост, у којој желимо да смањимо степен $d$ (уз исте услове). Математичари су успели да спусте тај степен, прво на $\frac{d}{2} + 1$, а онда и на $O(\sqrt{d})$, од којих је најбоља била $\sqrt{2d}$. Највећи резултат овог истраживања је уследио када је математичар Рот не само спустио степен тако да не зависи од $d$ већ и на најбољи могући. Та теорема ће се наћи касније у најзначајнијим резултатима ових области.

За крај, као показатељ колико су ови проблеми тешки, напоменимо да се за бројеве $\pi \pm e$ и $\pi \cdot e$ и даље не зна ни да ли су алгебарски, а чак се и не зна да ли су и ирационални уопште! Веома корисни апарат за Диофантове апроксимације су следећи типови разломака *Фарејев низ* и *верижни разломци*. Наведене ствари се могу наћи у [1], [3], [5].

**Пелова једначина, помоћ Диофантових апроксимација**

Пелова једначина је једначина облика $x^2 - dy^2 = 1$, где је $d$ бесквадратни природан број и траже се целобројна решења. Једна од познатих прича које се везују за Пелову једначину је питање колико минимално треба војска да има војника (више од 1) тако да се може поређати у квадратну формацију, али такође да се може поређати у 61 квадратну формацију тако да преостане тачно један

војник. Ово је наравно исто као да тражимо минимално нетривијално решење Пелове једначине $x^2 - 61y^2 = 1$. Врло је тешко наћи то решење, јер су у питању велики бројеви $x = 1766319049$ и $y = 226153980$, што су нашли индијски математичари, одакле је минималан број војника - $x$ већи од броја становника било које државе (бар по званичним подацима).

Међу мањим бројевима (до 128), једино за $d = 109$ је веће минимално решење, што се може видети на Википедији. Такође, једна од занимљивих ствари везаних за ову једначину јесте и нешто што није тако ретко у математици, велики број математичара сумња да је Пел уопште имао било какав допринос решавању ове једначине, па чак и да се уопште њом и бавио.

Уз помоћ *Диофантових апроксимација* се доказује да постоји нетривијално решење Пелове једначине (различито од $(\pm 1, 0)$). Тада се оно записује у облику $x_1 + y_1\sqrt{d}$, а свако друго решење се добија из једнакости $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. Лако се види да ови бројеви јесу решења једначине, а уз помоћ вештог баратања са неједнакостима и уз познате резултате Диофантових апроксимација се доказује да су једина.

Постоји и други начин, више *геометријски* који одређује решења Пелове једначине и личи на геометријски метод код Питагориних тројки (што не изненађује, јер су у питању једначине степена 2). Ова крива је хипербола, те уочимо само део са позитивним $x$. Знамо да једначина има тривијално решење $(1, 0)$ и минимално $(x_1, y_1)$. Желимо да одредимо рационалну линеарну трансформацију (тј. трансформацију облика $(x, y) \mapsto (ax + by, px + ry)$, где су $a, b, p, r \in \mathbb{Z}$) која слика параболу у себе, а $(1, 0)$ у $(x_1, y_1)$. Из овог последњег услова закључујемо $a = x_1$, $p = y_1$, док из тога што се парабола слика у себе се онда добија $b = dy_1$ и $r = x_1$, што нам даје исте рекурентне формуле као и степеновање. Ово пресликавање је бијективно, одакле се могу извести целобројна решења Пелове једначине, јер ће се целобројна решења сликати у нека друга целобројна решења.

Као што смо видели, некад је тешко одредити минимално решење Пелове једначине, а сем метода који су знали индијски математичари, постоји и метод уз помоћ верижних раломака, што је описано у [5]. О Пеловим једначинама, као и о једначинама Пеловог типа се може наћи још материјала у [3], [32].

**Теорија скупова и Диофантове једначине - метода минималног решења**

Иако *теорија скупова* и *теорија модела* имају веома велики утицај данас на Диофантове једначине, то је сувише напредна материја за овај мастер рад, тако да овде наводимо само једну најосновнију идеју, тј коришћење својства да сваки подскуп скупа природних бројева има *минимални елемент*.

Поред неких уводних једначина које се могу решити овом методом, као на пример $x^2 + y^2 = 3z^2$ или $x^2 + y^2 + z^2 = 2xyz$ у скупу целих бројева, вероватно најпознатији примере је случај $n = 4$ Велике Фермаове Теореме, тј. доказ да једначина $x^4 + y^4 = z^4$ нема нетривијалних целобројних решења. У ствари, доказ се своди на то да се докаже да једначина $x^4 + y^4 = z^2$ нема решења у скупу природних бројева и у доказу се корити опис Питагориних тројки. Ово се може наћи у разним књигама, на пример у [3], [32], [5].

**Алгебра помаже у решавању Диофантових једначина**

Један од начина уз помоћ којих смо одредили Питагорине тројке је растављање $x^2 = z^2 - y^2 = (z - y)(z + y)$ и уз претпоставку о томе да су $y$ и $z$ узајамно прости смо дошли до закључка који описује сва решења. Многе једначине се могу решити на овај начин, на пример, $x^3 + y^3 = 1729$, $x^2 + 2^y = z^2$ у целим бројевима.

Међутим, некад је немогуће раставити почетну једначину, на пример, $x^2 + 2 = y^3$. Међутим, некад и када можемо да раставимо изразе, као у $x^2 + 1 = y^3$, тј. $x^2 = (y - 1)(y^2 + y + 1)$ не можемо лако да решимо једначину, јер имамо незгодан случај $y^2 + y + 1 = 3m^2$ и $y - 1 = 3n^2$. Слично је и са $x^2 - 1 = y^3$, јер поред сличног проблема из претходне једначине, ни друго растављање нам не помаже, јер $(x - 1)(x + 1) = y^3$ може да да случајеве $x - 1 = 2m^3$ и $x + 1 = 4n^3$ и обрнуто, који нису лаки.

Из ових разлога, одлазимо из $\mathbb{Z}$ у већи прстен где можемо раставити једначину на погоднije факторе. Ту се види помоћ *алгебре* преко *проширења прстена*. Ради илустрације, једначину $x^2 + 2 = y^3$ растављамо на $(x + i\sqrt{2})(x - i\sqrt{2}) = y^3$, а сада ову једначину више не решавамо у целим бројевима, него у прстену $\mathbb{Z}[i\sqrt{2}]$.

Грешка коју можемо да направимо јесте да верујемо да је прстен $\mathbb{Z}[i\sqrt{2}]$ исти као и $\mathbb{Z}$, бар у смислу аритметике. У том прстену имамо среће, јер ће он заиста имати јако слична својства као прстен $\mathbb{Z}$, међутим, неће то да важи за сва раширења прстена $\mathbb{Z}$, зато нам треба алгебра да нам помогне у анализирању тих прстена.

Једна од најпознатијих једначина која се решава овом методом је случај $n = 3$ Велике Фермаове теореме. Једначина $x^3+y^3 = z^3$ се може записати као $(x + y)(wx + w^2y)(w^2x + wy) = z^3$, где је $w$ примитиван трећи корен из јединице. Дакле, решава се једначина у прстену $\mathbb{Z}[w]$, који је еуклидски, и показује се да ту нема нетривијалних решења, а се доказ може наћи у [32] или у [3], док се многа својства раширења прстена (њихове особине, теореме које важе, примери) $\mathbb{Z}$ могу наћи у [1].

**Геометрија помаже у решавању Диофантових једначина**

Као што смо видели, Питагорине тројке се могу описати геометријски. Тај метод може да опише решења многих једначина степена 2 по $x$, $y$ и $z$, што се може наћи у [3]. Међутим, геометријски метод пролази и за неке криве степена три, конкретно за елиптичке криве, тј. (углавном) за једначине облика $y^2 = x^3+ax^2+bx+c$.

Ако знамо две рационалне тачке на овој кривој, јасно је да их не можемо сабрати на уобичајен начин, а да добијемо ново решење једначине. Зато уводимо сабирање уз помоћ *геометријског правила*. Даћемо опис сабирања за облик једначине који је наведен изнад, а и иначе се сабирање изводи на јако сличан начин. Повлачимо линију кроз те две тачке и пресецамо трећи пут са кривом. Онда узимамо тачку супротну њој у односу на $x$-осу (која је исто на кривој, јер ова промена само мења знак $y$ координати).

И овде има мало помоћи *алгебре* када показујемо да је ово сабирање добро дефинисано. Испоставља се да на овај начин рационална решења чине комутативну групу. Могу се експлицитно одредити једначине овог сабирања, а може и уз помоћ једне теореме из *алгебарске геометрије* (ако за три криве трећег степена (кубике) $C$, $C_1$, $C_2$ важи да $C$ пролази кроз 8 пресечних тачака $C_1$ и $C_2$, тада $C$ пролази и кроз девету пресечну тачку $C_1$ и $C_2$) да се провери асоцијативност овог сабирања, пошто се остала својста

лако проверавају.

Важан резултат јесте да је та група коначно генерисана. Варијанта ове теореме само за поље $\mathbb{Q}$ се може наћи у [52], као и примери, слике и објашњења оваквог решавања елиптичких кривих, док је за изучавање елиптичких кривих над бројним пољима позната литература [51]. У овој књизи се може наћи још доста математике које је потребно за одређивање рационалних тачака или тачака са координатама у неком бројном пољу на елиптичким кривама, и где се може видети алгебарска позадина геометријског сабирања тачака на кривој. Још увек није познат алгоритам којим се могу одредити све рационалне тачке било које елиптичке криве (више о томе се може видети касније, код кривих рода $g = 1$), а и због ограничености времена и простора ћемо прескочити начине на које се може доћи до решења. Наводимо две лепе примене елиптичких кривих на Велику Фермаову Теорему (има и још интересантних примера, а ово се може пронаћи у [35]).

(1) Случај $n = 3$: $x^3 + y^3 = z^3$.

Ово можемо да видимо као пројективну криву рода 1, која има бар једну рационалну тачку (нпр. $(0, 1, 1)$), тако да је ово једна елиптичка крива. Променом координата (у духу поступка из [52]), $x = x + y + z$, $y = -x - y + z$, $z = y + z$, која је оправдана, добијамо једначину $6x^2z + 12xyz - y^3 + 3y^2z - 3yz^2 + z^3 = 0$. Приметимо да ново $z$ не може бити 0, па можемо претпоставити да је $z = 1$, односно добијамо афину елиптичку криву (заменом $x$ и $y$)

$$6y^2 + 12xy = x^3 - 3x^2 + 3x - 1.$$

Заменом $(x, y)$ у $(\frac{x}{6}, \frac{y}{36})$ имамо познатији облик

$$y^2 + 12xy = x^3 - 18x^2 + 108x - 216.$$

Познатим методама или коришћењем програма **SAGE** долазимо до тога да су једине рационалне тачке на овој кривој $(6, 0)$, $(6, -72)$ и бесконачна тачка. Бесконачна тачка нам не даје рационално решење полазне једначине, јер смо рекли да овде $z \neq 0$, а заменом ова два решења назад добијамо $y = 0$, односно $x = 0$, што су тривијална решења. Дакле, једначина $x^3 + y^3 = z^3$ има само тривијална решења (неки од бројева $x$, $y$, $z$ је нула).

(2) Случај $n = 4$: $x^4 + y^4 = z^4$

Доказаћемо да једначина $x^4 + y^4 = z^2$ нема нетривијалних решења. Поделимо са $y^4$, одакле сменом $u = \frac{x}{y}$ и $v = \frac{z}{y^2}$ добијамо једначину $u^4 + 1 = v^2$ у $\mathbb{Q}$. Уместо ове једначине посматрамо еквивалентан систем $t = u^2$ и $t^2 + 1 = v^2$ у $\mathbb{Q}$. Када помножимо ове две једначине добијамо елиптичку криву $t^3 + t = s^2$ (где је $s = uv$). Као и у претходном случају, можемо решити ову једначину или користити програм **SAGE**. Добијамо да ова једначина има тачно 2 рационална решења, бесконачно које нам не доприноси решењу наше једначине и $(t, s) = (0, 0)$, а одавде је $u = 0$, па и $x = 0$, што је тривијално решење.

**Напомена.** Елиптичке криве имају и важну улогу у доказу Велике Фермаове Теореме и у осталим случајевима, што ћемо видети мало касније.

### Анализа и решавање Диофантових једначина, $p$-адски бројеви

Када доказујемо да једначине $x^2 + 3x^3 + 1 = 3y^2$, $x^3 + y^3 + z^3 = 4$, $27^x + 2016 = y^3$ немају решења, онда то радимо по модулу 3, 9, 27, редом, али не можемо да их решимо по модулу мањег степена тројке од наведеног. Било би згодно да нађемо неки универзални метод који би покупио све овакве технике одједном. Зато уводимо бројеве облика $a_0 + a_1 p + ... + a_n p^n + ...$, $0 \leq a_i \leq p - 1$. Овај ред очигледно не конвергира у $\mathbb{R}$, па уводимо другачију метрику (и то такву да имамо користи у теорији бројева) у којој је већи степен $p$ у ствари мањи број, тако да у новом случају имамо конвергенцију.

Тако настаје $\mathbb{Z}_p$ - *прстен $p$-адских целих бројева*, мада обично прво конструишемо $\mathbb{Q}_p$ - *поље $p$-адских бројева*, које је количнико поље $p$-адских целих бројева, а испоставља се да се $p$-адски бројеви записују као Лоранови редови по $p$ са коначним половима, тј. да се сума продужава коначно на негативне степене $p$.

Пошто се поља $\mathbb{Q}_p$ раширења поља $\mathbb{Q}$, важи да ако једначина нема решења у неком од тих поља, онда нема ни у $\mathbb{Q}$. То је један од начина да користимо ове нове бројеве. На пример, једначина $3x^2 + 2y^2 - z^2 = 0$ нема нетривијална решења у $\mathbb{Q}_3$, док $y^2 = 2x^6 - 4$

нема решења у $\mathbb{Q}_2$, одакле прва једначина има само тривијално решење у $\mathbb{Q}$, док их друга нема уопште. Постоји поступак којим можемо да проверимо да ли једначина има решења у пољима $\mathbb{Q}_p$, који ћемо описати у трећој глави, док такав поступак не постоји за $\mathbb{Q}$, одакле видимо једну ових $p$-адских поља.
Нема потребе овде више трошити простор о овоме, због тога што ће у трећој глави бити доста речи о $p$-адским бројевима, али са јако кратким уводом. Литература за $p$-адске бројеве: [25], [29], [2], [44], [57], [41], [53].

**Линеарна алгебра у решавању неких Диофантових проблема**

Познати су математички проблеми у којима се тражи да се природан број представи као збир неколико квадрата целих бројева, који су били нарочито популарни у 18. веку. Наведимо их неколико.
(1) Који се природни бројеви могу представити као збир два квадрата целих бројева?
(2) Који се природни бројеви могу представити као збир три квадрата целих бројева?
(3) Који се природни бројеви могу представити као збир четири квадрата целих бројева?
(4) Који се природни бројеви могу представити као збир три троугаона броја?
(5) Да ли можемо решити једначину у којој збир 5 и више квадрата, поможених коефицијентима треба да буде једнак 0 у скупу рационалних бројева?

Одмах видимо да се четврти задатак разликује, међутим није то баш толико тачно у шта ћемо се убрзо уверити, а само напоменимо да су троугаони бројеви збирови бројева од 1 до $n$, тј. бројеви облика $\frac{n(n+1)}{2}$.

Задаци (1) и (3) су познати од давнина и имају решења која користе само елементарну теорију бројева. Наравно, могу се решити и на други начин, на пример број (1) уз помоћ Гаусових целих бројева $\mathbb{Z}[i]$. Али то нам није од интереса овде, па ћемо се фокусирати на преостала три проблема.

Појмови квадратних форми, њихових матрица, промене базе и свођења на канонски облик где имамо само збир квадратних члано-

ва и немамо мешовите су појмови *линеарне алгебре*. Међутим, вешто баратање квадратним формама уз помоћ $p$-адске анализе доноси веома важан резултат - *Хасеов принцип*.

Кажемо да се $a$ може представити квадратном формом $f$ у неком пољу ако постоје скалари из тог поља који када се убаце у $f$ дају $a$, када је $a \neq 0$, док за $a = 0$ захтевамо да не буду сви скалари 0. Хасеов принцип нам тврди да за квадртну форму са рационалним коефицијентима важи да је 0 представљива том формом у $\mathbb{Q}$ (представљање у $\mathbb{Q}$ зовемо глобално) ако и само ако је представљива у сваком комплетирању $\mathbb{Q}$, тј. у свим $\mathbb{Q}_p$ и $\mathbb{R}$ (представљања у овим пољима зовемо локална).

Једна од формулација овог тврђења је да Диофантова једначина другог степена има решења у $\mathbb{Q}$ ако и само ако има решења у свим $\mathbb{Q}_p$ и $\mathbb{R}$. Морамо признати да овај резултат делује магично. У мору примена које има овај резултат, специјално издвајамо и примене на наше задатке.

(2) Лакши део овог тешког задатка је уочити да се бројеви облика $n = 4^a(8b + 7)$ не могу записати као збир три квадрата. Тежи део задатка је да докажемо да сви остали бројеви могу да се запишу као збир три квадрата. Приметимо да важи $n = 4^a(8b+7)$ ако и само ако је $-n$ квадрат у пољу $\mathbb{Q}_2$. Уз помоћ знања о квадратним формама над $p$-адским пољима изводимо резултат да се $n$ може записати у $\mathbb{Q}$ као збир три квадрата ако и само ако $-n$ није квадрат у $\mathbb{Q}_2$.
Из свега претходног добијамо преостали део теореме о представљивости као збир три квадрата, али у $\mathbb{Q}$. Зато нам треба и резултат који нам из представљивоти у $\mathbb{Q}$ даје представљивост у $\mathbb{Z}$, који је дело *Девенпорта* и *Каселса*. Све ово заједно нам даје тражени одговор, а овај задатак се некад назива теорема *Гауса*, а некад *Лагранжова теорема о три квадрата*. Обојица су у периоду 1796. – 1801. решила овај проблем, при чему је Гаус извео и нешто општији резултат.

(3) Из (2) видимо да је довољно да докажемо да се бројеви облика $n = 4^a(8b + 7)$ могу представити као збир четири квадрата. Али, тада $n-1$ није број тог облика, одакле знамо да $n-1$ можемо да представимо као збир три квадрата и када додамо $1 = 1^2$ до-

бијемо представљање $n$ у облику четири квадрата. Све природне бројеве можемо да представимо као збир четири квадрата.

(4) Кључно је да уочимо $\frac{n(n+1)}{2} = \frac{1}{8}\left((2n+1)^2 - 1\right)$ и да приметимо да се сваки број облика $8k+3$ записује као збир три непарна квадрата, одакле добијамо тражени резултат. Зато и овај проблем има везе са представљањем броја преко збирова квадрата.

(5) Анализом квадратних форми над пољима $\mathbb{Q}_p$ долазимо до закључка да, ако се квадратна форма може свести на збир бар пет квадрата (пута неки коефицијент), постоји представљање 0 том квадратном формом (наравно, где нису само 0 убачене). Дакле, представљање 0 овом формом у $\mathbb{Q}$ еквивалентно је са представљањем 0 том формом у $\mathbb{R}$. Дакле, једначина

$$a_1x_1^2 + ...a_nx_n^2 = 0,$$

где је $n \geq 5$ има решења у $\mathbb{Q}$ ако и само ако их има у $\mathbb{R}$! Мора се признати да је ово јако занимљив резултат.

Ови задаци прате књигу [44], али за неке делове овог текста су добра литература и [32] и [41].

**Раманујан - Нађелова једначина**

Одлична илустрација тога колико је математике потребно да би се решиле неке Диофантове једначине је једначина $x^2 + 7 = 2^m$. Ова, наизглед једноставна једначина има јако компликовано, али зато и прелепо решење. Занимљиво је истаћи да ова једначина има чак 5 различитих решења по $m$: 3, 4, 5, 7, 15.

У њеном решавању, потребно је да користимо и *алгебру*, јер прелазимо у раширење прстена $\mathbb{Z}$ - $\mathbb{Z}(\frac{1+i\sqrt{7}}{2})$ (јер ту можемо да растависмо $x^2 + 7$), који је еуклидски прстен и *анализу* јер користимо $p$-адске методе и то баш праве аналитичке. Све ово се може наћи у [2]. Такође, на сличан начин се може решити и једначина $3^x = 2y^2 + 1$.

## 1.2 Важни резултати до данас

Свакој кривој можемо придружити важну геометријско-тополошку инваријанту - *род криве*. Ако криву замислимо као пројективну комплексну криву, па је онда гледамо као реалну површ, свака крива ће имати коначан број „рупа" (нпр. сфера нема рупе, торус има једну рупу) и тај број рупа се назива род криве. Постоји фантастична теорема која може рећи информацију о коначности броја рационалних решења Диофантове једначине у завиности од рода који има крива коју формира та једначина! Претпоставићемо неке услове о тој једначини.

Нека је $C$ глатка, пројективна, апсолутно несводљива крива (замислимо само да немамо могућност неке јасно уочљиве бесконачне фамилије решења у бројном пољу, тј. коначном раширењу поља $\mathbb{Q}$, то представљају ови услови) дефинисана над $\mathbb{Q}$ (криву, тј. једначину коју решавамо дефинишемо са рационалним коефицијентима). Нека је крива $C$ рода $g$ и уведимо ознаку $C(\mathbb{Q})$ за скуп рационалних тачака на $C$.

**Теорема 2.** Нека за глатку криву $C$ важе сви услови набројани изнад.
(1) Ако је $g = 0$, тада је $C(\mathbb{Q}) = \emptyset$ или је $C$ изоморфно над $\mathbb{Q}$ са пројективном правом $\mathbb{P}^1$. Специјално, тај изоморфизам индукује бијекцију $\mathbb{Q} \cup \{\infty\} \to C(\mathbb{Q})$.
(2) Ако је $g = 1$, тада је $C(\mathbb{Q}) = \emptyset$ или постоји тачка $P_0 \in C(\mathbb{Q})$. У овом случају, $(C, P_0)$ се назива назива елиптичка крива над $\mathbb{Q}$ и скуп $C(\mathbb{Q})$ има структуру коначно генерисане комутативне групе у којој је $P_0$ неутрал.
(3) Ако је $g \geq 2$, тада је $C(\mathbb{Q})$ коначан скуп.

Укратко ћемо прокоментарисати сваки од случајева.

**Случај $g = 0$:**

Криве рода 0 се могу афино видети као $f(x, y) = 0$, где је $\deg(f) \leq 2$. Ако је $\deg(f) = 1$, онда је тривијално описати $C(\mathbb{Q})$, пошто се добије линеарна Диофантова једначина. Занимљивији случај је $\deg(f) = 2$.

Постоје криве рода 0 које стварно немају рационалних тачака, на пример $x^2 + y^2 = 3$, што се лако и брзо провери. Овакве криве нам нису интересантне, тако да препоставимо да је $C(\mathbb{Q}) \neq \emptyset$, тј. постоји $P_0 \in C(\mathbb{Q})$.

Може нам пасти на памет једначина из првог примера $x^2 = 2y^2$, само сада у рационалним бројевима. Наравно, она опет има једино решење $(x, y) = (0, 0)$, што се не слаже са претходном теоремом. То је поента услова апсолутне несводљивости, јер се ова једначина раставља у $\mathbb{Q}(\sqrt{2})$ на $(x - \sqrt{2}y)(x + \sqrt{2}y) = 0$. Зато претпостављамо да немамо такву врсту проблема.

Сада провлачењем рационалних линија кроз $P_0$ очекујемо још један пресек са кривом (јер би требало да се права и крива степена 2 секу тачно два пута), а тачка пресека ће имати рационалне координате, по Вијетовим формулама. Тако успостављамо бијекцију између рационалних правих и преосталих рационалних тачака. Отприлике ово је опис како параметризујемо све рационалне тачке на оваквим кривама (примењујемо исти поступак као код описа свих Питагориних тројки).

Такође, за овакве криве важи једна веома моћна теорема, која не важи за криве већег рода.

**Теорема 3.** *(Хасеов принцип)* Нека је $C$ глатка крива рода 0. Тада је $C(\mathbb{Q}) \neq \emptyset$ ако и само ако $C(\mathbb{Q}_p) \neq \emptyset$ и $C(\mathbb{R}) \neq \emptyset$.

Другим речима, довољно је испитати да ли једначина има решења у свим комплетирањима поља $\mathbb{Q}$. О овоме ће још бити речи у трећој глави.

**Случај $g = 1$:**

Опет претпоставимо да имамо бар једну рационалну тачку иако и овде свакако постоје криве које немају рационалних тачака, као на пример $3x^3 + 4y^3 = 5$ (доказ се може наћи у [17] и није лак) и $2y^2 = 1 - 17x^4$. Ови примери су интересантни због тога што за њих не важи Хасеов принцип, тј, у оба случаја постоје решења у било ком од поља $\mathbb{Q}_p$ и $\mathbb{R}$, али не постоје рационална решења. Може се показати да при испуњеним свим траженим условима

до сада, постоји изоморфизам који слика криву $C$ на криву облика $y^2 = x^3 + ax + b$, при чему су $a, b \in \mathbb{Q}$ за које $4a^3 + 27b^2 \neq 0$ (некад морамо да дефинишемо пресликавање користећи коефицијенте из $\overline{\mathbb{Q}}$). Ово је познати облик елиптичких кривих који се назива *(упрошћена) Вајерштрасова једначина*. Случај (2) теореме 2 је *Мордел-Вејлова теорема*, коју је доказао Мордел 1922. године, а Вејл уопштио касније на Абелове варијетете и бројна поља (ако је $A$ Абелов варијетет и $K$ бројно поље, тада је група $A(K)$ свих $K$-рационалних тачака Абеловог варијетета $A$ коначно генерисана), па по обојици носи име. У овом случају знамо структуру групе свих рационалних решења,

$$C(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

при чему $\mathbb{Z}^r$ представља слободни део (подгрупу која се састоји од свих елемената бесконачног реда и неутрала) и $r$ ранг те елиптичке криве, који је по теореми коначан, дакле природан број или нула, а $T$ је торзиона подгрупа (скуп свих елемената коначног реда).

Постоји алгоритам за одређивање торзионе подгрупе елиптичке криве над $\mathbb{Q}$ који даје *Нацел-Латзова теорема*. За елиптичку криву облика $y^2 = x^3 + ax + b$, где су $a, b \in \mathbb{Z}$ Нацел-Латзова теорема каже да тачке коначног реда имају целобројние координате и даје ограничење за $y$ - или је $y = 0$ или $y^2 \mid 4a^3 + 27b^2$. Постоји и *Мазурова теорема* која даје ограничење за редове елемената са коначним редом (и даље посматрамо само елиптичке криве над $\mathbb{Q}$) и тај број може бити између 1 и 10 или 12, као и могућности за облик целе торзионе подгрупе, која ће увек бити једноставна група (највише реда 12).

Главни проблем при тражењу структуре групе коју формирају рационалне тачке на елиптичкој кривој је да се одреди слободни део и до данас није познат алгоритам који даје одговор на ово питање.

Зато се посматра *Тејт-Шафаревич група* придружена тој елиптичкој кривој, која „мери колико је одступање од Хасеовог принципа". У неким случајевима је могуће одредити ову групу, али и даље то није решен проблем у општем случају.

Такође, елиптичкој кривој се додељује њена *L-функција*, која садржи аритметичке информације везане за ту криву. Чувена

*Бирч-Свинертон-Дајер хипотеза* тврди да је ранг $r$ елиптичке криве једнак реду нуле њене $L$-функције у тачки 1.

Ако бисмо знали да је та хипотеза тачна, онда бисмо могли да израчунамо и Тејт-Шафаревич групу елиптичке криве, као и слободни део групе њених рационалних тачака. Међутим, доказивање те хипотезе је један страшно тежак проблем.

За крај, наведимо и још познату *Зигелову теорему* која каже да је број целобројних тачака на глаткој елиптичкој кривој дефинисаној над $\mathbb{Q}$, коначан.

**Случај $g \geq 2$:**

У свом раду где је доказао теорему да је група рационалних тачака на глаткој елиптичкој кривој над $\mathbb{Q}$ коначно генерисана, Мордел је поставио хипотезу да је скуп рационалних тачака на кривама рода 2 и више увек коначан. Математичари су проучавали овај проблем, чак и направили неки резултат уз додатне претпоставке, као, на пример, баш *Шаботи*, а *Герд Фалтингс* је 1983. коначно доказао ову теорему (тј. део (3) из горе наведене теореме). Касније је и *Bojta* дао други доказ ове теореме, коришћењем Диофантових апроксимација.

Овде се добро илуструје важност услова глаткости, ако посматрамо на пример једначину $y^2 = x^{2016}$. Ова крива је рода 1008, али она дефинитивно има бесконачно рационалних решења, јасно се види да фамилија $\{(t, t^{1008}) \mid t \in \mathbb{Q}\}$ представља решења једначине. Проблем је у томе што ова крива није глатка у тачки $(0, 0)$.

Једина разлика између пројективне криве и афине криве је у неколико (коначно) тачака у бесконачности, за које је лако да проверимо да ли су рационалне, па је онда главни део посла да одредимо рационалне тачке афиног дела криве.

То значи да треба да испитамо које су од тачака из $\mathbb{Q} \times \mathbb{Q}$ на кривој. Овај скуп је пребројив, па можемо, у принципу, да излистамо парове рационалних бројева и да проверавамо који од њих су на кривој. Чак можемо и брже, тако што излистамо само рационалне бројеве као кандидате за $x$ и редом да проверавамо постоји ли $y \in \mathbb{Q}$ на кривој за свако конкретно $x$. Пошто знамо да једначина има само коначно много рационалних решења, у неком тренутку би требало да пронађемо сва решења.

Такође, разумно је да очекујемо да су бројиоци и имениоци $x$ и $y$ у „неком нормалном односу" са коефицнијентима једначине (тј. да нису „много већи" од њих). Постоје резултати који иду овим тврдњама у прилог и наводимо их мало касније.

И када нам остане да испитамо коначан број случајева, у већини случајева је то огроман број бројева који треба испитати, тако да је то неизводљиво. Наравно, та рачунања се изводе помоћу рачунара, али ни то није довољно брзо (сложеност проблема је сувише велика).

Стога, понављамо опет, иако их није лако одредити, најтежи део посла је да докажемо да смо нашли сва решења. Као што знамо, не постоји алгоритам за то и зато постоје разни покушаји да се то изведе, а неки од њих су наведени у следећем делу ове главе.

Неко може да се запита да ли је узалудно ово што радимо, јер постоји следећа хипотеза:

0% кривих рода 2 има рационалне тачке.

Логично је да очекујемо да за криве већг рода претходни резултат важи и да се „резултат достиже и брже", што ће објаснити велики *Баргавин* резултат у [7]:

Када $g \to \infty$, густина хиперелиптичких кривих које немају рационалне тачке тежи 100%, тачније доња граница за густину се изражава са $1 - o(2^{-g})$, одакле је та конвергенција јако брза.

Напоменимо да се под појмом густине интуивно мисли на количник броја кривих које имају рационалне тачке са укупним бројем испитаних кривих. Наравно, овако дефинисана густина има облик бесконачно подељено са бесконачно, зато пуштамо лимес када $N$ тежи бесконачно, а криве које испитујемо су оне које имају коефицијенте по апсолутној вредности мање од $N$. За доњу или горњу густину, пуштамо доњи, односно горњи лимес.

Интересантно је одредити и колики проценат кривих одступа од Хасеовог принципа. На пример, за род 2, проценат кривих које имају решења у свим $\mathbb{Q}_p$ и $\mathbb{R}$ је око $84\% - 85\%$, што је резултат у [40]. То је и проценат кривих за које не важи Хасеов принцип ако се испостави да је хипотеза да 0% кривих рода 2 има рационалне тачке тачна. И то се види као последица у Баргавином раду:

Када $g \to \infty$, густина хиперелиптичких кривих за које не

важи Хасеов принцип тежи 100%.

Наводимо да (очекивано), Зигелова теорема важи и у овом, општем случају, а доказ можемо наћи у [28]:

Нека је $F \in \mathbb{Z}[x, y]$ такав да решења $F(x, y) = 0$ не могу да буду рационално параметризована (тј. не можемо наћи „јасну" бесконачну фамилију решења). Тада $F(x, y) = 0$ има само коначно много решења у целим бројевима.

Са друге стране, постоје и криве са „доста" рационалних тачака. Можемо да уочимо криву рода $g$

$$y^2 = x(x-1)(x-2)...(x-2g)(x-2g-1).$$

Она има бар $2g+2$ очигледних рационалних тачака: $(0,0)$, $(1,0)$, $(2,0)$, ... , $(2g+1,0)$. Када $g \to \infty$, тада и број рационалних тачака на овим кривама тежи бексоначно. Наравно, ово нема баш смисла, занимљивије је да за фиксиран род криве гледамо колико се максимално може наћи тачака на њој. Постоје неке варијанте *Бомбијери-Лангове хипотезе* које би дале горњу границу. Зато је и једно од отворених питања одредити криву унапред фиксираног рода са што већим бројем рационалних тачака. Рекорд из 2014. за криву рода 2 је крива која има бар 642 рационалне тачке и која има за коефицијенте бројеве који имају око 10 цифара. Једначина те криве је

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 +$$

$$+2396040466x^3 + 567207969x^2 - 985905640x + 247747600.$$

Сада наводимо неке најважије резултате у области Диофантових апроксимација.

Крећемо са феноменалном теоремом *Клауса Рота*, који је направио драстичан напредак у Диофантовим апроксимацијама:
За сваки алгебарски ирационални број $\alpha$ и за било које $\varepsilon > 0$, постоји константа $c > 0$ (која зависи од $\alpha$ и $\varepsilon$) таква да за све сведене разломке $\frac{p}{q}$ важи

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{2+\varepsilon}}.$$

Ова теорема је значајна из више разлога. Прво, најбољи степен $q$ до тада је био $O(\sqrt{d})$, где је $d$ степен алгебарског броја $\alpha$, а након те теореме, спуштена је граница до броја који не зависи више од $\alpha$. Друго, боље од овога и не може, јер као што смо видели у одељку о Диофантовим апроксимацијама, постоји бесконачно сведених разломака $\frac{p}{q}$ за које

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

Проблем у Ротовој теореми је тај што се та константа $c$ не може израчунати. Ипак, и поред тог недостатка, Ротова теорема има многе примене, а сада наводимо једну од њих.

Једначина $x^n - ay^n = k$, где су $k \in \mathbb{Z}$, $a, n \in \mathbb{N}$, $n \geq 3$ непаран, илуструје једну примену Ротове теореме на Диофантове једначине. Доказаћемо да је број целобројних решења ове једначине коначан. Случај када је $a$ потпун $n$-ти степен је лакши и доказ следи из чињенице да је тада $ay^n$ потпун $n$-ти степен и $\lim_{x\to\infty}(x+1)^n - x^n = +\infty$. Када $a$ није потпун степен, онда леву страну једначине растављамо на следећи начин

$$(x - \sqrt[n]{a}y)(x - \xi_n\sqrt[n]{a}y)...(x - \xi_n^{n-1}\sqrt[n]{a}y) = k,$$

где је $\xi_n$ $n$-ти примитивни корен из 1. Дељењем са $y^n$ имамо

$$\left(\frac{x}{y} - \sqrt[n]{a}\right)\left(\frac{x}{y} - \xi_n\sqrt[n]{a}\right)...\left(\frac{x}{y} - \xi_n^{n-1}\sqrt[n]{a}\right) = \frac{k}{y^n}.$$

Приметимо да за бројеве $\frac{x}{y} - \xi_n^j\sqrt[n]{a}$, $1 \leq j \leq n-1$, важи да су разлика рационалног броја и комплексног броја, који није реалан, тако да је овај израз ограничен одоздо независно од разломка $\frac{x}{y}$ (нпр. апслотуном вредношћу имагинарног дела тог комплексног броја). Одавде добијамо да је

$$\left|\frac{x}{y} - \sqrt[n]{a}\right| \leq \frac{C}{y^n},$$

за неку константу $C$ која не зависи од $x$ и $y$. Један од начина да прочитамо Ротову теорему јесте да постоји само коначно много

сведених разломака за које ово важи, јер $n \geq 3$. Међутим сваки сведени разломак може дати највише једно решење једначине, тако да је број решења наведене једначине коначан. Ову теорему можемо наћи у [1] или на пример у [28] или [51].

За крај овог дела, наводимо чувени допринос математичара *Алана Бејкера* у Диофантовим апроксимацијама. Бејкер је написао књигу у којој се налазе његови резултати - [6]. Наводимо једну од најзначајнијих теорема из књиге [6].

Нека су $\alpha_1$, $\alpha_2$, ... , $\alpha_n$ алгебарски бројеви. Тада постоји константа $c$ (која зависи од ових алгебарских бројева), која се може ефективно израчунати, тако да за све целе бројеве $b_1$, $b_2$, ... , $b_n$ и $B$ који је већи од максимумума $b_i$-ова важи

$$\alpha_1^{b_1}\alpha_2^{b_2}...\alpha_n^{b_n} = 1$$

или

$$|\alpha_1^{b_1}\alpha_2^{b_2}...\alpha_n^{b_n} - 1| \geq B^{-c}.$$

Последица Бејкерових резултата је и Зигелова теорема о коначности броја целобројних решења једначина, када једначина формира криву рода бар 1 над $\mathbb{Q}$. То није једина предност, могућност да се ефективно израчуна константа своди решавање једначине на неки коначан проблем.

На пример, за једначину

$$\binom{y}{2} = \binom{x}{5},$$

применом Бејкерових резултата можемо ограничити

$$|x| < 10^{10^{10^{10^{600}}}}.$$

Сада је стварно остало испитати „само" толико коначно случајева, међутим и то је превише! Неке модерне методе су смањиле то ограничење, прво на $10^{10^{600}}$, а онда и на $10^{1800}$, што је и даље огроман број и треба нам читава вечност да проверимо све те случајеве.

## 1.3 Модерне методе за решавање Диофантових једначина

Овде ћемо само укратко навести технике које се данас користе за решавање Диофантових једначина.

(1) **Локалне методе**

Као што смо видели, ако је $C(\mathbb{Q}_p) = \emptyset$ или $C(\mathbb{R}) = \emptyset$, тада је и $C(\mathbb{Q}) = \emptyset$. Наравно, ово није често случај, али може да помогне и зато то прво проверавамо. Уз помоћ *Хасе-Вејлове процене* испоставља се да овде треба да проверимо само коначан број случајева, тј. $\mathbb{R}$ и само за још коначно простих бројева $p$ њихова $p$-адска поља. О овоме ће бити речи у трећој глави, те сада само наводимо два примера:
(1а) $C : y^2 = -x^6 - x^2 - 2016$ - тада је јасно $C(\mathbb{R}) = \emptyset$, па и $C(\mathbb{Q}) = \emptyset$.
(1б) $C : y^2 = x^{11} - x - 1$ (или мање тривијалан пример $C : y^2 = -x^6 - 3x^5 + 4x^4 + 2x^3 + 4x^2 - 3x - 1$) - тада се провером утврђује да је $C(\mathbb{F}_{11}) = \emptyset$, одакле је $C(\mathbb{Q}_{11}) = \emptyset$, па и $C(\mathbb{Q}) = \emptyset$.

Ово се све налази у [59].

(2) **Спуст**

Овај метод се на енглеском језику зове *descent* и мало га је тешко превести поготово што се употребљава у различитим контекстима. Овде ћемо објаснити шта то значи спуст. Идеја је да проблем решавања неке „компликованије" једначине сведемо на проблем решавања неке „једноставније" једначине. Наводимо један једноставан пример.

Решавамо $y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2)$ у скупу рационалних бројева. Рачунањем резултанте полинома $-x^2 - x + 1$ и $x^4 + x^3 + x^2 + x + 2$ или елементарном проверимо долазимо до закључка да „највећи заједнички делилац" (ово је под наводницима јер су у питању рационални бројеви, али гледамо само бесквадратне делове, па можемо тако да оставимо) ће да дели 19, одакле задатак сводимо на два истовремена проблема

$$-x^2 - x + 1 = da^2,$$

$$x^4 + x^3 + x^2 + x + 2 = db^2,$$

за неке $a, b \in \mathbb{Q}$ и $d$ цео број који дели 19.

Одмах видимо да мора бити $d > 0$, иначе друга једначина нема решења. Дакле $d = 1$ или је $d = 19$. Сада посматрањем друге једначине у $\mathbb{F}_3$ следи $x = 1$ у пољу $\mathbb{F}_3$, али тада добијамо контрадикцију у $\mathbb{F}_3$ у првој једначини. Одавде је $C(\mathbb{Q}_3) = \emptyset$, што повлачи $C(\mathbb{Q}) = \emptyset$.

Ова тактика нам већи проблем своди на мањи где онда лакше извлачимо закључке помоћу којих решавамо једначину. Такође, као и у (1), текст је преузет из [59].

(3) **Количничке методе (или одлазак-надоле)**

И ове методе је изузетно тешко превести са енглеског језика, јер их неко назива *quotients*, а неко *going-down*. Идеја је да посматрамо неконстантне морфизме $f : C \longrightarrow D$ над $\mathbb{Q}$ из $C$ на неку другу криву $D$. Тада је $f(C(\mathbb{Q})) \subset D(\mathbb{Q})$ и ако знамо $D(\mathbb{Q})$ које је и коначно, можемо одредити и $C(\mathbb{Q})$. Наводимо скице неколико примера:
(3а) Посматрајмо једначину $C : y^2 = 13x^6 + 1$. Она се морфизмом $f : (x, y) \mapsto (\frac{-1}{x^2}, \frac{y}{x^3})$ слика на криву $D : y^2 = x^3 + 13$. Може се показати да је $D(\mathbb{Q}) = \{\infty\}$, одакле је $C(\mathbb{Q}) \subset f^{-1}(\{\infty\})$, па закључујемо да је $C(\mathbb{Q}) = \emptyset$.
(3б) Нека је $C : y^2 = 11x^6 - 19$. Може се брзо проверити да је $C$ локално решива, одакле не добијамо никакав закључак. Даље, покушавамо са морфизмима $f : C \longrightarrow D$, где $f(x, y) = (11x^2, 11y)$ и $D : y^2 = x^3 - 11^2 \cdot 19$ и $g : C \longrightarrow E$, где $g(x, y) = (\frac{-19}{x^2}, \frac{19y}{x^3})$ и $E : y^2 = x^3 + 11 \cdot 19^2$. Имамо два морфизма из наше криве на две елиптичке криве, за које можемо доказати да је $D(\mathbb{Q}) \cong E(\mathbb{Q}) \cong \mathbb{Z}$, при чему можемо експлицитно да израчунамо генераторе ових кривих. Онда из $C(\mathbb{Q}) \subset f^{-1}(D(\mathbb{Q}))$ и $C(\mathbb{Q}) \subset g^{-1}(E(\mathbb{Q}))$ и чињенице да се инверзне слике не поклапају по модулу 7, следи да мора бити $C(\mathbb{Q}) = \emptyset$.
(3в) Можемо доказати и да крива $C : y^2 = (x^2 + x + 1)(x^4 + 7)$ нема рационалних решења, применом ове методе заједно са спустом.
(3г) Следећа крива нам је већ позната из досадашњег текста $C : x^4 - 17 = 2y^2$. За њу знамо да је решива локално, а у доказу да нема рационалних решења, употребљавамо исте две методе као и у претходном примеру, с тим што је овај пример занимљивији, јер радимо спуст у прстену $\mathbb{Z}\left[\frac{1+\sqrt{17}}{2}\right]$, што је прстен са јединственом

факторизацијом.

Ови примери се налазе у[45].

(4) **Метод Шаботи-Колемана**

Овај метод је главни предмет мастер рада, тако да ће о њему бити речи током целог рада.

(5) **Мордел-Вејлово решето**

Овај метод представља неку варијанту уопштења Шаботи-Колемановог метода и укратко ће бити изложен у једном примеру у седмој глави. За разлику од Шаботи-Колемановог метода где користимо само један прост број $p$, овде их користимо далеко више и зато је скоро немогуће применити овај метод без рачунара.

Користе се исти објекти као и код Шаботи-Колемановог метода, а то је посматрање инјективног пресликавања $i : C \longrightarrow J(C)$, дефинисаног са $i(P) = [P - P_0]$, за било коју тачку $P_0$ са криве, а $J(C)$ је Јакобијан криве $C$ (над одговарајућим пољем). Такође, метод се исто бави ограничавањем броја рационалних тачака које се по неком модулу редукују на исте оне тачке као и већ познате тачке криве. Идеја је доказати да се та граница поклапа са бројем већ одређених тачака.

Међутим, граница се добија на нешто другачији начин у односу на Шаботи-Колеманов метод, па зато овај метод није директно његово уопштење, али предност је да могу да се комбинују заједно и да се добијају веома корисне процене укупног броја рационалних решења, посебно у случају када је род криве $g = 2$, а ранг њеног Јакобијана $r = 1$.

За Мордел-Вејлово решето тражимо „мали" подскуп $W \subset J(\mathbb{Q})$ и подгрупу $L \leq J(\mathbb{Q})$ „великог" индекса, такве да

$$i(C(\mathbb{Q})) \subset \bigcup_{D \in W} (D + L) = W + L.$$

Крећемо од $L = J(\mathbb{Q})$ и $W = \{0\}$ и индуктивно конструишемо низ подгрупа коначног индекса $L_i \leq J(\mathbb{Q})$ и коначних подскупова $W_i \subset$

$J(\mathbb{Q})$ таквих да

$$L_0 \geq L_1 \geq L_2 \geq ..., \qquad i(C(\mathbb{Q})) \subset W_i + L_i.$$

То радимо коришћењем комутативног дијаграма

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{i} & W_i + L_i \subset J(\mathbb{Q}) \\ \downarrow{\scriptstyle red} & & \downarrow{\scriptstyle red} \\ \overline{C}(\mathbb{F}_p) & \xrightarrow{\quad i \quad} & \overline{J}(\mathbb{F}_p) \end{array}$$

Тада можемо ставити да је

$$L_{i+1} = \ker(L_i \longrightarrow J(\mathbb{Q}) \longrightarrow J(\mathbb{F}_p)) \leq L_i.$$

Уочимо скуп

$$W'_{i+1} = W_i + (L_i/L_{i+1}),$$

при чему у овом количнику мислимо на представнике косета. Тада ће бити $i(C(\mathbb{Q})) \subset W'_{i+1} + L_{i+1}$, па можемо показати да је

$$W_{i+1} = \{w \in W'_{i+1} \mid red(W) \in i(C(\mathbb{F}_p))\}$$

скуп са траженим својством. Шта нам је потребно да бисмо успешно применили овај метод?

Прво, потребно нам је да $[L_i : L_{i+1}]$ буде што мање, како бисмо могли без неких нерешивих проблема да одредимо скуп $W'_{i+1}$, који није пуно већи од $W_i$, одакле би лако требало да добијемо $W_{i+1}$. Вероватно ћемо више пута да рачунамо групе $L_i$ и скупове $W_i$, јер, као што смо најавили на почетку, циљ нам је да дођемо до подгрупе Јакобијана што већег индекса.

Друго, битно је да бројеви $N_p = \#\overline{J}(\mathbb{F}_p)$, које добијамо за различите изборе простих бројева $p$ имају што више заједничких фактора. Тада информације које сакупимо могу да донесу међусобну контрадикцију. На пример, ако за $p = 5$, знамо да је $N_5 = 12$ и да ред слике рационалне тачке у $\overline{J}(\mathbb{F}_5)$ може бити 2 и 4, док за $p = 7$ буде $N_7 = 16$ и да ред слике рационалне тачке у $\overline{J}(\mathbb{F}_7)$ може бити 8

и 11, отпадају могућности у којима је 2 ред слике у $\overline{J}(\mathbb{F}_5)$ и 11 у $\overline{J}(\mathbb{F}_7)$. Оваквим поступком, узимајући већи број простих бројева, одбацујемо многе могућности. Илустрација примене овог метода (и начина размишљања који је овде наведен) је пример решавања једначине

$$y^2 = 2x^6 - 3x^2 - 2x + 1$$

у седмој глави. Ако применимо метод успешно, обично ћемо добити да је $W_k = i(A)$, за неки велики број $k$, док је $A$ скуп познатих рационалних тачака.

Идеје и технике које се користе када се решавају једначине уз помоћ Мордел-Вејловог решета се могу наћи у радовима [12] и [13] у којима се испитују криве облика

$$y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

при чему су $f_0$, $f_1$, ... , $f_6$ мали цели бројеви, тј. за све њих важи $|f_i| \leq 3$.

(6) **Одлазак-нагоре**

Ово је буквални превод са енглеског језика од назива *going-up*, идеја је обрнута од идеје (3), тако да овде посматрамо нерамификоване морфизме $f : D \longrightarrow C$ над $\mathbb{Q}$ и у процесу решавања користимо својство да постоји израчунљиво коначно раширење поља $K/\mathbb{Q}$ у којем важи $f^{-1}(C(\mathbb{Q})) \subset D(K)$. Даље се решавање своди на одређивање $D(K)$. Познато је да, ако је $C$ крива рода бар 2, таква мора да буде и $D$, одакле ће $D(K)$ бити коначан скуп. За даље информације видети [38].

(7) **Демјаненко-Мањинов метод**

Овај метод се примењује ретко, јер веома често криве не испуњавају услове за примену. Међутим када се примењује, даје ефикасну оцену за бројиоце и имениоце рационалних решења једначине. Идеја је да се уочи неки Абелов варијетет $A$, чија структура групе индукује и структуру групе на скупу морфизама $X \longrightarrow A$ над $\mathbb{Q}$. Абелов варијетет тражимо тако да ранг ове групе морфизама

буде већи од ранга $A(\mathbb{Q})$, тј. да можемо да нађемо више независних морфизама $X \longrightarrow A$ него независних тачака у $A(\mathbb{Q})$. Када је испуњен овај услов, овај метод даје јако добре резултате, али јако тешко се испуњава. Више информација се може наћи у [38] и [58].

(8) **Елиптички Шаботи**

Елиптички Шаботи је модификација Шаботијевог метода таква да једначини коју решавамо придружујемо одређене елиптичке криве. Предност у односу на стандардни Шаботијев метод је то што је лакше спровести рачун на елиптичким кривама него на Јакобијанима. Међутим, те елиптичке криве које посматрамо неће бити дефинисане над $\mathbb{Q}$, већ над бројним пољима, што повећава сложеност рачуна. Наводимо литературу даље изучавање овог метода - [38] и [31].

(9) **Модуларност**

Модуларне форме су јако моћан објекат са великим резултатима у теорији бројева. Једна од примена модуларних форми је и на Диофантове једначине и то ни мање ни више - на доказ Велике Фермаове Теореме. Наравно, математика која је у позадини тог доказа је сувише озбиљна за овај мастер рад и овде наводимо само скицу доказа. Пре доказа прескачемо дефиниције основних појмова за модуларне форме, као што је *тежина модуларне форме* или *Хекеов оператор*. За наше потребе, *нова форма* (на енглеском *newform*) је модуларна форма која је сопствени вектор за све Хекеове операторе у исто време. Као и сваки сопствени вектор, може бити нормализована, тј. степени ред ће почети са $q$ (уместо $cq$). Посматраћемо модуларне форме тежине 2. Такође, битан нам је и ниво нове форме, који ћемо само описно дефинисати, то је $N$, ако је $N$ најмањи природан број, такав да је дејство те нове форме инваријантно у односу на дејство конгруентне подгрупе $\Gamma_0(N)$ (матрице из $\mathrm{SL}(2,\mathbb{Z})$, такве да $N$ дели доњи леви елемент) на горњу полураван $\Im z > 0$. Постоји само коначно много нових форми фиксираног нивоа $N$, заправо има и једна важна теорема везана за то, која

каже да **не постоје нове форме нивоа**

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60.$$

Дакле, нова форма је $q$-развој ($q = e^{2i\pi z}$)

$$f = q + \sum_{n=2}^{\infty} c_n q^n,$$

при чему се испоставља да су коефицијенти $c_n$ реални и алгебарски над $\mathbb{Q}$. Штавише, сви су елементи једног тотално реалног бројног поља $K$. Тотално реално бројно поље је бројно поље $K$ такво да за свако његово утапање у $i : K \longrightarrow \mathbb{C}$ важи да је $i(K) \subset \mathbb{R}$. За сва утапања $\sigma : K \longrightarrow \mathbb{R}$ важи $|\sigma(c_l)| \leq 2\sqrt{l}$, за просте $l$. Кажемо да је нова форма *рационална* ако су јој сви коефицијенти рационални. Подсетимо се (или можемо видети у [51]) да је *кондуктор* елиптичке криве (над $\mathbb{Q}$) број који карактерише каква је редукција елиптичке криве по простим модулима. Следећа теорема је веома важна и изузетно тешка. Та теорема је последњи корак у доказу Велике Фермаове Теореме. Главни део ове теореме је доказао Ендру Вајлс, математичар који је и завршио доказ Велике Фермаове Теореме.

**Теорема модуларности.** Свакој рационалној новој форми $f$ нивоа $N$ придружимо елиптичку криву $E_f$ кондуктора $N$, такву да за све просте бројеве $l \nmid N$ важи $c_l = a_l(E_f)$, где је $a_l(E_f) = l+1-\#E_f(\mathbb{F}_l)$, а $c_l$ $l$-ти коефицијент у развоју модуларне форме. За сваки природан број $N$, придруживање $f \mapsto E_f$ је бијекција између рационалних нових форми нивоа $N$ и класа изогенија елиптичких кривих кондуктора $N$.

Нека је $p$ прост број, $f = q + \sum_{n=2}^{\infty} c_n q^n$, нова форма нивоа $N'$, $K = \mathbb{Q}(c_2, c_3, ...)$ и $\mathcal{O}_K$ прстен целих бројног поља $K$. Нека је $E$ елиптичка крива кондуктора $N$. Кажемо да елиптичка крива $E$ *настаје модуло $p$ из нове форме* ако постоји неки прост идеал $\mathfrak{P} \mid p$ у $\mathcal{O}_K$, такав да за све просте бројеве $l$ важи:
(1) Ако $l \nmid pNN'$, онда $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$;
(2) Ако $l \nmid pN'$ и $l \,||\, N$, тада $l + 1 \equiv \pm c_l \pmod{\mathfrak{P}}$.

Ово пишемо $E \sim_p f$. Ако је $f$ рационална нова форма, онда она одговара тачно једној елиптичкој кривој $E'$ и то пишемо $E \sim_p E'$ и кажемо да $E$ *настаје модуло* $p$ *од* $E'$.

Нека су кондуктори за $E$ и $E'$, редом $N$ и $N'$ и претпоставимо $E \sim_p E'$. Тада, за све просте бројеве $l$ важи:
(1) Ако $l \nmid NN'$, онда $a_l(E) \equiv a_l(E') \pmod{p}$;
(2) Ако $l \nmid N'$ и $l \mid\mid N$, онда $l + 1 \equiv \pm a_l(E') \pmod{p}$.

Треба нам још једна теорема. У оквиру припреме за ту теорему, нека је $E$ једна елиптичка крива над $\mathbb{Q}$, која је у минималном моделу, са минималном дискриминантом $\Delta = \Delta_{min}$, $N$ кондуктор $E$ и $p$ прост број. Дефинишимо број $N_p$ на следећи начин

$$N_p = \frac{N}{\prod\limits_{q||N, p|\mathrm{ord}_q(\Delta)} q}.$$

Наводимо поједностављен случај теореме.
**Рибетова теорема о смањењу ниова.** Нека је $p \geq 5$ прост број. Нека је $E$ елиптичка крива над $\mathbb{Q}$, која нема $p$-изогенија. Тада постоји нова форма $f$, нивоа $N_p$, за коју $E \sim_p f$.

Напоменимо да теорема не гарантује да ће нова форма бити рационална. Увиђамо да нам треба и нека теорема која нам обезбеђује када елиптичка крива нема $p$-изогеније. Наводимо три теореме.
**Теорема.** (Мазур 1) Нека је $E/\mathbb{Q}$ елиптичка крива и $p$ прост број који задовољава бар један од услова:
(1) $p > 163$;
(2) $p \geq 5$ и $\#E(\mathbb{Q})[2] = 4$ и кондуктор криве $E$ је бесквадратан.

Тада $E$ нема $p$-изогенија.
**Теорема.** (Мазур 2) Нека је $E/\mathbb{Q}$ елиптичка крива и $p$ прост број који задовољава бар један од услова:
(1) $p \geq 17$ и $j(E) \notin \mathbb{Z}[\frac{1}{2}]$;
(2) $p \geq 11$ и E је полустабилна елиптичка крива;
(3) $p \geq 5$ и $\#E(\mathbb{Q})[2] = 4$ и E је полустабилна елиптичка крива.

Тада $E$ нема $p$-изогенија.
**Теорема** Нека је $E/\mathbb{Q}$ елиптичка крива са кондуктором $N$. Ако је $\mathrm{ord}_2 N \in \{3, 5, 7\}$, тада $E$ нема изогенија непарног степена.

Коначно долазимо до примене модуларних форми на Диофантове једначине.

**Велика Фермаова Теорема** Једначина $x^n + y^n = z^n$, где је $n \in \mathbb{N}$, $n > 2$ има само тривијална целобројна решења.

**Доказ (прецизније скица доказа).** Видели смо већ да једначина нема решења за $n = 3$ и $n = 4$. Довољно је да докажемо да ова једначина нема нетривијалних решења за просте бројеве $p \geq 5$. Претпоставимо супротно. Можемо да претпоставимо $a^p + b^p + c^p = 0$, $a, b, c \in \mathbb{Z}$ и $abc \neq 0$. Без губљења општости, можемо наместити $(a, b, c) = 1$, $2 \mid b$ и $a^p \equiv -1 \pmod 4$. Овом решењу придружујемо одговарајућу *Фрајову криву*

$$E : y^2 = x(x - a^p)(x + b^p).$$

Ово је елиптичка крива чија је дискриминанта

$$\Delta = 16a^{2p}b^{2p}(a^p + b^p)^2 = 16a^{2p}b^{2p}c^{2p}.$$

Овај модел није минималан, али можемо применити Тејтов алгоритам да бисмо добили $\Delta_{min} = \dfrac{a^{2p}b^{2p}c^{2p}}{2^8}$ и кондуктор те елиптичке криве $N = \prod_{l \mid abc} l$, при чему производ иде по простим бројевима $l$ који деле прозивод $abc$. Закључујемо да је $N$ бесквадратан, претпоставку $p \geq 5$ имамо, а ова елиптичка крива има пуну рационалну торзију реда 2, поред бесконачне тачке, то су тачке $(0, 0)$, $(a^p, 0)$, $(-b^p, 0)$ - дакле укупно 4. По Мазуровој теореми 1, ова елиптичка крива нема $p$-изогенија. Сада је испуњен услов Рибетове теореме. Према томе, постоји нова форма $f$, нивоа $N_p$, таква да $E \sim_p f$. Треба да израчунамо број $N_p$. Како је $N$ бесквадратан, то је $q \mid N$ еквивалентно са $q \mid\mid N$. Такође, пошто $N$ има просте факторе од $a$, $b$ и $c$, а $\Delta_{min}$ има исте просте факторе, при чему сваки прост број, сем 2 (због дељења са $2^8$), дели $\Delta_{min}$ са степеном дељивим са $p$, у дефиницији броја $N_p$, у разломку ће се пократити сви прости бројеви у производу, сем броја 2, који ће се наћи у бројиоцу, али не и у имениоцу, па је $N_p = 2$. Дакле, Рибетова теорема каже да је нова форма $f$ нивоа 2, међутим теорема коју смо навели каже

да не постоји нова форма нивоа 2. КОНТРАДИКЦИЈА!

Овај текст прати литературу у [47], [35].

Уз помоћ модуларних форми се могу решити и још неке друге једначине, на пример $2^x = 3^y + 5^z$ у скупу природних бројева или $x^{2p} + y^{2p} = z^5$, за целе, узајамно просте бројеве $x$, $y$ и $z$ и $p \geq 7$ прост број.

## 1.4 Шаботијев и Колеманов метод укратко и структура овог мастер рада

Можда и највећи резултат у историји проучавања Диофантових једначина јесте Фалтингсова теорема, која класификује број решења у зависности од рода криве која је дефинисана једначином коју решавамо. Међутим, доказ теореме не даје поступак како се може решити једначина! Иако је познато да у великом броју случајева Диофантова једначина има само коначно много решења и даље не знамо универзални алгоритам који би је решио. Зато је корисно ограничити број решења.

Пре него што је Фалтингс доказао своју чувену теорему, Шаботи је доказао коначност броја рационалних тачака на „лепој" кривој рода бар 2, али уз неке услове. Као што смо видели у теореми 2 (3), Фалтингсова теорема нема услове (сем да крива буде „лепа"), одакле је то јачи резултат после којег делује да Шаботијева теорема губи смисао. Ипак, касније је Роберт Колеман нашао начин како да употреби Шаботијев метод тако да ограничи број решења Диофантове једначине (уз неке услове) одозго, што је био недостатак Шаботијеве теореме, која (уз услове) тврди да је број рационалних тачака на кривој (крива је дефинисана Диофантовом једначином коју решавамо) коначан, без процене.

Када примењујемо Шаботи-Колеманов метод, жеља нам је да нађемо довољно јако горње ограничење броја рационалних тачака које би се поклопило са бројем већ нађених рационалних тачака. Тада би поступак решавања те једначине био готов.

Очекивано, ни овај метод није довољно добар да покрије задовољавајући број случајева и зато се и данас проучава, одакле

постоје нека побољшања те теореме, и комбинује са неким другим методима, као што је, на пример, Мордел-Вејлово решето, чиме могу да се добију боље горње границе.

Овај метод захтева познавање алгебарских кривих и њихових својстава, чему је посвећена друга глава, $p$-адских бројева и $p$-адске анализе, што се обрађује у трећој глави, Јакобијана криве, који је описан у четвртој глави и Колеманове интеграције, која је кратко представљена у петој глави. Касније се у шестој глави налазе главне теореме са доказима, док се у седмој глави налазе примери примене Шаботи-Колемановог метода на решавање Диофантових једначина.

Књиге (тј. њихово пажљиво читање) [28], [8] и [30] могу много помоћи у процесу стицања довољног знања математичког апарата који је потребан да би се кренуло у озбиљно истраживање Диофантових проблема.

За крај, желео бих да истакнем велику захвалност ментору и мом професору теорије бројева, др Горану Ђанковићу, на предлогу теме, знању теорије бројева које ме је научио, могућностима у које ме је упутио, на многобројим саветима и исправкама, као и на помоћи око многих техничких ствари које су пратиле израду овог мастер рада.

Такође, желео бих да искажем и захвалност професорима, чија је област истраживања уско везана за Диофантове проблеме, које сам упознао на конференцијама и школама посвећеним овој области.

I would like to express my great appreciation to Professor Jennifer Balakrishnan, Professor Marc Hindry, Professor Samir Siksek, Professor Michael Stoll, and my older colleagues PhD Laura Capuano and PhD Francesco Veneziano for helping me in writting this master thesis by discussion with me about the topic and by recommendation of references for Diophantine Equations.

# 2 Алгебарске криве

## 2.1 Уводно о алгебарским кривама

**Препоручена литература:** За леп и лаган увод уз доста примера и задатака [42], [22], [20], док за озбиљније проучавање је енциклопедија [27], а за оне које занима аритметичка страна, брз преглед тврђења је у [51] (која за доказе усмерава на [27]), а преглед сличан томе се и овде налази. За поједине делове, може бити добра литература и [21], јер има неколико урађених примера, од којих су неки и овде преузети. У овом делу се налазе тврђења без доказа, само са коментарима.

Појам криве се везује за криву линију на папиру или на табли, односно у равни. То је једна од природних интуиција које човек има, али да би се криве математички проучавале, потребно је да се тај појам прецизно дефинише. За почетак ћемо да видимо како могу да се дефинишу афина и пројективна крива, уз неколико примера. Пошто желимо да опишемо алгебарску криву, очекујемо да нам је потребна нека једначина, коју ћемо да посматрамо над пољем $K$.

*Афина алгебарска равanska крива* је скуп тачака $(a_1, a_2)$ у афином простору $\mathbb{A}^2(K)$ за које је $F(a_1, a_2) = 0$, за неки ненула полином $F(x, y) \in K[x, y]$. Одмах примећујемо да се скуп тачака не разликује, ако се посматрају полиноми који се разликују (множењем) до на константу или ако полином $F$ има или нема вишеструке факторе у факторизацији. Ипак, константа нам не мења ништа битно, те на њу нећемо обраћати пажњу, док ћемо видети касније да је корисно да допустимо вишеструке факторе.

Требало би да до сада знамо неке основне између кривих разлике када криве дефинишемо полиномима различитих степена, редом 1, 2, 3, 4, степеном већим од 4, те криве се називају другачије: *права, коника (круг, елипса, хипербола, парабола), кубика (елиптичка крива), квартика, хиперелиптичка крива...* Видећемо касније какву битну разлику могу да поседују криве дефинисане полиномима различитог степена.

На сличан начин можемо да уведемо и *алгебарску пројективну ранваску криву* као скуп тачака $[a_0, a_1, a_2] \in \mathbb{P}^2(K)$ пројективног прос-

тора за које је $F(a_0, a_1, a_2) = 0$, за неки хомоген полином $F \in K[x, y, z]$. Као и код афиних кривих, константа није важна, а дозвољавамо вишеструке факторе полинома $F$. Разлика између афиних и пројективних кривих је „само" у тачкама у бесконачности, али те тачке исправљају многе аномалије које могу да се догоде.

Најпознатије тврђење које ово објашњава је **Безуова теорема**: *Нека су* $C_1 : F = 0$ *и* $C_2 : G = 0$ *пројективне криве које немају заједничке компоненте (тј. F и G немају заједничке компоненте). Тада се оне секу (рачунајући вишеструкости) у тачно* $\deg F \cdot \deg G$ *тачака!* Јасно је да ово не мора да важи у афином простору. Да бисмо радили у довољној општости, задржаћемо се у пројективном простору и да се не ограничавамо на раван, даћемо општу дефиницију алгебарске криве. Пошто нема довољно времена и простора, можемо само укратко да се подсетимо неких уводних појмова у алгебарској геометрији, на неформалан начин.

*Алгебарски скупови* су скупови тачака нула одређених полинома. Алгебарски скуп је *несводљив* ако се не може написати као унија два строго мања алгебарска скупа. *Афини варијетет* је несводљиви алгебарски скуп. Испоставља се да се скуп полинома може заменити идеалом генерисаним тим скупом, тако да алгебарске скупове видимо као нуле полинома који чине идеал у прстену полинома. Даље, алгебарски скуп је несводљив ако и само ако је идеал од ког настаје прост у прстену полинома. Из претходног закључујемо да је афини варијетет и алгебарски скуп нула простог идеала у прстену полинома.

Пошто афини простор не покрива нашу интуицију, користимо и пројективни простор, где радимо са хомогеним полиномима. Тада *пројективни варијетет* можемо видети као скуп нула полинома хомогеног идеала (генерисаног хомогеним полиномима) који је прост у одговарајућем прстену полинома.

Сваком варијетету $V$ који је скуп нула полинома идеала $I$ придружујемо *координатни прстен функција* са $K[V] = K[X]/I$, где $K[X]$ представља прстен полинома простора у ком живимо (није нужно само по једној променљивој). Мотивација за ово је да су сада све функције овог прстена заиста различите на варијетету. Пошто је $I$ прост идеал, прстен функција је домен целих, па се

од њега може направити количничко поље - $K(V)$, *функцијско поље варијетета* $V$. Елементе поља $K(V)$ видимо као рационална пресликавања из $V$ у $K$, тј. као количнике $\frac{F}{G}$, где су $F, G \in K[X]$ (ако се ради о пројективном простору, онда су $F$ и $G$ хомогени полиноми истог степена).

Наравно, овакво пресликавање не мора бити дефинисано у свакој тачки $P \in V$, може се десити да буде $G(P) = 0$. Некад је то могуће отклонити (ту користимо индентификацију полинома чија је разлика у $I$), а некад није. Ако је могуће да дефинишемо пресликавање у тачки $P \in V$, тада се пресликавање *регуларно* (или *дефинисано*) у тачки $P$. Ако је пресликавање дефинисано у свакој тачки $P$, онда кажемо да је пресликавање *регуларно*.

У координатном прстену функција уочавамо идеал

$$M_P = \{F \in K[V] \mid F(P) = 0\},$$

овај идеал је максимални у $K[V]$. Такође, у функцијском пољу уочавамо прстен

$$\mathcal{O}_{V,P} = \{\phi \in K(V) \mid \phi = \frac{F}{G}, F, G \in K[V], G(P) \neq 0\},$$

који се назива *локални прстен варијетета* $V$ *у* $P$. Другим речима, то је прстен свих дефинисаних рационалних функција у тачки $P \in V$. Локални је зато што је у њему $\mathfrak{m}_P = \{\phi \in \mathcal{O}_{V,P} \mid \phi(P) = 0\}$ једини максималан идеал. То се лако доказује, јер сваки елемент $\phi \in \mathcal{O}_{V,P} \backslash \mathfrak{m}_P$ је пресликавање дефинисано (регуларно) у $P$ за које важи $\phi(P) = \frac{F(P)}{G(P)} \neq 0$, одакле је и његово инверзно пресликавање $\phi^{-1} = \frac{G}{F}$ је дефинисано (регуларно) у $P$, одакле $\phi^{-1} \in \mathcal{O}_{V,P}$, одакле следи да је $\phi \in \mathcal{O}^*_{V,P}$, а ово је карактеризација локалних прстена са њиховим јединственим максималним идеалном (видети, на пример [4]).

Иако смо у првој глави већ видели један пример рационалног пресликавања и морфизма, тек ћемо их овде дефинисати. *Рационално пресликавање* између варијетета $V_1$ и $V_2 \subseteq \mathbb{P}^n$ је пресликавање облика $\phi = [\phi_0, ..., \phi_n]$, где су $\phi_0$, ... , $\phi_n \in K(V_1)$. Наравно, ово пресликавање треба да има смисла, тј. да за све $P \in V_1$ за које

су $\phi_0$, ... , $\phi_n$ дефинисани важи да је $\phi(P) = [\phi_0(P), ...., \phi_n(P)] \in V_2$. Примећујемо да се не захтева да пресликавања $\phi_0$, ... , $\phi_n$ буду дефинисана у свакој тачки $P \in V_1$. Некада се то може отклонити, а некада и не.

У пројективним просторима постоји очекиван начин да решимо проблем лоше дефинисаности. Рационално пресликавање

$$\phi = [\phi_0, ..., \phi_n] : V_1 \longrightarrow V_2$$

је *дефинисано* (или *регуларно*) у тачки $P \in V_1$ ако постоји пресликавање $g \in K(V_1)$ за које важи да су $g\phi_0$, ... , $g\phi_n$ дефинисана у $P$ и бар једна једна од њих у тачки $P$ није нула. Тада је $\phi(P) = [g\phi_0(P), ..., g\phi_n(P)]$.

Видимо да је овај начин заиста добро дефинисано пресликавање у тачки $P$ које је у пројективном простору једнако полазном. Види се да можемо да узмемо различите функције $g$ за различите тачке $P$, не мора једна функција бити довољна за све тачке код којих има проблем. Ако проблем дефинисаности можемо да решимо у свакој тачки, тј. ако је пресликавање $\phi$ регуларно у свакој тачки, онда се назива *морфизам*. Није свако рационално пресликавање и морфизам.

*Димензија варијетета* се дефинише као трансцендентни степен раширења $[K(V) : K]$, што би интуитивно требало да видимо као број параметара који описује варијетет (јер оне преостале онда можемо да изразимо полиномски преко ових познатих параметара) и то нам даје разумну представу димензије.

**Дефиниција 1.** *Алгебарска крива* је пројективни варијетет димензије 1.

Већ може да нам буде јасно зашто је овако дефинисана алгебарска крива, на пример, ако узмемо скуп $F(x, y) = 0$ у равни, то је афина алгебарска крива, али уједно можемо полиномски да изразимо $y$ преко $x$ у пољу $K$ над којим гледамо и зато добијамо димензију 1, јер је $x$ неодређена, па и трансцендентно над $K$. На даље ћемо алгебарску криву звати једноставно крива и претпостављаћемо да

је крива задата једном једначином (афино или пројективно).

Криве које имају шиљке или самопресеке се понашају доста другачије у односу на остале, а и обично када цртамо криву, цртамо је „нормалну", глатку, зато ћемо углавном проучавати само такве криве, јер код њих важе очекивани закључци. Неко ко зна стуктуру рационалних тачака елиптичких кривих већ зна један пример велике разлике у случају када је крива глатка и сингуларна (погледати [51]).

**Дефиниција 2.** Крива $C : F = 0$ је *глатка у тачки* $P \in C$ ако бар неки парцијални извод полинома $F$ у тачки $P$ нема вредност нула. Крива је *глатка* ако је глатка у свакој својој тачки $P \in C$. У супротном се назива *сингуларна*.

**Пример 1.** Нека је (афина) крива дата једначином $C : y^2 = f(x)$, при чему је $f \in K[x]$. Тада је $C$ глатка ако и само ако $f$ нема вишеструких нула у $K$. Јасно се види да једине тачке које могу бити сингуларне су тачке облика $P_\alpha = (\alpha, 0)$, при чему је $\alpha$ вишеструка нула полинома $f$.

Глатке криве имају многе лепе особине. Почињемо са једном која је нетривијална, али која има многе згодне последице.

**Тврђење 1.** Нека је $P \in C$ глатка тачка криве $C$. Тада је $\mathcal{O}_{C,P}$ прстен дискретне валуације.

Литература где су лепо објашњени прстени дискретне валуације је [24] или [4]. Доказ овог тврђења дајемо у специјалном случају када је крива хиперелиптичка у делу намењеном за то. Подсећања ради, комутативни домен целих $R$ је *прстен дискретне валуације* ако постоји дискретна валуација $v$ на њему за коју је $R^* = \{r \in R \mid v(r) = 0\}$ и идеал $\{r \in R \mid v(r) > 0\}$ је главни. *Дискретна валуација* на $R$ је пресликавање $v : R \longrightarrow \mathbb{N}_0 \cup \{\infty\}$ које је „на" и задовољава следећа својства (за све $r$ и $r'$ из прстена $R$):
(1) $v(r) = \infty \iff r = 0$;
(2) $v(rr') = v(r) + v(r')$;
(3) $v(r + r') \geq \min\{v(r), v(r')\}$.

Специјално, када је крива $C$ глатка, онда је у свакој тачки $P \in C$ $\mathcal{O}_{C,P}$ прстен дискретне валуације.

**Дефиниција 3.** У свакој глаткој тачки $P \in C$ можемо увести природну *(нормализовану) валуацију*, која се некад назива и *$P$-адична валуација*

$$\mathrm{ord}_P : \mathcal{O}_{C,P} \longrightarrow \mathbb{N}_0 \cup \{\infty\},$$

$$\mathrm{ord}_P(\phi) = \sup\{d \in \mathbb{N}_0 \mid \phi \in \mathfrak{m}_P^d\}.$$

Коришћењем да је $\mathrm{ord}_P(\frac{F}{G}) = \mathrm{ord}_P(F) - \mathrm{ord}_P(G)$ продужавамо валуацију $\mathrm{ord}_P$ на $K(C)$ и добијамо пресликавање

$$\mathrm{ord}_P : K(C) \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

*Равномернизатор за $C$ у $P$* је било која функција $t \in K(C)$ за коју је $\mathrm{ord}_P(t) = 1$, тј. било који генератор идеала $\mathfrak{m}_P$.

**Дефиниција 4.** Нека је $P$ глатка тачка на кривој $C$ и $\phi \in K(C)$. *Ред функције $\phi$ у $P$* је $\mathrm{ord}_P(\phi)$. Ако је $\mathrm{ord}_P(\phi) > 0$, онда кажемо да је $P$ *нула* функције $\phi$, а ако је $\mathrm{ord}_P(\phi) < 0$, онда кажемо да је $P$ *пол* функције $\phi$. Ако је $\mathrm{ord}_P(\phi) \geq 0$, онда је $\phi$ *регуларно (дефинисано)* у тачки $P$ и можемо израчунати вредност $\phi(P)$. У супротом, $\phi$ има пол у $P$ и тада стављамо $\phi(P) = \infty$.

**Пример 2.** Пројективна права $\mathbb{P}^1$ се описује са две координате. Пошто немамо услова за координате $x$ и $y$, онда је $K[\mathbb{P}^1] = K[x, y]$, односно $K(\mathbb{P}^1) = K(x, y)$, али не цело, већ, ради добре дефинисаности, количници хомогених полинома истог степена. Ако гледамо само афини део, аналогно је $K[\mathbb{A}^1] = K[x]$ и $K(\mathbb{A}^1) = K(x)$.

Због услова да у пројективном простору морамо имати количнике хомогених полинома истог степена, након дељења свега са $y$ можемо индентификовати просторе $K(\mathbb{P}^1) = K(\mathbb{A}^1) = K(x)$. Некад ћемо користити ову идентификацију, а некад не. Одредимо равномернизатор произвољне тачке пројективне праве $[a, b]$.

Треба нам полином који је у тој тачки нула тачно једног реда, па је најједноставније узети $\frac{bx-ay}{y}$, за $[a,b] \neq [1,0]$, док за $[1,0]$ узимамо $\frac{y}{x}$. Ако гледамо афине координате, ту морамо разликовати случај кад је тачка коначна - за тачку $a \in \mathbb{A}^1$ равномернизатор је $x-a$, док је за бесконачну тачку $\infty$ равномернизатор $\frac{1}{x}$.

Следећи пример наводимо без доказа, доказ ове чињенице уопште није лак и веома је напоран и налази се касније у тексту са идејом да илуструје колико је тешко доказати нешто што је веома очекивано.

**Пример 3.** Посматрајмо криву $C : y^2 = f(x)$ над алгебарским затворењем поља $K$ - $\overline{K}$ када полином $f$ нема вишеструке корене. Нека је $\alpha \in \overline{K}$ нула полинома $f$, тада је $P_\alpha = (\alpha, 0)$ глатка тачка на кривој $C$. Сада знамо да постоји равномернизатор за $C$ у тачакама $P_\alpha$, то ће бити функција $y \in \mathfrak{m}_{P_\alpha}$.

Јасно је да је $y(P_\alpha) = 0$, а не очекујемо да постоји функција која је мањег реда, једноставно не можемо видети ништа што би уз помоћ једначине криве могло да има мањи ред. Можемо да приметимо и да за функцију $x-\alpha$ важи $(x-\alpha)(P_\alpha) = 0$, међутим она није равномернизатор, заправо из једначине криве налазимо

$$(x-\alpha) = \frac{y^2}{\frac{f(x)}{x-\alpha}},$$

и $P_\alpha$ је нула реда 2, јер по претпоставци је $\alpha$ једноструки корен полинома $f$, а у $P_\alpha$ $y^2$ има двоструку нулу. Са друге стране, ако узмемо произвољну тачку криве $P_{\alpha\beta} = (\alpha, \beta) \in C$ такву да је $\beta \neq 0$, тада не пролази претходни аргумент и сада ће $x-\alpha$ бити равномернизатор у тачки $P_{\alpha\beta}$. Као и малопре, не доказујемо ово, али има смисла да поверујемо у то.

За крај, пошто криве посматрамо као пројективне објекте, треба обратити пажњу на случајеве у бесконачности. Уочавамо да имамо два случаја.

Први случај је ако је степен полинома $f$ паран број, рецимо $2g+2$, за неко $g \in \mathbb{N}_0$, тада имамо две тачке у бесконачности, које ћемо означити са $\infty_s$ и $\infty_{-s}$ (ако знамо да је водећи коефицијент $f$ једнак 1, онда само са $\infty_+$ и $\infty_-$). Функција $\frac{1}{x}$ ће бити равномернизатор

у тим тачкама, па ћемо имати $\mathrm{ord}_{\infty_{\pm s}}(x) = -1$, тј. $x$ има пол реда 1 у бесконачним тачкама и $\mathrm{ord}_{\infty_{\pm s}}(y) = -g-1$, одакле $y$ има још већи пол у овим тачкама.

У другом случају, када је степен полинома $f$ непаран број, немамо две „супротне" бесконачности, већ само једну, $\infty$. Сада је $\mathrm{ord}_{\infty}(x) = -2$, док је $\mathrm{ord}_{\infty}(y) = -2g-1$. Пошто са једне стране имамо функцију која има најјачи паран степен 2, а са друге стране непаран степен, и сваки поредак је цео број, не изненађује нас ни овај резултат. Због ових познатих вредности, видимо да за равномернизатор у овој бесконачности $\infty$ можемо узети $\frac{x^g}{y}$.

Како је $\phi \in K(C)$ количник два полинома, очекиван је и следећи резултат.

**Тврђење 2.** Нека је $C$ глатка крива и $\phi \in K(C)$, при чему $\phi \neq 0$ (где је 0 константна нула функција). Тада $\phi$ има коначно много нула и полова.

**Тврђење 3.** Нека је $K$ алгебарски затворено поље и $C$ глатка крива над $K$. Тада је за свако $\phi \neq 0 \in K(C)$ број нула и полова (рачунатих са вишеструкошћу) једнак. Ако $\phi$ нема полова уопште, онда је $\phi$ константна функција.

Да бисмо стекли осећај о функцијским пољима, наводимо још једно тврђење које личи на оно што ћемо касније користити.

**Тврђење 4.** Претпоставимо да је $K$ перфектно поље. Нека је $P \in C$ глатка тачка и $t \in K(C)$ равномернизатор за ту тачку. Тада је $K(C)$ коначно сепарабилно раширење поља $K(t)$.

Коначност овог раширења можемо да видимо због тога што су и $K(C)$ и његово потпоље $K(t)$ трансцендентог степена 1 над $K$. За доказ да је ово раширење и сепарабилно, погледати, на пример, [51]. Следеће тврђење се може брзо доказати коришћењем својства да је $\mathfrak{m}_P$ прстен дискретне валуације за све глатке тачке $P$ криве $C$.

**Тврђење 5.** Нека је $\phi : C \longrightarrow V$ рационално пресликавање, при чему је $V \subseteq \mathbb{P}^n$ варијетет и нека је $P \in C$ глатка тачка. Тада је

$\phi$ регуларно у $P$. Специјално, ако је $C$ глатка, тада је $\phi$ морфизам.

Следећа теорема делује невероватно на први поглед! Као што се и може претпоставити, веома је корисна и има доста примена.

**Теорема 4.** Нека је $\phi : C_1 \longrightarrow C_2$ морфизам глатких кривих. Тада је $\phi$ константно или „на".

За крај овог навођења теорема, наводимо још једно важно тврђење, које је битно из разлога да бисмо могли да формализујемо неке објекте које очекујемо да ће се баш тако понашати. Убрзо ћемо да видимо тај процес уз неколико примера, јер је ово за прво читање мало збуњујуће. Пре тога, треба нам и нова дефиниција.

**Дефиниција 5.** Нека је $\phi : C_1 \longrightarrow C_2$ неконстантно рационално пресликавање глатких кривих над пољем $K$. Ово пресликавање индукује инјективно пресликавање $\phi^* : K(C_2) \longrightarrow K(C_1)$ дефинисано са $\phi^*(f) = f \circ \phi$.

Најчешће се приликом овог пресликавања ни не користе заграде, тј. пише се $\phi^* f$ уместо $\phi^*(f)$. Пошто је $f$ рационално пресликавање из $C_2$ у $K$, можемо узети композицију рационалног неконстантног пресликавања $\phi$ које пресликава $C_1$ у $C_2$ и $f$ које ће слике у $C_2$ даље послати у $K$ и овом композицијом заиста добијамо рационално пресликавање из $C_1$ у $K$. По конструкцији се види да је овакво пресликавање инјективно (јер је $\phi$ „на", пошто није константно).

**Теорема 5.** Нека су $C_1$ и $C_2$ глатке криве посматране над пољем $K$ и $\phi$ неконстантно рационално пресликавање између њих. Тада је $K(C_1)$ коначно раширење поља $\phi^*(K(C_2))$.

Ова теорема је значајна, јер нам омогућава да дефинишемо степен рационалних пресликавања између кривих. Следе две дефиниције које су веома важне за даљи рад.

**Дефиниција 6.** Нека је $\phi : C_1 \longrightarrow C_2$ рационално пресликавање између кривих над пољем $K$. Ако је $\phi$ константно, онда је *степен*

тог пресликавања 0. Иначе, кажемо да је пресликавање $\phi$ *коначно* и *степен* тог пресликавања дефинишемо као

$$\deg \phi = [K(C_1) : \phi^* K(C_2)].$$

Кажемо да је $\phi$ *сепарабилно*, *несепарабилно*, *чисто несепараабино* ако је такво раширење поља $K(C_1)/\phi^*(C_2)$ и означавамо сепарабилни и несепарабилни степен пресликавања $\phi$ са $\deg_s \phi$ и $\deg_i \phi$, редом.

Дефиниција степена је мало компликована, треба да имамо на уму да оваква дефиниција подржава нама познато својство степена полинома, пресликавање је степена $d$ ако је скоро свуда пресликавање „$d$-на-1". Иако је ово корисно упамтити, у коначној карактеристици уме ипак да буде нетачно.

**Пример 4.** Нека је $K$ поље карактеристике која није 2. Тада морфизам $\phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^1$, задат са $\phi(x) = x^2$, је јасно скоро свуда „2-на-1", те очекујемо да је његов степен 2. Одредимо $\phi^* K(\mathbb{A}^1)$. Пре свега, знамо да је $K(\mathbb{A}^1) = K(x)$. Онда $\phi^*$ дејствује на функцију, тако што јој уместо аргумента $x$ убаци аргумент $x^2$. Дакле, могу се добити све рационалне функције од $x^2$ и ништа више. Према томе, степен пресликавања $\phi$ је степен раширења $[K(x) : K(x^2)]$, који је јасно 2.

Аналогно би било да смо посматрали пресликавање $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$, задато са $\phi[x, y] = [x^2, y^2]$. Пошто је $K(\mathbb{P}^1)$ се састоји од количника хомогених полинома по $x$ и $y$ деобом свега са $y$ (тј. одговарајућим степеном), добијамо да су функције из $K(\mathbb{P}^1)$ могу преставити као функције из $K(\mathbb{A}^1)$ и да је пресликавање $\phi$ у овом случају, када се гледа афини облик $x \mapsto x^2$, тако да се ово своди на претходни случај.

**Пример 5.** Нека је $K = \mathbb{F}_p$ и уочимо Фробенијусово пресликавање $\pi_p : \mathbb{A}^1(\overline{K}) \longrightarrow \mathbb{A}^1(\overline{K})$. Слично као у претходном примеру, $\deg \pi_p = [\overline{K}(x) : \overline{K}(x^p)] = p$ и знамо и више, да је ово чисто несепарабилно раширење. Дакле $\deg \pi_p = \deg_i \pi_p = p$, $\deg_s \pi_p = 1$. Међутим, као што знамо, Фробенисујово пресликавање је „1-1", према томе у овом случају се интуција о броју тачака које се сликају у исту тачку и степену пресликавања не поклапа.

**Пример 6.** Овај пример је уопштење претходна два примера, то је за генерални случај полиномског пресликавања афиних правих. Нека је $\phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^1$ дефинисано са $\phi(x) = a(x)$, за неки полином $a \in K[x]$. Тада $\deg \phi = \deg a(x)$, при чему је $\deg a(x)$ ознака за степен полинома.

Нека је $t = a(x)$. Сада као и у претходним случајевима $\phi^* K(\mathbb{A}^1) = K(t) \subseteq K(x)$ и треба да одредимо степен овог раширења. Најуочљивији полином над $K(t)$ који $x$ поништава је $a(T) - t \in K(t)[T]$. Овај полином је степена $\deg a(x)$. Остаје још да докажемо да је несводљив.

Како је $t$ трансцендентан над $K$, то је $K[t]$ прстен са јединственом факторизацијом и можемо применити Гаусову лему која нам каже да је довољно да докажемо несводљивост над $K[t][T] = K[t, T]$. Напишимо $a(T) - t$ као производ два полинома из $K[t, T]$. Нека је $a(T) - t = g(t, T)h(t, T)$. Пошто је $a(T) - t$ линеаран по $t$ један од полинома $g$ и $h$ мора бити линеаран по $t$, а други константан. На пример, $g(t, T) = g_1(T)t + g_2(T)$ и $h(t, T) = h_1(T)$. Када заменимо ово у једначину, добијамо

$$a(T) - t = g_2(T)h_1(T) + g_1(T)h_1(T)t.$$

Сада је $g_1(T)h_1(T) = -1$, одакле је $h_1$ константан полином и по $T$, па је $h(t, T)$ константан полином. Ово управо значи да је полином $a(T) - t$ несводљив над $K[t, T]$, а самим тим и над траженим прстеном $K(t)[T]$, одакле је заиста $[K(x) : K(t)] = \deg a(x)$.

Посебно је згодно ако знамо да је степен пресликавања између глатких кривих 1, јер тада имамо користан закључак.

**Тврђење 6.** Нека је $\phi : C_1 \longrightarrow C_2$ рационално пресликавање између глатких кривих степена 1. Тада је $\phi$ изоморфизам.

**Пример 7.** Сетимо се примера из прве главе: Питагорине тројке над пољем $K$ (које формирају глатку пројективну криву $C : X^2 + Y^2 = Z^2$) су изоморфне пројективној правој (што је такође глатка пројективна крива). Морфизам који слика $\phi : C \longrightarrow \mathbb{P}^1$ дефинишемо са $\phi : [X, Y, Z] \mapsto [X + Z, Y]$. Погледајмо како дејствује $\phi^* : K(\mathbb{P}^1) \longrightarrow K(C)$. Слике $\phi^*$ су пресликавања облика $\frac{P(X+Z,Y)}{Q(X+Z,Y)}$, где су $P, Q \in K[x, y]$ било који хомогени полиноми истог степена.

Специјално, посматрајући $\frac{P(X,Y)}{Q(X,Y)} = \frac{X}{Y}$ и $\frac{P(X,Y)}{Q(X,Y)} = \frac{Y}{X}$, закључујемо да $\frac{X+Z}{Y}, \frac{Y}{X+Z} \in \phi^* K(\mathbb{P}^1)$. Међутим, пошто ту важи $Z^2 = X^2 + Y^2$, тада $\frac{Y}{X+Z} = \frac{Y(Z-X)}{Z^2-X^2} = \frac{Z-X}{Y} \in \phi^* K(\mathbb{P}^1)$, одакле је $\frac{X}{Y}, \frac{Z}{Y} \in \phi^* K(\mathbb{P}^1)$, а како су то генератори $K(C) = K[X,Y,Z]/\langle X^2 + Y^2 - Z^2 \rangle$, тиме је $\phi^* K(\mathbb{P}^1) = K(C)$, одакле је $\phi$ степена 1, а по претходном тврђењу и изоморфизам.

**Дефиниција 7.** Нека је $\phi : C_1 \longrightarrow C_2$ неконстантно рационално пресликавање између глатких кривих над пољем $K$ и $P \in C_1$ произвољна тачка. *Индекс рамификације пресликавања $\phi$ у $P$* се означава са $e_\phi(P)$ и дефинише се као

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)}),$$

где је $t_{\phi(P)} \in K(C_2)$ равномернизатор у тачки $\phi(P)$. Кажемо да је $\phi$ *рамификовано* у тачки $P$ ако је $e_\phi(P) > 1$, а да је *нерамификовано* ако је $e_\phi(P) = 1$, док је $\phi$ *нерамификовано* ако је нерамификовано у свакој тачки криве $C_1$.

Одмах примећујемо да дефиниција имплицитно подразумева да је $e_\phi(P) \geq 1$. То се проверава тако што запишемо пресликавање из дефиниције $P \mapsto \phi^* t_{\phi(P)}(P) = t_{\phi(P)}(\phi(P)) = 0$, дакле пресликавање се стварно анулира у тачки $P$ и у зависности од тога колико је реда та нула, добијамо индекс рамификације (који је бар 1). Из следећег тврђења можемо наслутити да је пресликавање између кривих степена $d$ ако је оно скоро свуда $d$ према 1.

**Тврђење 7.** Нека је $\phi : C_1 \longrightarrow C_2$ неконстантно рационално пресликавање између глатких кривих и $Q \in C_2$ произвољна тачка. Тада

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi).$$

**Пример 8.** Уочимо пресликавање $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ дато са $\phi([x,y]) = [x^3(x-y)^2, y^5]$. Као и у неком од претходних примера, нпр. број 4, уместо да посматрамо функцијска поља пројективне праве, можемо да пређемо на функцијска поља афине праве, где сада имамо $\phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^1$, $\phi(x) = x^3(x-1)^2$, $\phi(\infty) = \infty$. Сада по примеру број 6, закључујемо да је ово пресликавање степена 5.

Остаје још да одредимо индексе рамификације. Посебно ћемо дискутовати афине тачке, а посебно бесконачну тачку. Ово је прилика да експлицитно видимо како може да се рачуна индекс рамификације, пошто је дефиниција на први поглед јако незгодна.

Први случај: нека је $a \in \mathbb{A}^1$ афина тачка. Тада је равномернизатор у тој тачки $x - a$. Даље је $\phi(a) = a^3(a-1)^2$, одакле је равномернизатор за $\phi(a)$ једнак $y - a^3(a-1)^2$. По дефиницији индекса рамификације, треба одредити колика је нула $a$ функције $(y - a^3(a-1)^2) \circ (x^3(x-1)^2)$, тј. другим речима треба одредити колики степен $x-a$ дели полином $p(x) = x^3(x-1)^2 - a^3(a-1)^2$. Свакако је овај полином дељив са $x - a$, а за вишеструке корене, узимамо извод $p'(x) = x^2(x-1)(5x-3)$.

Одавде видимо да су једине могуће вишеструке нуле $p(x)$: $x = 0$, $x = 1$, $x = \frac{3}{5}$. Узимајући други извод, видимо да ће једино $x = 0$ да буде његова нула од понуђених, која неће бити и нула трећег извода. Одавде изводимо укупан закључак, једине рамификоване афине тачке пресликавања $\phi$ су: $x = 0$, са индексом рамификације $e_\phi(0) = 3$, $x = 1$, $e_\phi(1) = 2$, $x = \frac{3}{5}$, $e_\phi(\frac{3}{5}) = 2$.

Други сучај: нека је $[1, 0]$ бесконачна тачка, у овом случају морамо да користимо пројективни облик. Она се слика у саму себе. Равномернизатор у тој тачки је $\frac{y}{x}$. Сада треба проверити колико се анулира $\frac{y}{x}$ у $\dfrac{y^5}{x^3(x-y)^2}$. Наравно, ово је сада лако препаковати

$$\frac{y^5}{x^3(x-y)^2} = \frac{(\frac{y}{x})^5}{(1-\frac{y}{x})^2}.$$

Одавде видимо да је ред $\frac{y}{x}$ у овом изразу 5, јер се $1 - \frac{y}{x}$ не рачуна у ред. Дакле, ова тачка је рамификована и то индекса рамификације 5.

Сада, на пример, можемо проверити формулу за тачку 0 и $\infty$.
$\phi^{-1}(0) = \{0, 1\}$ и $e_\phi(0) + e_\phi(1) = 3 + 2 = 5 = \deg \phi$;
$\phi^{-1}(\infty) = \infty$ и $e_\phi(\infty) = 5 = \deg \phi$.

**Пример 9.** Посматрајмо стару криву $C : y^2 = f(x)$, где је $f \in K[x]$ полином који нема вишеструке корене. Уочимо пресликавање

(дато у афином облику) $\phi : C \longrightarrow \mathbb{A}^1$ дефинисано са $\phi : (x, y) \mapsto x$.

Придружено пресликавање је $\phi^* : K(\mathbb{A}^1) = K(x) \longrightarrow K(C)$ чија су слика све функције по $x$ у пољу $K(C)$. Те функције нису цело $K(C)$, јер функција $y$, тј. њена пројекција, не може да се изрази по $x$ (пошто би тада полином $f$ био квадрат, а то смо претпоставили да није), док се функција $y^2$ изражава по $x$, тако смо дефинисали једначину. Зато су константна 1 функција и $y$ функција база за $K(C)$(=количничко поље $K[x, y]/\langle y^2 - f(x)\rangle$) над $\phi^*K(x)$, одакле је ово раширење степена 2, па је самим тим и пресликавање $\phi$ степена 2.

Сада ћемо тестирати везу из претходног тврђења. Дискутоваћемо случајеве да ли је $\alpha$ нула полинома $f$ или није или је бесконачно.

Нека је за почетак $f(\alpha) \neq 0$. Тада је

$$\phi^{-1} = \{P_{\alpha+} = (\alpha, \sqrt{f(\alpha)}), P_{\alpha-} = (\alpha, -\sqrt{f(\alpha)})\}$$

скуп од две различите тачке. Пошто је $\deg \phi = 2$, формула нам одмах даје да је $\phi$ нерамификовано у тачкама $P_{\alpha+}$ и $P_{\alpha-}$. Ово можемо проверити и по дефиницији, довољно је за једну од њих. $e_\phi(P_{\alpha+}) = \mathrm{ord}_{P_{\alpha+}}(\phi^*(x - \alpha))$, јер је $x - \alpha \in K(x) = K(\mathbb{A}^1)$ равномернизатор за $\alpha = \phi(P_{\alpha+})$. Сада, по дефиницији, желимо да одредимо поредак нуле којим $P_{\alpha+}$ анулира $\phi^*(x - \alpha)$: $\phi^*(x - \alpha)(P_{\alpha+}) = (x - \alpha) \circ \phi(P_{\alpha+}) = (x - \alpha)(\alpha)$. У претходном примеру смо показали да је у овом случају $x - \alpha$ и равномернизатор тачке $P_{\alpha+}$ на кривој $C$, одакле је овај индекс заиста једнак 1.

Нека је $f(\alpha) = 0$. Тада је $\phi^{-1} = \{P_\alpha = (\alpha, 0)\}$. Пошто овакве вредности имају само једну инверзну тачку на кривој $C$, формула нам даје да је $\phi$ рамификована у тачкама $P_\alpha$, јер добијамо $e_\phi(P_\alpha) = 2$. И у ово се можемо уверити $e_\phi(P_\alpha) = \mathrm{ord}_{P_\alpha}(\phi^*(x - \alpha))$, одакле опет тражимо ред нуле $P_\alpha \mapsto \phi^*(x - \alpha)(P_\alpha) = (x - \alpha)(\alpha) = 2$, јер ово знамо из примера број 3.

Остаје још бесконачни случај, јер иако записујемо афино да би било једноставније, не треба да заборавимо да живимо у пројективном простору. Остаје нам још једна бесконачна тачка $\infty$.

Као и у претходном примеру, имамо два случаја, у зависности од парности степена полинома $f$.

Ако је $\deg(f) = 2g+2$, за $g \in \mathbb{N}_0$, тада имамо две бесконачности на кривој $C$, $\infty_s$ и $\infty_{-s}$ и обе се сликају у $\infty$. Као у првом случају, закључујемо да су оне нерамификоване, а довољно је да се уверимо да то важи за једну од њих, што можемо брзо да учинимо: $e_\phi(\infty_s) = \mathrm{ord}_{\infty_s}(\phi^* \frac{1}{x})$, јер је $\frac{1}{x}$ равномернизатор за бесконачну тачку, а пошто је то уједно и равномернизатор за $\infty_s$ на кривој $C$, онда је $\infty_s \mapsto \phi^* \frac{1}{x}(\infty_s) = \frac{1}{x}(\infty)$ нула реда 1.

Ако је $\deg(f) = 2g+1$, за $g \in \mathbb{N}_0$, тада имамо једну бесконачност на кривој $C$, коју смо исто означили са $\infty$ и она мора бити рамификована, јер важи $e_\phi \infty = 2$. Директно се уверавамо у ово, имајући на уму $\mathrm{ord}_\infty(\frac{1}{x}) = 2$ на кривој $C$ у овом слухају: $e_\phi(\infty) = \mathrm{ord}_\infty(\phi^* \frac{1}{x})$; $\infty \mapsto \phi^* \frac{1}{x}(\infty) = \frac{1}{x}(\infty)$ - а ово је нула реда два, посматрајући $\infty \in C$. У овом примеру имамо злоупотребу нотације, пошто се две различите ствари означавају исто, али то не би требало да буде збуњујуће, чак и иста ознака треба да подржи тај осећај да имамо само једну бесконачност у овом случају.

**Пример 10.** Нека је глатка крива $C \subseteq \mathbb{P}^2$ задата једначином $F = 0$, где је $F = F(x,y,z) \in K[x,y,z]$ хомоген полином степена $d$. Претпоставимо да $[0,0,1] \notin C$, тј. да полином $F$ садржи члан $z^d$.

Ово можемо постићи дозвољеном променом координата - ако не постоји неки од $x^d$, $y^d$, онда заменимо ту координату са $z$, а иначе можемо применити линеарну промену координата $y \mapsto y + \xi z$, при чему је $\xi \in K$, такво да $\xi^d = -1$, што постоји јер препостављамо да је $K$ алгебарски затворено. Тада можемо добро дефинисати пресликавање $\phi : C \longrightarrow \mathbb{P}^1$ са $\phi[x,y,z] = [x,y]$. Ово пресликавање је степена $d$. То проверавамо на сличан начин као и до сада. Видимо да је $\phi^* K(\mathbb{P}^1) = \left\{ \frac{P(x,y)}{Q(x,y)} \right\}$, где су $P$ и $Q$ хомогени полиноми по $x$ и $y$ истог степена. Поделимо једначину $F(x,y,z) = 0$ са $x^d$, одакле одређујемо полином степена $d$ са коефицијентима у $\phi^* K(\mathbb{P}^1)$ који поништава $\frac{z}{x}$.

Слично, као и у примеру број 6 добијамо да је тај полином несводљив над $\phi^* K(\mathbb{P}^1)$, одакле добијамо да је

$$[\phi^* K(\mathbb{P}^1)(\frac{z}{x}) : \phi^* K(\mathbb{P}^1)] = d,$$

а пошто је $\frac{z}{x}$ генератор који нам фали да добијемо $K(C)$ из $\phi^*K(\mathbb{P}^1)$, одатле је $[K(C) : \phi^*K(\mathbb{P}^1)] = d$, што је и требало да покажемо. У овом примеру је тешко израчунати индексе рамификације.

## 2.2 Конкретно о хиперелиптичким кривама

**Препоручена литература:** Овај текст се у највећој мери поклапа са текстом у [53].

За проучавање хиперелиптичких кривих је згоднија мало измењена пројективна раван, у којој координате неће бити скроз хомогене, а то је због тога што ће ове криве бити већег рода од 1.

**Дефиниција 8.** Нека је $g \in \mathbb{N}_0$. *Отежињена пројективна раван* $\mathbb{P}^2_g = \mathbb{P}^2_{(1,g+1,1)}$ је скуп тачака из $K^3$ посечен по релацији еквиваленције $\sim$, где је релација $\sim$ дефинисана са $(x, y, z) \sim (x', y', z')$ ако и само ако постоји неко $\lambda \in K^*$ такво да је $(x', y', z') = (\lambda x, \lambda^{g+1} y, \lambda z)$. Пишемо $[x, y, z]$ за тачке (класе еквиваленције) отежињене пројективне равни. Скуп $K$-рационалних тачака $\mathbb{P}^2$ се означава са $\mathbb{P}^2(K)$.

*Координатни прстен* над $K$ је прстен $K[x, y, z]$, али такав да је неодређеним $x$ и $z$ додељена тежина (степен) 1, док је неодређеној $y$ додељена тежина (степен) $g+1$. Полином $F \in K[x, y, z]$ је *хомоген* степена $d$ ако сви његови чланови степена $d$ у овом новом смислу, тј. ако се полином састоји од коначног збира монома $cx^{i_1}y^{i_2}z^{i_3}$, при чему $i_1 + (g + 1)i_2 + i_3 = d$.

Приметимо да се за $g = 0$ добије обична пројективна раван и да су хомогени полиноми по овој дефиницији уобичајени хомогени полиноми. Такође, очекујемо још неке сличне особине које има пројективна раван. На пример, тачке код којих је $z \neq 0$ можемо сматрати тачкама афине равни $\mathbb{A}^2(K)$ и то тако што су бијективна пресликавања дата са: $[x, y, z] \mapsto (\frac{x}{z}, \frac{y}{z^{g+1}})$, односно $(x, y) \mapsto [x, y, z]$.

На сличан начин се може успоставити бијекција између тачака $\mathbb{P}^2(K)$ за које је $x \neq 0$ и $\mathbb{A}^2(K)$. Ова два подскупа $\mathbb{P}^2(K)$ се називају *стандардни афини делови* $\mathbb{P}^2(K)$. Међутим, они не покривају цео $\mathbb{P}^2(K)$! Али, покриће скоро све тачке, заправо, само једна тачка $[0, 1, 0]$ остаје непокривена, међутим ова тачка се неће налазити на

хиперелиптичким кривама које посматрамо, тако да то не треба да нас брине. Сада ћемо дефинисати хиперелиптичке криве.

**Дефиниција 9.** Нека је $g \in \mathbb{N}\backslash\{1\}$. *Хиперелиптичка крива рода* $g$ над пољем $K$ које није карактеристике 2 је подвариједетет $\mathbb{P}_g^2$ задат једначином облика $y^2 = F(x,z)$, где је $F \in K[x,z]$ бесквадратни хомоген полином (у нормалном смислу) степена $2g+2$. Ако је $C$ крива, тада је скуп њених *$K$-рационалних тачака*

$$C(K) = \{[x_0, y_0, z_0] \in \mathbb{P}_g^2(K) \mid y_0^2 = F(x_0, z_0)\}.$$

Када је $K = \mathbb{Q}$, за $\mathbb{Q}$-рационалне тачке кажемо само *рационалне тачке*.

Видимо да је полином који дефинише хиперелиптичку криву $C$ : $y^2 - F(x,z)$ хомоген у овом новом смислу, те да су добро дефинисане њене тачке: Ако су $[x_0, y_0, z_0]$ и $[x_1, y_1, z_1]$ различити преставници исте тачке у $\mathbb{P}_g^2$, тада је $[x_1, y_1, z_1] = [\lambda x_0, \lambda^{g+1} y_0, \lambda z_0]$ за неко $\lambda \in K^*$, одакле је

$$y_1^2 - F(x_1, z_1) = \lambda^{2g+2}(y_0^2 - F(x_0, z_0)),$$

па је

$$y_1^2 - F(x_1, z_1) = 0 \iff y_0^2 - F(x_0, z_0) = 0.$$

Из претходног поглавља видимо и зашто је оправдано ову криву називати кривом рода $g$. Одмах примећујемо да проблематична тачка $[0,1,0]$ заиста не припада хиперелиптичкој кривој $C$. Зато можемо поделити криву на два афина дела.

**Дефиниција 10.** Пресеци криве $C$ са афиниим деловима $\mathbb{P}_g^2$ се називају *стандардни афини делови* криве $C$.

Афини делови криве $C$ су афине равне криве, задате једначинама $y^2 = F(x,1)$ и $y^2 = F(1,z)$. Означимо $f(x) = F(x,1)$. На даље ћемо користити једноставну ознаку $y^2 = f(x)$ за криву $C$, а иако је ово афина једначина, нећемо заборавити да посматрамо криву $C$ као пројективну криву. Полином $F(x,z)$ је бесквадратан, према томе, не дели га $z^2$, одакле мора бити да је бар један од коефицијената уз $x^{2g+2}$ и $x^{2g+1}z$ различит од нуле, одакле закључујемо да је $\deg f = 2g+2$ или $\deg f = 2g+1$. Видимо да и полазећи од полинома

$f(x)$ можемо реконструисати полином $F(x,z)$, додавањем степена $z$ тако да добијемо хомоген полином степена $2g+2$.

Нека је $F(x,z) = f_{2g+2}x^{2g+2} + f_{2g+1}x^{2g+1}z + ... + f_1xz^{2g+1} + f_0z^{2g+2}$ полином којим дефинишемо хиперелиптичку криву $C : y^2 = F(x,z)$. Тада тачке $[x_0, y_0, z_0] \in C(K)$ за које је $z_0 \neq 0$ могу да се преставе у облику $[x_1, y_1, 1]$, при чему онда важи $y_1^2 = f(x_1)$. Одавде видимо да све овакве тачке на кривој $C$ одговарају некој $K$-рационалној тачки на кривој $y^2 = f(x)$ која представља криву у стандардном афином делу отежињене пројективне равни. Зато ћемо за овакву тачку писати само $(x_1, y_1)$.

Иако преостале тачке можемо добити преласком у други стандардни афини део (где је $x_0 \neq 0$), ипак ове тачке, за које је $z_0 = 0$ и можемо да изаберемо произвољно $x$, где бирамо $x_1 = 1$, називамо *тачкама у бесконачности криве* $C$. Овим поступком, једначина се своди на $y^2 = f_{2g+2}$, где настаје неколико случајева. Најлакши случај је када је $f_{2g+2} = 0$ и сада мора бити $y = 0$, одакле закључујемо да ако се једначина у афином делу своди на једначину непарног степена, крива има тачно једну тачку у бесконачности - $[1, 0, 0]$. Ако је $f_{2g+2} \neq 0$, тј. ако се афина једначина своди на једначину парног степена, имамо два подслучаја. Први случај је да је $f_{2g+2}$ квадрат у пољу $K$ и тада имамо две тачке у бесконачности - $[1, \pm s, 0]$, где је $s \in K$ такво да $(\pm s)^2 = f_{2g+2}$. Ове тачке означавамо са $\infty_{\pm s}$. Ако $f_{2g+2}$ није квадрат у пољу $K$, онда у овом случају не постоје тачке у бесконачности, али ће постојати над раширењем поља $K$ степена 2 - $K(\sqrt{f_{2g+2}})$.

**Пример 11.** Афине једначине хиперелиптичких кривих се већ виде из дефиниције. Овде наводимо неке примере, а у свим примерима је $K = \mathbb{Q}$:
1) $C : y^2 = x^5 + 1$. У овом случају је $g = 2$, пројективни облик једначине је $y^2 = x^5z + z^6$ и ова крива има само једну бесконачну тачку $\infty = [1, 0, 0]$. Лако се уочавају још три рационалне афине тачке $(0, 1)$, $(0, -1)$ и $(-1, 0)$. У ствари, важи

$$C(\mathbb{Q}) = \{(0, 1), (0, -1), (-1, 0), \infty\}.$$

Касније у раду ћемо доказати ову чињеницу.
2) $C : y^2 = x(x-1)(x-2)(x-5)(x-6)$. У даљем тексту ћемо доказати

да ова једначина има тачно 10 рационалних решења.
3) $C : y^2 = x(x-3)(x-4)(x-6)(x-7)$. У даљем тексту ћемо доказати да ова једначина има тачно 6 рационалних решења.
4) $C : y^2 = x^6+8x^5+22x^4+22x^3+5x^2+6x+1$. Ево и једне криве парног афиног степена. Она има две рационалне тачке у бесконачности, јер је водећи коефицијент 1 квадрат у $\mathbb{Q}$. И ову једначину ћемо решити касније у раду.

Уводимо још два битна пресликавања хиперелиптичких кривих, и наводимо са доказом две важне теореме. Видећемо да докази, иако различитих тврђења, користе сличне идеје.

**Дефиниција 11.** *Хиперелиптичка инволуција* $\iota_C = \iota$ криве $C$ је пресликавање које тачке криве $[x_0, y_0, z_0] \in C$ пресликава у $[x_0, -y_0, z_0]$.

Видимо да је $\iota : C \longrightarrow C$ нетривијалан аутоморфизам криве $C$. Фиксне тачке овог пресликавања су тачке код којих је $y_0 = 0$, тј. тачке облика $[x_0, 0, z_0]$, при чему су тада $[x_0, z_0] \in \mathbb{P}^1$ корени хомогеног полинома $F(x, z)$. Овакве тачке нас мотивишу да посматрамо и друго пресликавање.

**Дефиниција 12.** *Хиперелиптичко количничко пресликавање* $\pi = \pi_C : C \longrightarrow \mathbb{P}^1$ је пресликавање које тачке криве $[x_0, y_0, z_0] \in C$ пресликава у $[x_0, z_0]$.

Пресликавање $\pi : C \longrightarrow \mathbb{P}^1$ је добро дефинисано, јер проблематична тачка $[0, 1, 0]$ не припада кривој $C$. Ово пресликавање је скоро свуда „2-на-1", сем у тачкама које су нуле хомогеног полинома $F(x, z)$. То су фиксне тачке пресликавања $\iota$ и називају се *тачке рамификације пресликавања* $\pi$.

**Теорема 6.** Нека је $C : y^2 = F(x, z)$ хиперелиптичка крива над пољем $K$ и нека је $P = [x_0, y_0, z_0] \in C(K)$ тачка на њој. Тада је локални прстен $\mathcal{O}_{C,P}$ је прстен дискретне валуције чије је поље разломака $K(C)$.

**Доказ.** Пре самог доказа, наводимо један познат пример прстена дискретне валуације, то је прстен формалних степених редова над било којим пољем $K$, који се означава са $K[[t]]$. Његови елементи

су формални степени редови $\sum_{n=0}^{+\infty} a_n t^n$, где су коефицијенти $a_n \in K$. Реч формални овде означава да сабирамо и множимо редове на уобичајени начин, без вођења рачуна о конвергенцији. Рутински се проверава да је $K[[t]]$ прстен дискретне валуације ако уведемо валуацију $v$ на следећи начин

$$v\left(\sum_{n=0}^{+\infty} a_n t^n\right) = \min\{n \geq 0 \mid a_n \neq 0\}.$$

При тој провери користимо чињеницу да је степени ред инвертибилан ако и само ако му је константан члан $a_0 \neq 0$ (у том случају можемо лако уочити да су коефицијенти његовог инверзног степеног реда количник полинома по коефицијентима степеног реда са $a_0$, што остаје у пољу, а ако је $a_0 = 0$ не постоји инверзни степени ред). Сада крећемо са доказом теореме.

Можемо да претпоставимо $z_0 = 1$, тј. да је тачка $P = (x_0, y_0)$ део стандардне афине равни (случај $x_0 = 1$ доказујемо на потпуно исти начин) и посматрамо $C$ као афину криву. Разликујемо два случаја.

Нека је прво $y_0 \neq 0$. Конструисаћемо $K$-линеарни хомоморфизам прстена $\alpha : K[C] \longrightarrow K[[t]]$. Како је $K[C] = K[x, y]/\langle y^2 - f(x)\rangle$, довољно је пресликати $x$ и $y$, само морамо да водимо рачуна да тада буде $f(\alpha(x)) = \alpha(y)^2$. Послаћемо $x$ у $x_0 + t$ и $y$ у степени ред са константним чланом $y_0$ тако да испунимо услов $f(\alpha(x)) = \alpha(y)^2$. Ево зашто то можемо да урадимо. Треба проверити да ли је $f(x_0 + t) = (y_0 + a_1 t + a_2 t^2 + ...)^2$, за неке $a_1$, $a_2$, ... елементе поља $K$. Полином је бесконачно глатка функција, па можемо да развијемо $f(x_0 + t)$ у Тејлоров ред (који ће у овом случају бити и коначан, али то није важно). Тада

$$f(x_0 + t) = f(x_0) + f'(x_0)t + \frac{f''(x_0)t}{2} + ... = y_0^2 + b_1 t + b_2 t^2 + ... =$$

$$= (y_0 + a_1 t + a_2 t^2 + ...)^2$$

за неке $b_1$, $b_2$, ... елементе поља $K$, док тражимо $a_1$, $a_2$, ... Када распишемо коефицијенте уз $t^n$ добијамо услов $2y_0 a_n = ...$, где је на

десној страни израз од познатих бројева и пошто је $y_0 \neq 0$, редом одређујемо бројеве $a_n$. Дакле, конструисали смо $K$-линеарни хомоморфизам прстена $K[x,y]$ у $K[[t]]$, у чијем језгру је полином $y^2 - f(x)$. Зато, овај хомоморфизам индукује тражени хомоморфизам $\alpha : K[C] = K[x,y]\,\langle y^2 - f(x)\rangle \longrightarrow K[[t]]$.

Нека је $\phi \in K[C]$ произвољна функција. По дефиницији $K[C]$ се може представити у облику $\phi = f_1(x) + f_2(x)y$, где $f_1, f_2 \in K[x]$ (јер је $y^2 = f(x)$ на $C$). Сада је $\phi(P) = f_1(x_0) + f_2(x_0)y_0$. Са друге стране,

$$\alpha(\phi) = \alpha(f_1(x) + f_2(x)y) = \alpha(f_1(x)) + \alpha(f_2(x))\alpha(y) =$$

$$= f_1(\alpha(x)) + f_2(\alpha(x))\alpha(y) =$$

$$= f_1(x_0+t)+f_2(x_0+t)(y_0+a_3(t)) = f_1(x_0)+a_1(t)+(f_2(x_0)+a_2(t))(y_0+a_3(t)) =$$

$$= f_1(x_0) + f_2(x_0)y_0 + a(t) = \phi(P) + a(t),$$

где су $a(t)$, $a_1(t)$, $a_2(t)$, $a_3(t)$ неки степени редови по $t$ у $K$ који немају константан члан. Одавде закључујемо да је константан члан степеног реда $\alpha(\phi)$ управо $\phi(P)$. Како знамо да је степени ред инвертибилан ако и само ако му је константан члан различит од нуле, то су слике $\alpha(\phi)$ инвертибилне за све $\phi$ такве да је $\phi(P) \neq 0$, одакле можемо да проширимо хомоморфизам $\alpha : K[C] \longrightarrow K[[t]]$ на $\alpha : \mathcal{O}_{C,P} \longrightarrow K[[t]]$. Знамо да је $K[[t]]$ прстен дискретне валуације, са валуацијом $v$, док то треба да докажемо за прстен $\mathcal{O}_{C,P}$ и природно је дефинисати валуацију на $\mathcal{O}_{C,P}$ са $v_P = v \circ \alpha$. Да бисмо доказали да је $\mathcal{O}_{C,P}$ прстен дискретне валуације, треба да докажемо три ствари:

1) $v_P$ је валуација:
а) $v_P(\phi) = \infty \iff v \circ \alpha(\phi) = 0 \iff \alpha(\phi) = 0 \iff \phi = 0$, јер је $\alpha$ „1-1" по конструкцији. Овде свака нула има значење нуле у свом простору, прва нула је заиста нула, друга је нула степени ред, а треће је нула функција у $\mathcal{O}_{C,P}$.
б) $v_P(\phi_1\phi_2) = v\circ\alpha(\phi_1\phi_2) = v(\alpha(\phi_1)\alpha(\phi_2)) = v(\alpha(\phi_1))v(\alpha(\phi_2)) = v_P(\phi_1)v_P(\phi_2)$;
в) $v_P(\phi_1+\phi_2) = v\circ\alpha(\phi_1+\phi_2) = v(\alpha(\phi_1)+\alpha(\phi_2)) \geq \min\{v(\alpha(\phi_1)), v(\alpha(\phi_2))\} = \min\{v_P(\phi_1), v_P(\phi_2)\}$.

2) Ако је за неко $\phi \in \mathcal{O}_{C,P}$ $v(\phi) = 0$, тада је $\phi^{-1} \in \mathcal{O}_{C,P}$.

Ово следи одмах, јер $v(\phi) = 0$ значи да је константан члан степеног реда $\alpha(\phi)$ различит од нуле, а то је управо $\phi(P) \neq 0$, одакле $\phi^{-1} \in \mathcal{O}_{C,P}$.

3) Идеал $\{\phi \in \mathcal{O}_{C,P} \mid v(\phi) > 0\} = \{\phi \in \mathcal{O}_{C,P} \mid \phi(P) = 0\} = \mathfrak{m}_P$ је главни, тј. генерисан једним елементом. Доказаћемо да је $\mathfrak{m}_P$ генерисан са $x - x_0$.

Потребно и довољно је да докажемо да за $h \in K[x, y]$ које гледамо по модулу $y^2 - f(x)$ за које је $h(P) = 0$ важи да $h \in (x - x_0) \cdot \mathcal{O}_{C,P}$. Како можемо све степене $y$ веће од два да смањимо користећи полином по $x$, претпостављамо да је $h(x, y) = h_1(x) + h_2(x)y$, где су $h_1, h_2 \in K[x]$. Њему придружимо полином $\overline{h}(x, y) = h_1(x) - h_2(x)y$. Ако је $\overline{h}(P) = 0$ такође, тада имамо две једнакости: $h_1(x_0) + h_2(x_0)y_0 = 0$ и $h_1(x_0) - h_2(x_0)y_0 = 0$. Пошто је $y_0 \neq 0$, одавде следи да је $h_1(x_0) = h_2(x_0) = 0$, односно да $x - x_0 \mid h_1(x)$ и $x - x_0 \mid h_2(x)$, а одавде и $x - x_0 \mid h$, што и желимо да покажемо. На даље претпостављамо $\overline{h}(P) \neq 0$. Помножимо ли $h$ и $\overline{h}$ добијамо полином $h_1^2(x) - h_2^2(x)y^2 = h_1^2(x) - h_2^2(x)f(x)$. Убацимо $x = x_0$ и $y = y_0$ у овај израз и добијамо

$$0 = (h_1(x_0) + h_2(x_0)y_0)((h_1(x_0) - h_2(x_0)y_0)) = h_1^2(x_0) - h_2^2(x_0)f(x_0).$$

Ово значи да је $x_0$ нула полинома (по $x$!) $h_1^2(x) - h_2^2(x)f(x)$, одакле $x - x_0$ дели тај полином. Запишимо једнакост

$$(x - x_0)P(x) = h_1^2(x) - h_2^2(x)f(x) =$$

$$= (h_1(x) + h_2(x)y)(h_1(x) - h_2(x)y) = h(x, y)\overline{h}(x, y).$$

Пошто $\overline{h}(P) \neq 0$, одатле $\overline{h}^{-1} \in \mathcal{O}_{C,P}$, па једнакост изнад можемо поможити са $\overline{h}^{-1}$, одакле добијамо

$$h(x, y) = (x - x_0)P(x)\overline{h}^{-1}(x, y),$$

при чему је $P(x)\overline{h}^{-1}(x, y) \in \mathcal{O}_{C,P}$, одакле добијамо оно што је требало доказати. Како услов $\phi \in \mathfrak{m}_P$ значи да се $\phi$ може записати као количник полинома $\frac{h(x,y)}{g(x,y)}$, при чему $h(P) = 0$ и $g(P) \neq 0$, закључујемо да $\phi \in (x - x_0) \cdot \mathcal{O}_{C,P}$, што завршава доказ.

Остаје још случај $y_0 = 0$. Опет тражимо $K$-линеарни хомоморфизам прстена $K[C] \longrightarrow K[[t]]$, али ћемо га сада мало другачије конструисати. Желимо да $x$ оде у степени ред са само парним члановима и константним чланом $x_0$, а да $y$ пошаљемо у $t$. Овде треба да проверимо да ли ће бити испуњено $t^2 = f(x_0 + a_2t^2 + a_4t^4 + ...)$, за неке $a_2$, $a_4$, ... елементе поља $K$. Тејлорова формула нам даје $f(x_0 + a) = f(x_0)'a + ...$, јер $f(x_0) = 0$ и пошто $f$ нема двоструке нуле, $f'(x_0) \neq 0$. Применом на $a = a_2t^2 + a_4t^4 + ...$ добијамо

$$t^2 = f'(x_0)(a_2t^2 + a_4t^4 + ...) + \frac{f''(x_0)}{2}(a_2t^2 + a_4t^4 + ...)^2 + ...)^2$$

одакле ћемо при посматрању $t^2n$ добити једначину облика $f'(x_0)a_{2n} = ...$, где је са десне стране израз по познатим бројевима. Овим поступком налазимо све $a_{2n}$ и завршавамо конструкцију хомоморфизма $\alpha : K[x, y] \longrightarrow K[[t]]$, а онда аналогно као у првом случају проширујемо на $\alpha : \mathcal{O}_{C,P} \longrightarrow K[[t]]$.

При томе, једино што се разликује је провера да је константан члан слике $\alpha(\phi)$ опет $\phi(P)$, за $\phi \in K[C]$ и то се проверава на следећи начин. Нека је $\phi = f_1(x) + f_2(x)y$, за неке $f_1, f_2 \in K[x]$. Сада је $\phi(P) = f_1(x_0)$. Са друге стране је $\alpha(y) = t$, па

$$\alpha(\phi) = \alpha(f_1(x) + f_2(x)y) =$$

$$= f_1(\alpha(x)) + f_2(\alpha(x))t = f_1(x_0 + a(t)) + b(t) = f_1(x_0) + c(t),$$

где су $a(t)$, $b(t)$ и $c(t)$ степени редови по $t$ у $K$ који немају константан члан, при чему није ни било потребе да рачунамо $f_2(\alpha(x))$ јер се то одмах множи са $t$. Валуацију дефинишемо на исти начин као у претходном случају $v_P = v \circ \alpha$ и исто се проверава све из претходног случаја сем тога да је $\mathfrak{m}_P$ главни идеал.

Доказаћемо да је $\mathfrak{m}_P$ генерисан са $y$. Опет је довољно доказати да ако за полином $h \in K[x, y]$, по модулу $y^2 - f(x)$ важи $h(P) = 0$, да тада $y$ „дели" $h$. Полином $f(x)$ је дељив са $x - x_0$, јер је $x_0$ његова нула, одакле $f(x) = (x - x_0)f_1(x)$, за неко $f_1 \in K[x]$. Када то заменимо у једначину криве добијамо $y^2 = (x - x_0)f_1(x_0)$.

Пошто је $f$ бесквадратан полином, то је $f_1(x_0) \neq 0$, а самим тим и $f_1(P) \neq 0$, одакле $f_1^{-1} \in \mathcal{O}_{C,P}$. Дакле, $x - x_0 = y \cdot p(x, y)$,

за неко $p(x,y) \in \mathcal{O}_{C,P}$. На даље, функцију $h$ можемо записати у облику $h(x,y) = h_1(x) + h_2(x)y$, за неке $h_1, h_2 \in K[x]$. Услов да је $h(P) = h(x_0, 0) = 0$ је еквивалентан са $h_1(x_0) = 0$, а ово значи да је $h(x)$ дељиво са $x - x_0$. Пошто знамо да је $x - x_0$ „дељиво" са $y$, завршавамо доказ

$$h(x,y) = h_1(x) + h_2(x)y = (x - x_0)h_3(x) + h_2(x)y = y(p(x,y)h_3(x) + h_2(x)),$$

јер је $p(x,y)h_3(x) + h_2(x) \in \mathcal{O}_{C,P}$. Овим су испитани сви случајеви и проверене све могућности, те је ово крај целог доказа да је $\mathcal{O}_{C,P}$ прстен дискретне валуације.

Остаје још да докажемо да је количничко поље $\mathcal{O}_{C,P}$ баш цело $K(C)$. Јасно је да је садржано у њему. Са друге стране, пошто за генераторе $K(C)$ важи $x, y \in \mathcal{O}_{C,P}$ (за случај $z_0 = 1$, аналогно се ради за $x_0 = 1$), добијамо и обрнуту инклузију.

**Коментар:** Из доказа теореме се види резултат примера број 3, као и то колико је потребно уложити труда у овај доказ. У ознакама из примера, ако је $P = (\alpha, \beta)$, тада за $\beta \neq 0$, равномернизатор за $P$ је $x - \alpha$, док за $\beta = 0$ узимамо $y$. У афиним ознакама, где користимо координатне функције $x$ и $y$, равномернизатор бесконачне тачке је $\frac{1}{x}$, када је у питању једначина парног степена, док за непаран степен једначине можемо узети функцију $\frac{x^g}{y}$ или $\frac{y}{x^{g+1}}$.

За крај овог дела, наводимо тврђење које ћемо користити у следећем поглављу, али да би оно постало тачно, морамо отићи у мало веће поље. Уместо $K$ радићемо у $\overline{K}$, алгебарском затворењу поља $K$.

**Теорема 7.** Нека је $C : y^2 = f(x)$ задата афином једначином и $\phi \in \overline{K}(C)^*$. Тада $\phi$ има једнак број нула и полова, рачунатих са одговарајућом вишеструкошћу.

**Доказ.** За почетак, подсетимо се да је $\overline{K}(C)$ количничко поље прстена $\overline{K}[x,y]/\langle y^2 - f(x)\rangle$, одакле се свака функција $\phi \in \overline{K}(C)$ може записати као $\phi = h_1(x) + h_2(x)y$, за неке $h_1, h_2 \in \overline{K}(x)$. За функуцију $\phi$, означимо са $N_\phi$ број њених нула и са $P_\phi$ број њених полова, све са вишеструкошћу. Треба да докажемо да је $N_\phi - P_\phi = 0$.

Функцији $\phi$, придружујемо и две функције. Прва функција је $\iota^*\phi = \phi \circ \iota$, где је $\iota$ афина хиперелиптичка инволуција, која слика $(x, y)$ у $(x, -y)$. Сада је по конструкцији јасно да је $N_{\iota^*\phi} = N_\phi$ и $P_{\iota^*\phi} = P_\phi$. Друга функција коју уочавамо је $\Phi = \phi \cdot \iota^*\phi$. По дефиницији, функције $\Phi$ је $N_\Phi = 2N_\phi$ и $P_\Phi = 2P_\phi$, одакле је $N_\Phi - P_\Phi = 0$ ако и само ако је $N_\phi - P_\phi = 0$, па је довољно доказати тврђење за функцију $\Phi$.

Како је $\phi = h_1(x) + h_2(x)y$, закључујемо да је $\iota^*\phi = h_1(x) - h_2(x)y$, одакле је

$$\Phi = h_1(x)^2 - h_2(x)^2y^2 = h_1(x)^2 - h_2(x)^2 f(x) \in \overline{K}(x).$$

Дакле, $\Phi$ је функција само по $x$ и када тражимо нуле и полове, треба да је вратимо у пројективни облик, а то ћемо урадити тако што ћемо прво $\Phi$ написати као количник два полинома по $x$, а онда хомогенизовати изразе са неодређеном $z$ и то тако да добијемо да су оба хомогена полинома истог степена, јер на овај начин добијамо добро дефинисану функцију на $\mathbb{P}^1$.

Када скратимо исте факторе, што можемо јер живимо у алгебарском затворењу $\overline{K}$, остаје нам да је пројективни облик функције $\Phi = \frac{F(x,z)}{G(x,z)}$, где $F$ и $G$ немају заједничких фактора и истог су степена $d$. Тада су све нуле функције $\Phi$ у ствари нуле полинома $F(x, z)$, којих има, рачунајући вишеструкост $d$ и сви полови функције $\Phi$ нуле полинома $G(x, z)$, којих такође има $d$, рачунајући вишеструкост. Овим смо показали да тврђење важи за функцију $\Phi$, што нам је довољно да докажемо да тврђење важи и за произвољну функцију $\phi$.

**Препоручена литература до краја друге главе:** Текст који се овде налази је комбинација више материјала од којих је сваки сем [51] погодан за прво читање, а то су [23], [22], [20], [53], [21].

## 2.3 Дивизори

У овом поглављу ћемо проширити поље $K$ до његовог алгебарског затворења $\overline{K}$ и посматраћемо криве над $\overline{K}$. Нека је $C$ глатка крива дефинисана над $K$, тј. полином који је дефинише је из $K[x, y]$ или $K[x, y, z]$, у зависности од тога да ли је афини или

пројективни случај, али са уоченим свим тачкама у $\overline{K}$. Дивизор је згодан објекат, зато што у исто време налази све нуле и полове функције и то са њиховом вишеструкошћу, јер се испоставља да независно тражење нула и полова или само бројање нула и полова нису довољно јаке информације, већ да их треба груписати заједно.

**Дефиниција 13.** *Дивизор* на кривој $C$ је формална $\mathbb{Z}$-линеарна комбинација коначно тачака са криве $C$. Дакле, сваки дивизор $D$ се представља у облику коначног збира

$$D = \sum_{P \in C(\overline{K})} n_P P,$$

где су сви $n_P \in \mathbb{Z}$ и само њих коначно много није нула. Скуп свих дивизора се означава са $\mathrm{Div}(C)$. *Степен* дивизора $D$ је збир његових коефицијената, тј. $\deg D = \sum_{P \in C(\overline{K})} n_P$. Посебно се издвајају дивизори који је степен нула, скуп свих оваквих дивизора се назива, како му и име каже, *скуп дивизора степена нула* и означава се са $\mathrm{Div}^0(C)$. Ако за свако $P \in C(\overline{K})$ важи $n_P \geq 0$, дивизор се назива *позитиван* или *ефективан*. *Носач дивизора* $D$ је скуп тачака $P \in C(\overline{K})$ за које је $n_P \neq 0$, тј. скуп тачака које се стварно појављују у запису дивизора $D$ и означава се $\mathrm{supp}(d)$.

Из дефиниције видимо да је скуп свих дивизора једна комутативна група, да је по дефиницији за два дивизора $\deg(D_1 + D_2) = \deg D_1 + \deg D_2$, одакле скуп дивизора степена нула формира једну његову подгрупу. На скупу дивизора можемо да уведемо једну релацију парцијалног поретка где ће бити $D_1 \leq D_2$ ако и само ако је $D_2 - D_1$ позитиван дивизор.

**Дефиниција 14.** Свакој функцији $f \in \overline{K}(C)^*$ можемо придружити дивизор, *дивизор функције* $f$ са

$$\mathrm{div}(f) = \sum_{P \in C(\overline{K})} \mathrm{ord}_P(f) P.$$

Свака функција $f \in \overline{K}(C)^*$ има коначан број нула и полова, одакле је дивизор функције $f$ заиста добро дефинисан. Ово додељивање можемо шватити и као пресликавање $\operatorname{div} : \overline{K}(C)^* \longrightarrow \operatorname{Div}(C)$. Како је $\operatorname{ord}_P(f \cdot g) = \operatorname{ord}_P(f) + \operatorname{ord}_P(g)$, онда је ово пресликавање и хомоморфизам комутативних група. Пошто знамо да свака функција $f \in \overline{K}(C)^*$ има једнак број нула и полова, закључујемо да је $\deg(\operatorname{div}(f)) = 0$, односно да $\operatorname{div}(\overline{K}(C)^*)$ је подгрупа од $\operatorname{Div}^0(C)$. Из дефиниције видимо и да је $\operatorname{div}(f^{-1}) = -\operatorname{div}(f)$. Још можемо да приметимо и да је за произвољне $f, f' \in \overline{K}(C)$

$$\operatorname{div}(f + f') \geq \sum_{P \in C(\overline{K})} \min\{\operatorname{ord}_P(f), \operatorname{ord}_P(f')\}P.$$

**Пример 12.** Рационалној функцији $f = \frac{xy^2}{(x-y)^3}$ на $\mathbb{P}^1$ придружујемо дивизор $\operatorname{div}(f) = [0,1] + 2[1,0] - 3[1,1]$.

**Пример 13.** Нека је $C : y^2 = f(x)$ глатка крива над $K$, елиптичка или хиперелиптичка. Желимо да одредимо дивизоре координатних функција $x$ и $y$. Због различитог броја тачака у бесконачности, у зависности од тога да ли је $\deg f$ паран или непаран, разликујемо два случаја.

Ако је $\deg f = 2g + 1$, тада из примера број 3 (односно теореме број 6) налазимо

$$\operatorname{div}(x) = (0, \sqrt{f(0)}) + (0, -\sqrt{f(0)}) - 2\infty;$$

$$\operatorname{div}(y) = \sum_{\alpha : f(\alpha) = 0} (\alpha, 0) - (2g+1)\infty.$$

Ако је $\deg f = 2g + 2$, тада у $\overline{K}$ постоји $s$ такво да је $f_{2g+2} = s^2$, па из примера број 3 (односно теореме број 6) налазимо

$$\operatorname{div}(x) = (0, \sqrt{f(0)}) + (0, -\sqrt{f(0)}) - \infty_s - \infty_{-s};$$

$$\operatorname{div}(y) = \sum_{\alpha : f(\alpha) = 0} (\alpha, 0) - (g+1)\infty_s - (g+1)\infty_{-s}.$$

**Пример 14.** Овај пример је мало конкретнији претходни пример, додуше у пројективном запису. Нека је $C : y^2z = x^3 + xz^2$ пројективни запис глатке елиптичке криве $y^2 = x^3 + x$. Одредимо $\mathrm{div}(\frac{y}{z})$. Рачунањем у пројективним координатама видимо да ако је $y = 0$ имамо $x(x^2 + z^2) = 0$, што нам даје три пројективне тачке $[0, 0, 1]$, $[i, 0, 1]$, $[-i, 0, 1]$, где је, наравно $i$ ознака за број чији је квадрат $-1$. Овде већ видимо потребу да проширимо поље $K$ на његово алгебарско затворење $\overline{K}$, без тога не бисмо могли да видимо све нуле функција, а онда немамо довољно информација за даље изучавање кривих!

Са друге стране, ако је $z = 0$, из једначине видимо да мора бити и $x = 0$, што нам даје само једну пројективну тачку $[0, 1, 0]$. Ово се слаже са нашим афиним разматрањима, прве три набројане тачке су афине, јер $z \neq 0$, и ту афино $y$, што је пројективно записано управо функција $\frac{y}{z}$ има нуле реда 1. Тачка $[0, 1, 0]$ представља јединствену бесконачну тачку, за коју знамо да афино $y$ има пол реда 3 (а то можемо и да видимо због тога што је степен главног дивизора нула, а знамо да имамо три нуле реда 1). Дакле,

$$\mathrm{div}\left(\frac{y}{z}\right) = [0, 0, 1] + [i, 0, 1] + [-i, 0, 1] - 3[0, 1, 0].$$

Да $z$ има нулу реда 3 у тачки $\infty = [0, 1, 0]$ могли смо да видимо и из пројективног записа, коришћењем једначине, особине валуације и познавања тога да $x$ где се аналура има нулу реда 1. Постхо се $y$ не поништава у тој тачки, имамо $\mathrm{ord}_\infty(y^2z) = \mathrm{ord}_\infty(z)$. За десну страну једначине имамо $ord_\infty(x^3) = 3$ и $\mathrm{ord}_\infty(xz^2) = 1 + 2\,\mathrm{ord}(z)$ Дакле, $\mathrm{ord}_\infty(x^3 + xz^2) \geq 1$, одакле је $\mathrm{ord}_\infty(z) \geq 1$. Сада не може бити $\mathrm{ord}_\infty(z) > 3$, јер би тада за десну страну важило $\mathrm{ord}_\infty(x^3 + xz^2) = \min\{\mathrm{ord}_\infty(x^3), \mathrm{ord}_\infty(xz^2)\} = 3 < \mathrm{ord}_\infty(z)$, а такође не може ни бити $\mathrm{ord}_\infty(z) < 3$, јер би тада десна страна имала већи поредак $\mathrm{ord}_\infty(x^3 + xz^2) \geq \min\{\mathrm{ord}_\infty(x^3), \mathrm{ord}_\infty(xz^2)\} = 3$. Дакле, $\mathrm{ord}_\infty(z) = 3$.

**Важно!** Овакво пројективно закључивање можемо да примењујемо само у случају елиптичких кривих, јер у случају хиперелиптичких кривих посматрамо отежињену пројективну раван, а не обичну и онда хомогенизацију вршимо другачије!

**Дефиниција 15.** Дивизор $D \in \mathrm{Div}(C)$ је *главни* ако је облика $D = \mathrm{div}(f)$, за неко $f \in \overline{K}(C)^*$. Два дивизора су *линеарно еквивалентна*

ако се разликују за главни дивизор (тј. пишемо $D_1 \sim D_2$ ако и само ако је $D_1 - D_2$ главни дивизор). *Пикарова група* криве $C$ је количничка група $\mathrm{Div}(C)$ посечена са групом главних дивизора, коју означавамо са $\mathrm{Pic}(C)$. Пошто знамо да су главни дивизори степена нула, можемо да дефинишемо и *Пикарову групу степена нула* која се добије када се група $\mathrm{Div}^0(C)$ посече по групи главних дивизора, коју означавамо са $\mathrm{Pic}^0(C)$.

**Пример 15.** Приметимо да је на елиптичкој кривој из претходног примера $C : y^2z = x^3 + xz$ дивизор $D = 2[0,0,1] - 2[0,1,0]$ главни. Већ смо видели у претходном примеру да $z$ има нулу реда 3 у тачки $[0,1,0]$. Али, у $D$ се ова тачка појављује са вишеструкошћу два, одакле морамо да склонимо једну овакву тачку. Логичан покушај је да пробамо са функцијом $x$ која се исто анулира ту и знамо да је реда 1. Друга тачка где се $x$ анулира јесте $[0,0,1]$. То је афина тачка за коју знамо да, пошто се и $y$ у њој анулира, да је $y$ реда 1, а $x$ реда 2, баш као што нам и треба. Према томе $\mathrm{div}(\frac{x}{z}) = 2[0,0,1] - 2[0,1,0]$, а функција $\frac{x}{z}$ је свакако функција из $K(C)$.

**Пример 16.** Иако није сваки дивизор степена 0 уједно и главни (на пример, може се показати да на елиптичкој кривој за две различите тачке $P$ и $Q$ важи да дивизор $D = P - Q$ није главни), на пројективној правој $\mathbb{P}^1$ јесте сваки дивизор степена нула главни. Нека је $D = \sum n_P P$ дивизор степена 0. Свака тачка $P \in \mathbb{P}^1$ се записује у облику $[\alpha_P, \beta_P]$. Зато видимо да је дивизор $D$ у ствари дивизор функције

$$\prod_{P : n_P \neq 0} (\beta_P x - \alpha_P y)^{n_P},$$

која је добро дефинисана на $\mathbb{P}^1$ баш због услова да је $\sum n_P = 0$. Према томе, закључујемо да подгрупа $\mathrm{Div}^0(\mathbb{P}^1)$ групе $\mathrm{Div}(\mathbb{P}^1)$ се састоји управо од главних дивизора, а пошто је $\mathrm{Div}(\mathbb{P}^1)/\mathrm{Div}^0(\mathbb{P}^1) \cong \mathbb{Z}$, закључујемо да је $\mathrm{Pic}(\mathbb{P}^1) \cong \mathbb{Z}$ и $\mathrm{Pic}^0(\mathbb{P}^1)$ је тривијална група.

**Дефиниција 16.** Дејство Галуаове групе $\mathcal{G}_{\overline{K}/K}$ на дивизор $D = \sum_{P \in C(\overline{K})} n_P P$ дефинишемо на очигледан начин, за $\sigma \in \mathcal{G}_{\overline{K}/K}$

$$D^\sigma = \sum_{P \in C(\overline{K})} n_P P^\sigma.$$

Дивизор $D \in \mathrm{Div}(C)$ је *дефинисан над* $K$ или $K$*-рационалан* ако је фиксиран дејством Галуаове групе $\mathcal{G}_{\overline{K}/K}$, тј. ако важи $D^\sigma = D$, за све $\sigma \in \mathcal{G}_{\overline{K}/K}$. Скуп оваквих дивизора означавамо са $\mathrm{Div}_K(C)$. Аналогно се дефинишу и скупови $\mathrm{Div}_K^0(C)$, $\mathrm{Pic}_K(C)$, $\mathrm{Pic}_K^0(C)$.

**Пример 17.** Нека је $C : y^2 = f(x)$ глатка крива над $K$. Тада је за свако $x_0 \in K$, дивизор $D_{x_0} = (x_0, y_0) + (x_0, -y_0)$, где су $\pm y_0 \in \overline{K}$ корени броја $f(x_0)$, $K$-рационалан. Ако су $\pm y_0 \in K$, онда су обе тачке у $D$ фиксиране при дејству сваког $\sigma \in \mathcal{G}_{\overline{K}/K}$, док у супротном, или их $\sigma$ обе фиксира или шаље једну у другу.

Дакле, примећујемо да дивизор може бити фиксиран дејством сваког $\sigma \in \mathcal{G}_{\overline{K}/K}$, а да му тачке нису фиксиране, довољно је да се претумбају тако да увек остане исти збир тачака, тј. исти дивизор. Такође, пошто је Галуаова група изузетно компликован објекат, видимо да је довољно да узмемо раширење поља $K$ које садржи све тачке из носача дивизора $D$ и посматрамо Галуаову групу његовог Галуаовог затворења над $K$ (она ће бити коначна).

**Пример 18.** Сви дивизори облика $D_{x_0}$ из претходног примера су линеарно еквивалентни. Уочимо $x_0, x_0' \in K$. Тада функције $x - x_0, x - x_0' \in K(C)$ имају исти пол у бесконачности (пол реда 2 у једној бесконачност у непарном случају и два пола реда 1 у две бесконачности у парном случају). Зато ће се информације о овим половима у њиховим дивизорима пократити, одакле остаје

$$\mathrm{div}\left(\frac{x - x_0}{x - x_0'}\right) = (x_0, y_0) + (x_0, -y_0) - (x_0', y_0') + (x_0', -y_0') = D_{x_0} - D_{x_0'}.$$

Пошто се $D_{x_0}$ и $D_{x_0'}$ разликују за дивизор функције из $K(C)$, они су линеарно еквивалентни.

**Тврђење 8.** Нека је $f \in \overline{K}(C)^*$. Тада је еквивалентно:
(1) $\mathrm{div}(f) \geq 0$;
(2) $f$ је константна ненула функција;
(3) $\mathrm{div}(f) = 0$.

**Доказ.** Јасно је да (2) повлачи и (1) и (3). Нека је $\mathrm{div}(f) \geq 0$ или $\mathrm{div}(f) = 0$. Ово значи да функција $f$ нема полове, па по тврђењу број 3 је она константна.

**Тврђење 9.** Нека су $f, g \in \overline{K}(C)^*$. Тада је $\mathrm{div}(f) = \mathrm{div}(g)$ ако и само ако постоји $c \in \overline{K}$ такво да је $g = cf$.

**Доказ.** Услов $\mathrm{div}(f) = \mathrm{div}(g)$ је еквивалентан са $\mathrm{div}(\frac{f}{g}) = 0$, а по претходном тврђењу то је еквивалентно са тим да је $\frac{f}{g}$ константна функција.

За крај овог излагања наводимо нека својства релације $\sim$ која се веома једноставно доказују.

**Тврђење 10.** (1) Релација $\sim$ је релација еквиваленције на скупу $\mathrm{Div}(C)$.
(2) За $D \in \mathrm{Div}(C)$ важи $D \sim 0$ ако и само ако постоји $f \in \overline{K}(C)$ такво да $D = \mathrm{div}(f)$.
(3) Ако за $D, D' \in \mathrm{Div}(C)$ важи $D \sim D'$, тада $\deg(D) = \deg(D')$.
(4) Ако за $D_1, D_2, D_1', D_2' \in \mathrm{Div}(C)$ важи $D_1 \sim D_1'$ и $D_2 \sim D_2'$, тада $D_1 + D_2 \sim D_1' + D_2'$.

## 2.4 Простор диференцијала

За значајније резултате нам је потребан што већи математички апарат. За сада смо користили само алгебарске и алгебарско-геометријске методе. У овом делу уводимо аналитичке објекте - диференцирање и диференцијалне форме на кривој. Наравно, пошто нас занима аритметика, нећемо имати услове да користимо лимесе и уводимо диференцијале као формални објекат (слично као и код формалних степених редова, где не проверавамо конвергенцију), али тако да сачувамо она основна својства која смо научили на анализи. Нека је у овом поглављу $K$ и перфектно поље. Ова претпоставка помажу у одређивању сепарабилности (раширења функцијских поља или пресликавања између кривих). Повезаност диференцијала са сепарабилношћу није изненађујућа, јер када проверавамо да ли је неки елемент раширења поља сепарабилан над мањим пољем, проверавамо да ли његов минимални полином узајамно прост са својим изводом. Почињемо са појмом диференцирања.

**Дефиниција 17.** Нека је $C$ крива над пољем $K$. *Диференцирање* на $K(C)$ је $K$-линеарно пресликавање $\delta : K(C) \longrightarrow K(C)$ које задо-

вољава Лајбницово правило, тј. $\delta(f_1 f_2) = f_1\delta(f_2) + f_2\delta(f_1)$, за све $f_1, f_2 \in K(C)$.

**Тврђење 11.** Нека је $\delta : K(C) \longrightarrow K(C)$ произвољно диференцирање. Тада $\delta$ задовољава следећа својства:
(1) За свако $c \in K$ је $\delta(c) = 0$.
(2) За свако $x \in K(C)$ и $n \in \mathbb{N}$ важи $\delta(x^n) = nx^{n-1}\delta(x)$.
(3) Ако је $\operatorname{char} K = p$, тада је $\delta(x^p) = 0$, за свако $x \in K(C)$.
(4) За било које $h \in K(C)$ $\delta'(f) = h \cdot \delta(f)$ је такође диференцирање.
(5) За све $x, y \in K(C)$ је $\delta\left(\dfrac{x}{y}\right) = \dfrac{y\delta(x) - x\delta(y)}{y^2}$.
(6) За све $x, y \in K(C)$ и за произвољан полином $F(u, v) \in K[u, v]$ важи $\delta(F(x, y)) = \dfrac{\partial F}{\partial x}\delta(x) + \dfrac{\partial F}{\partial y}\delta(y)$.

**Доказ.** (1) Због $K$-линеарности, довољно је доказати да је $\delta(1) = 0$, што добијемо када у Лајбницово правило убацимо $f_1 = f_2 = 1$.
(2) Ово се лако изводи индукцијом, убацивањем $f_1 = x^n$ и $f_2 = x$ у Лајбницово правило, а (3) следи из (2).
(4) Јасно се види да $\delta'$ задовољава све што треба.
(5) $\delta(x) = \delta\left(x \cdot \dfrac{y}{x}\right) = \dfrac{y}{x}\delta(x) + x\delta\left(\dfrac{y}{x}\right)$, а када одавде израчунамо $\delta\left(\dfrac{y}{x}\right)$ добијамо тражену формулу.
(6) Нека је $F(u, v) = \sum c_{kl} u^k v^l$. Тада је

$$\delta(F(x, y)) = \sum c_{kl}(kx^{k-1}y^l\delta(x) + lx^k y^{l-1}\delta(y)) =$$

$$= \sum (kc_{kl}x^{k-1}y^l)\delta(x) + \sum (lc_{kl}x^k y^{l-1})\delta(y) = \frac{\partial F}{\partial x}\delta(x) + \frac{\partial F}{\partial y}\delta(y).$$

На даље, бирамо било коју функцију $x \in K(C)$ која задовољава да је раширење $K(C)/K(x)$ коначно и сепарабилно. На пример, такве функције су равномернизатори у произвољној тачки $P \in C$. На $K(x)$ имамо дефинисано диференцирање $\delta(f) = \dfrac{\partial f}{\partial x}$. Желимо да то диференцирање проширимо на цело $K(C)$. Због коначности раширења $K(C)/K(x)$, свака функција $f \in K(C)$ поништава неки полином $F \in K(x)[T]$, одаберимо да $F$ буде баш минимални полином за $f$. Тада је $F \in K[x, T]$, по Гаусовој леми. Пошто је

раширење $K(C)/K(x)$ и сепарабилно, онда је $\dfrac{\partial F}{\partial T} \neq 0$ (као функција на $C$). Услов да $f$ поништава овај полином је $F(x, f) = 0$. Сада по својству (6) претходног тврђења, можемо ово напасти диференцирањем $\delta$ одакле следи

$$0 = \delta(F(x, f)) = \frac{\partial F}{\partial x}\delta(x) + \frac{\partial F}{\partial T}\delta(f).$$

Овде је било битно да буде $\dfrac{\partial F}{\partial T} \neq 0$ и сада из ове једнакости можемо изразити

$$\frac{\delta(f)}{\delta(x)} = -\frac{\dfrac{\partial F}{\partial x}}{\dfrac{\partial F}{\partial T}}.$$

Количник $\dfrac{\delta(f)}{\delta(x)}$ представља тражено проширење диференцирања по $x$ на целом $K(C)$, те нас ово мотивише да уведемо следећу дефиницију.

**Дефиниција 18.** Нека је $C$ крива над $K$, $x \in K(C)$ такво да је $K(C)/K(x)$ коначно сепарабилно раширење и $y \in K(C)$ произвољна функција. Нека је $F(x, T)$ полином такав да је $F(x, y) = 0$. Дефинишемо

$$\frac{\partial y}{\partial x} = -\frac{\dfrac{\partial F}{\partial x}}{\dfrac{\partial F}{\partial T}},$$

при чему десну страну израчунавамо у $(x, y)$.

Ова дефиниција зависи од полинома $F$ и од представника функције $y$ у $K(C)$, а да бисмо показали да је конзистентна, морамо да покажемо да крајњи резултат не зависи од свега тога. За други полином $F'$ који исто задовољава $F'(x, y) = 0$ диференцирањем добијемо да су одговарајући количници једнаки као и код $F$. Сваки представник $z$ функције $y$ у $K(C)$ задовољава исти минимални полином као и $y$, па по претходном, добијамо исти количник као и за $y$. Дакле, важи следеће тврђење.

**Тврђење 12.** Нека су $F, F'$ полиноми такви да је $F(x,y) = F'(x,y) = 0$. Тада је $\dfrac{\dfrac{\partial F}{\partial x}}{\dfrac{\partial F}{\partial T}} = \dfrac{\dfrac{\partial F'}{\partial x}}{\dfrac{\partial F'}{\partial T}}$. Ако је $z$ неки други представник функције $y$ у $K(C)$, тада је $\dfrac{\partial y}{\partial x} = \dfrac{\partial z}{\partial x}$. Дакле, израз $\dfrac{\partial y}{\partial x}$ је добро дефинисан.

Остаје још да проверимо да је овако дефинисано пресликавање диференцирање на $K(C)$. То захтева још техничких детаља, које овде прескачемо, већ наводимо само тврђење. У тврђењу се помиње и како диференцирамо нову функцију по $y$, где треба да имамо на уму да је то диференцирање по $x$ и формулу

$$\frac{\partial H(y)}{\partial x} = \frac{\partial H}{\partial x} + \frac{\partial H}{\partial T}\frac{\partial y}{\partial x}.$$

**Тврђење 13.** Нека је $C$ крива над $K$, $x \in K(C)$ такво да је $K(C)/K(x)$ коначно сепарабилно раширење. Тада је пресликавање $\delta : K(C) \longrightarrow K(C)$ дефинисано са $\delta(y) = \dfrac{\partial y}{\partial x}$, где је $y \in K(C)$ произвољна функција диференцирање, тј. $K$-линеарно је и задовољава Лајбницово правило.

Даље, ако је $f = H(y) \in K(C)$, где је $H \in K(x)[T]$, нека друга функција из $K(C)$, тада је

$$\delta(f) = \frac{\partial H}{\partial x} - \frac{\partial H}{\partial T}\frac{\dfrac{\partial F}{\partial x}}{\dfrac{\partial F}{\partial T}},$$

где је десна страна израчуната у $(x,y)$, а $F$ као из дефиниције $\dfrac{\partial y}{\partial x}$.

За крај, нека је и $y \in K(C)$ такво да је $K(C)/K(y)$ такође сепарабилно и коначно. Тада за одговарајућа диференцирања важи ланчасто правило, тј.

$$\frac{\partial f}{\partial y} = \frac{\partial f}{\partial y}\frac{\partial y}{\partial x}.$$

Одавде је и, специјално,

$$\frac{\partial y}{\partial x} = \frac{1}{\dfrac{\partial x}{\partial y}} \neq 0.$$

Нека је $t \in K(C)$. Тада је $\dfrac{\partial t}{\partial x} \neq 0$ ако и само ако је и $t$ такво да је $K(C)/K(t)$ коначно сепарабилно раширење.

**Пример 19.** Посматрајмо елиптичку криву $C : y^2 = x^3 + x + 1$ над $\mathbb{Q}$ (перфектним пољем). Функција $x$ је равномернизатор у тачки $(0, 1)$, одакле је $K(C)/K(x)$ коначно и сепарабилно. Желимо прво да израчунамо $\dfrac{\partial y}{\partial x}$ по овој новој дефиницији. Зато, прво тражимо (минимални) полином који поништава $y$ над $K(x)$. То је и више него јасно - $F = y^2 - x^3 - x - 1$. Сада је

$$\frac{\partial y}{\partial x} = -\frac{\dfrac{\partial F}{\partial x}}{\dfrac{\partial F}{\partial T}} = \frac{3x^2 + 1}{2y}.$$

Одредимо сад диференцијале функција $f = xy$ и $g = \frac{y}{x}$. Приметимо да већ знамо формулу за рачунање, одакле одмах имамо

$$\delta(xy) = y + x\frac{3x^2 + 1}{2y} = \frac{2y^2 + 3x^3 + x}{2y} = \frac{5x^3 + 3x + 2}{2y};$$

$$\delta(\frac{y}{x}) = -\frac{y}{x^2} + \frac{1}{x}\frac{3x^2 + 1}{2y} = \frac{-2y^2 + 3x^3 + x}{2x^2y} = \frac{x^3 - x - 2}{2x^2y}.$$

Пошто смо дефинисали „диференцирање по $x$", сада смо у могућности да уведемо појам диференцијала (формални, не заборавимо!). Користићемо познату ознаку $dx$, а ево и дефиниције, која ће да испуњава својства која смо до сада утврдили за диференцирање.

**Дефиниција 19.** Нека је $C$ крива над $K$. Скуп свих *диференцијала*, у ознаци $\Omega(C)$ је количнички модул слободног $K(C)$-модула који генеришу симболи $dx$, за $x \in K(C)$, по следећим релацијама. У свим релацијама претпостављамо да је $x \in K(C)$ такво да је $K(C)/K(x)$ коначно сепарабино раширење.
(1) $dx \neq 0$.
(2) За $h_1, h_2 \in K(C)$ важи $h_1dx + h_2dx = (h_1 + h_2)dx$.
(3) За $y \in K(C)$ је $dy = \dfrac{\partial y}{\partial x}dx$.

Из дефиниције видимо да су диференцијали класе еквиваленције у односу на наведене релације међу формалним симболима облика $\sum_{i=1}^{m} h_i dx_i$, где су $h_i, x_i \in K(C)$, за $i = 1, 2, ..., m$ и $x_i$ су такви да је $K(C)/K(x_i)$ коначно сепарабилно раширење. Видимо да се диференцијал понаша у складу са оним што смо научили из анализе, али да се уједно слаже и са овим што смо уочили да важи за диференцирање дефинисано на овај начин. Следеће тврђење наводи основне особине диференцијала, које се могу рутински доказати и личе на оне горе за диференцирање, па нема потребе да их овде доказујемо.

**Тврђење 14.** Нека је $C$ крива над $K$. Ако се не каже другачије, претпоставља се да су $x, y \in K(C)$ такви да су $K(C)/K(x)$, односно $K(C)/K(y)$ коначна сепарабилна раширења.
(1) $dx = 0$, ако $K(C)/K(x)$ није коначно или сепарабилно раширење. Специјално и $dc = 0$, за $c \in K$, тј. константну функцију.
(2) $d(x + y) = dx + dy$.
(3) $d(cx) = cdx$, за $c \in K$.
(4) $d(xy) = xdy + ydx$.
(5) За свако $n \in \mathbb{Z}$ је $d(x^n) = nx^{n-1}dx$.
(6) $d\left(\frac{y}{x}\right) = \frac{ydx - xdy}{y^2}$.
(7) Ако је $f \in K(C)$ произвољно, тада је $d(f(x)) = \frac{\partial f}{\partial x}dx$.
(8) Ако је $F(x, y)$ рационална функција по $x$ и $y$, тада је

$$d(F(x, y)) = \frac{\partial F}{\partial x}dx + \frac{\partial F}{\partial y}dy.$$

**Пример 20.** Као што знамо, $K(\mathbb{P}^1)$ можемо идентификовати са $K(\mathbb{A}^1) = K(x)$. Онда су све функције $f \in K(\mathbb{P}^1)$ у ствари облика $f(x)$, одакле по правилу (7) претходног тврђења $d(f(x)) = \frac{\partial f}{\partial x}dx$,, сваки диференцијал је облика функција из $K(C)$ пута $dx$.

**Пример 21.** Можемо да се запитамо када су диференцијали $h_1dx_1$ и $h_2dx_2$ еквивалентни ($h_1, h_2, x_1, x_2 \in K(C)$, $K(C)/K(x_1)$ и $K(C)/K(x_2)$

коначна сепарабилна раширења). Зато је згодно да напишемо диференцијал $dx_1$ у облику функција пута $dx_2$. То је, по дефиницији, $dx_1 = \dfrac{\partial x_1}{\partial x_2} dx_2$. Због линеарности, $h_1 dx_1$ и $h_2 dx_2$ су еквивалентни ако и само ако је $\left( h_1 \dfrac{\partial x_1}{\partial x_2} - h_2 \right) dx_2$ еквивалнтан 0. Пошто $dx_2 \neq 0$, тада је $h_1 \dfrac{\partial x_1}{\partial x_2} - h_2 = 0$, а јасно је да важи и обрнуто. Дакле, $h_1 dx_1$ и $h_2 dx_2$ су еквивалентни ако и само ако је

$$h_2 = h_1 \frac{\partial x_1}{\partial x_2}.$$

Сада следи једна веома важна теорема која важи за простор диференцијала.

**Теорема 8.** Простор диференцијала $\Omega(C)$ је једнодимензиони векторски простор над пољем $K(C)$. Другим речима $\Omega(C) \neq \{0\}$ и за свако $x \in K(C)$, такво да је $K(C)/K(x)$ коначно и сепарабилно раширење и за свако $w \in \Omega(C)$, постоји нека функција $h \in K(C)$ таква да је $w = hdx$.

**Доказ.** Из дефиниције диференцијала знамо да су збирови диференцијала и множење функцијом диференцијала опет диференцијали, одакле је $\Omega(C)$ векторски простор над $K(C)$. Нека је $w \in \Omega(C)$ произвољан диференцијал. Тада он има свог представника облика $w = \sum_{i=1}^{m} h_i dx_i$. Тада је $dx_i = \dfrac{\partial x_i}{\partial x} dx$, одакле је

$$w = \sum_{i=1}^{m} h_i \frac{\partial x_i}{\partial x} dx = \left( \sum_{i=1}^{m} h_i \frac{\partial x_i}{\partial x} \right) dx,$$

према томе нашли смо функцију $h = \sum_{i=1}^{m} h_i \dfrac{\partial x_i}{\partial x} \in K(C)$ за коју је $w = hdx$. За крај, још само треба да напоменемо да $\Omega(C) \neq \{0\}$, али то је јасно јер, на пример, $dx \neq 0$.

Као последицу ове теореме имамо следеће тврђење, чији се доказ одмах види из претходног текста. Након овог тврђења ћемо моћи да дамо једну корисну дефиницију.

**Тврђење 15.** Нека је $C$ крива над пољем $K$.
(1) Нека је $x \in K(C)$. Тада је $dx$ база за $\Omega(C)$ над $K(C)$ ако и само ако је $K(C)/K(x)$ коначно сепарабилно раширење.
(2) Нека су $w_1, w_2 \in \Omega(C)$, при чему $w_2 \neq 0$. Тада постоји јединствена функција $f \in K(C)$ таква да је $w_1 = fw_2$. У овом случају $f$ означавамо са $\frac{w_1}{w_2}$.
(3) Нека је $P \in C(\overline{K})$ произвољна тачка и $t \in \overline{K}(C)$ равномернизатор за тачку $P$. Тада за свако $w \in \Omega(C)$ постоји јединствена функција $g \in \overline{K}(C)$ таква да је $w = gdt$.

**Дефиниција 20.** Нека је $C$ крива над $K$, $P \in C(\overline{K})$ произвољна тачка са равномернизатором за ту тачку $t \in \overline{K}(C)$. Тада *ред* диференцијала $w \neq 0$ у тачки $P$ дефинишемо као вредност $\mathrm{ord}_P(w) = \mathrm{ord}_P(\frac{w}{dt})$. Диференцијал $w$ се назива *регуларан* (или *холоморфан*) ако је $\mathrm{ord}_P(w) \geq 0$, за сваку тачку $P \in C(\overline{K})$. Ако важи $\mathrm{ord}_P(w) \leq 0$, за сваку тачку $P \in C(\overline{K})$, онда се диференцијал назива *неанулирајући* (или *непоништавајући*). Диференцијалу $w$ можемо да придружимо *дивизор диференцијала* $w$ (или *дивизор придружен диференцијалу* $w$) са

$$\mathrm{div}(w) = \sum_{P \in C(\overline{K})} \mathrm{ord}_P(w)P.$$

Морамо да проверимо да је ова дефиниција добро дефинисана. Постоје две ствари које морамо да проверимо, прво да ред функције у било којој тачки не зависи од избора униформизатора, а друго да је дивизор придружен диференцијалу добро дефинисан, тј. да ће само у конахцно много тачака имати ред различит од нуле. Из тих разлога, наводимо следеће тврђење.

**Тврђење 16.** Нека је $C$ крива над пољем $K$, $w \in \Omega(C)$, $w \neq 0$.
(1) Нека је $f \in \overline{K}(C)$ регуларна у $P$, а $t \in \overline{K}(C)$ равномернизатор у $P$. Тада је и $\dfrac{df}{dt}$ регуларна у $P$.
(2) Нека су $t, t' \in \overline{K}(C)$ равномернизатори за тачку $P \in C$. Тада је $\mathrm{ord}_P(\frac{w}{dt}) = \mathrm{ord}_P(\frac{w}{dt'})$.

(3) За све, сем можда коначно много $P \in C$ важи $\mathrm{ord}_P(w) = 0$.

**Доказ.** (1) За почетак приметимо шта је $\dfrac{df}{dt}$. По својству диференцијала $df = \dfrac{\partial f}{\partial t}dt$, одакле је $\dfrac{df}{dt} = \dfrac{\partial f}{\partial t}$, за шта треба да докажемо да је регуларно у $P$. Пошто је $f$ регуларна у $P$, $f = t^k g$, где је $k \in \mathbb{N}_0$ и $g \in \overline{K}(C)$ таква да је $\mathrm{ord}_P(g) = 0$. По Лајбницовом правилу диференцирања је

$$\frac{\partial t^k g}{\partial t} = kt^{k-1}g + \frac{\partial g}{\partial t}.$$

За $k > 0$ је леви члан регуларан у $P$, а за $k = 0$ не постоји, па је довољно доказати да је $\dfrac{\partial g}{\partial t}$ регуларан у $P$. Запишимо $g = \dfrac{P_1}{P_2}$ као количник два полинома, тада $P_1(P) \neq 0$, $P_2(P) \neq 0$. Тада, по познатом правилу имамо

$$\frac{\partial g}{\partial t} = \frac{P_2\dfrac{\partial P_1}{\partial t} - P_1\dfrac{\partial P_2}{\partial t}}{P_2^2}.$$

Именилац се не анулира у $P$, а бројилац се састоји од полинома и извода полинома по $t$ који никако не могу створити пол у $P$, према томе, доказали смо регуларност и $\dfrac{\partial g}{\partial t}$ и $\dfrac{\partial f}{\partial t}$.

(2) Нека је $w = fdt = f'dt'$, за неке $f, f' \in \overline{K}(C)$. Како су $t, t'$ равномернизатори за $P$, они су и регуларни у $P$, па по делу (1) знамо да су $\frac{dt}{dt'}$ и $\frac{dt'}{dt}$ у исто време регуларни у $P$. Ово је једино могуће ако је у исто време $\mathrm{ord}_P(\frac{dt}{dt'} = \mathrm{ord}_P(\frac{dt'}{dt} = 0$. Тада је $\mathrm{ord}_P(\frac{f}{f'}) = 0$, тј. $\mathrm{ord}_P(f) = \mathrm{ord}_P(f')$, а ово управо значи да је $\mathrm{ord}_P(\frac{w}{dt}) = \mathrm{ord}_P(\frac{w}{dt'})$.

(3) Одаберимо неко $x \in \overline{K}(C)$ тако да је $\overline{K}(C)/\overline{K}(x)$ коначно и сепарабилно раширење. Ово управо значи да је пресликавање $x : C \longrightarrow \mathbb{P}^1$ сепарабилно. Тада се оно рамификује у највише коначно много тачака (погледати у следећем поглављу, после Хурвицове формуле). Запишимо $w = fdx$, за јединствено $f \in \overline{K}(C)$. Скуп тачака $P$ за које важи неки од следећих услова: $f(P) = 0$, $f(P) = \infty$, $x(P) = \infty$ или у којима је $x$ рамификовано је коначан. Зато, довољно је да докажемо да је за преостале тачке $P$, $\mathrm{ord}_P(w) = 0$ сем можда за њих коначно много. Како посматрамо тачке $P$ у којима је вредност коначна и у којима је $x$ нерамификована, одатле је

$x - x(P)$ равномернизатор у тачки $P$. Пошто је $dx(P) = 0$, јер је $x(P)$ константа, па је $dx = d(x - x(P))$ тада по дефиницији можемо да рачунамо

$$\mathrm{ord}_P(w) = \mathrm{ord}_P(fd(x - x(P))) = \mathrm{ord}_P(f) = 0,$$

за све, сем за коначно много тачака $P$, јер свака функција има коначно много нула и полова.

Следећа два тврђења се користе у доказу Хурвицове теореме, коју наводимо у следећем поглављу, али како и Хурвицову теорему остављамо без доказа, тако ћемо и ова тврђења. При чему друго тврђење има и своју важну сврху у изучавању елиптичких кривих, посебно над коначним пољима. Докази, ова два трвђења, као и Хурвицове теореме се, на пример, налазе у [51].

**Тврђење 17.** Нека је $C$ крива над пољем $K$, $\mathrm{char}\, K = p$, $x, f \in \overline{K}(C)$, при чему је $x$ таква да је $x(P) = 0$ и $\overline{K}(C)/\overline{K}(x)$ коначно и сепарабилно раширење. Имамо два случаја.
Ако је $p = 0$ или $p \nmid \mathrm{ord}_P(x)$, тада $\mathrm{ord}_P(fdx) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1$.
Ако је $p > 0$ и $p \mid \mathrm{ord}_P(x)$, тада $\mathrm{ord}_P(fdx) \geq \mathrm{ord}_P(f) + \mathrm{ord}_P(x)$.

**Дефиниција 21.** Нека је $\phi : C_1 \longrightarrow C_2$ неконстантно рационално пресликавање између глатких кривих над пољем $K$. Придружено пресликавање $\phi^* : \overline{K}(C_2) \longrightarrow \overline{K}(C_1)$ индукује и пресликавање између њихових диференцијала $\phi^* : \Omega(C_2) \longrightarrow \Omega(C_1)$ дефинисано са

$$\phi^* \left( \sum_{i=1}^{m} f_i dx_i \right) = \sum_{i=1}^{m} (\phi^* f_i) d(\phi^* x_i).$$

**Тврђење 18.** Нека је $\phi : C_1 \longrightarrow C_2$ неконстантно рационално пресликавање између глатких кривих над пољем $K$. Тада је $\phi$ сепарабилно ако и само је пресликавање $\phi^* : \Omega(C_2) \longrightarrow \Omega(C_1)$ „1-1" (тј. ненула).

Сада уводимо један специјални дивизор, који има кључну улогу у теореми Римана-Роха, која следи у следећем поглављу.

**Дефиниција 22.** *Канонски дивизор* је било који дивизор облика $\mathrm{div}(w)$, $w \in \Omega(C)$. Скуп свих оваквих дивизора (неки аутори називају слику овог скупа у $\mathrm{Pic}(C)$) се назива *канонска класа дивизора на кривој* $C$.

Уочимо два диференцијала $w_1, w_2 \in \Omega(C)$. Знамо да постоји функција $f \in K(C)$, таква да је $w_1 = fw_2$. Тада је (види се из дефиниције)

$$\mathrm{div}(w_1) = \mathrm{div}(fw_2) = \mathrm{div}(f) + \mathrm{div}(w_2).$$

Између осталог, закључујемо, да сви канонски дивизори имају исти степен и припадају истој класи линеарне еквиваленције дивизора. Према томе, у групи $\mathrm{Pic}(C)$ постоји тачно један њихов представник, тј. сви се сликају у исти елемент. За крај овог дела текста, иду три примера.

**Пример 22.** Одредимо канонску класу дивизора на $\mathbb{P}^1$. Одредимо прво $\mathrm{div}(dx)$, али подсетимо се да користимо афини запис! Тада је за коначне (афине) тачке $a \in \mathbb{A}^1$, равномернизатор $x - a$. Тада је $dx = d(x-a)$, а по дефиницији за одређивање реда у овим тачкама, пишемо $dx = 1 \cdot d(x-a)$, одакле је $\mathrm{ord}_a(dx) = \mathrm{ord}_a(1) = 0$.

Остаје нам још бесконачна тачка, у којој је равномернизатор $\frac{1}{x}$. Тада користећи познате особине диференцијала пишемо $dx = -x^2 d(\frac{1}{x})$, одакле је $\mathrm{ord}_\infty(dx) = \mathrm{ord}_\infty(-x^2) = -2$. Дакле, $\mathrm{div}(dx) = -2\infty$. Сада знамо и да је $\deg(\mathrm{div}(w)) = -2$, за сваки $w \in \Omega(\mathbb{P}^1)$.

Знамо и више, пошто се сваки $w \in \Omega(\mathbb{P}^1)$ записује у облику $w = fdx$, где је $f \in K(\mathbb{P}^1)$, а већ смо раније показали да су сви дивизори степена нула на $\mathbb{P}^1$ уједно и главни, закључујемо да је сваки дивизор степена $-2$ и канонски дивизор. Ово специјално значи да на $\mathbb{P}^1$ нема регуларних диференцијала, јер такви диференцијали имају ненегативан степен.

**Пример 23.** Нека је $C : y^2 = f(x)$ елиптичка или хиперелиптичка глатка крива. Постхо гледамо тачке над пољем $\overline{K}$, можемо да претпоставимо да је водећи коефицијент 1 и да је једначина облика

$$y^2 = (x - \alpha_1)...(x - \alpha_n),$$

где су сви $\alpha_k$ различити. Желимо да одредимо $\mathrm{div}(dx)$. У тачкама $(\alpha, \beta)$ где $y = \beta \neq 0$ знамо да је $x - \alpha$ равномернизатор, па одмах

видимо да је $dx = 1 \cdot d(x-\alpha)$, односно $\mathrm{ord}_{(\alpha,\beta)}(dx) = 0$. Зато су интересантне само тачке које су нуле полинома $f(x)$ и бесконачност(и). Нападнимо једначину са диференцијалом, при чему, наравно, на десној страну користимо $d(x-\alpha_k) = dx$.

$$2ydy = [(x-\alpha_2)...(x-\alpha_n) + ... + (x-\alpha_1)...(x-\alpha_{n-1})]dx$$

Одавде се види да у тачкама $(\alpha_k, 0)$, где знамо да је $y$ равномернизатор, можемо представити

$$dx = \frac{2y}{(x-\alpha_2)...(x-\alpha_n) + ... + (x-\alpha_1)...(x-\alpha_n)}dy,$$

одакле је

$$\mathrm{ord}_{(\alpha_k,0)}(dx) = \mathrm{ord}_{(\alpha_k,0)}\left(\frac{2y}{(x-\alpha_2)...(x-\alpha_n) + ... + (x-\alpha_1)...(x-\alpha_n)}\right) = 1,$$

јер се именилац не анулира у тој тачки (сви сабирци су 0, сем једног, оног којем недостаје $\alpha_k$). За бесконачност, морамо разликовати два случаја.

Лакши случај је ако је $n = 2g+2$, парно. Тада је $\frac{1}{x}$ равномернизатор у бесконачностима, одакле је, због $dx = -x^2 d(\frac{1}{x})$,

$$\mathrm{ord}_{\infty_+}(dx) = \mathrm{ord}_{\infty_-}(dx) = -2.$$

У овом случају је

$$\mathrm{div}(dx) = \sum_{k=1}^{2g+2}(\alpha_k, 0) - 2\infty_+ - 2\infty_-.$$

Непаран случај, $n = 2g+1$, је доста компликованији, јер је тада $\frac{x^g}{y}$ равномернизатор у бесконачности $\infty$. Познавајући особине диференцијала, знамо

$$d\left(\frac{x^g}{y}\right) = \frac{gx^{g-1}ydx - x^g dy}{y^2}.$$

Такође, можемо да изразимо $dy$ преко $dx$ (изнад смо утврдили везу), одакле можемо да доведемо у везу $dx$ и $d(\frac{x^g}{y})$. Након што се замени и среди, добијамо

$$dx = \frac{2y^3}{2gx^{g-1}y^2 - x^g[(x-\alpha_2)...(x-\alpha_{2g+1}) + ... + (x-\alpha_1)...(x-\alpha_{2g})]}d\left(\frac{x^g}{y}\right).$$

Ево мало и анализе, посматрајмо понашање имениоца у бесконачности. Због једначине криве $C$ знамо да је $y^2$ исто као и $x^{2g+1}$, дакле $2gx^{g-1}y^2$ нам даје $2gx^{3g}$. Израз

$$(x-\alpha_2)...(x-\alpha_{2g+1})+...+(x-\alpha_1)...(x-\alpha_{2g})$$

је као $(2g+1)x^{2g}$, одакле је $-x^g[(x-\alpha_2)...(x-\alpha_{2g+1})+...+(x-\alpha_1)...(x-\alpha_{2g})]$ као $-(2g+1)x^{3g}$. Када утврдимо највећи члан у имениоцу, то је $-x^{3g}$ и у рачунању реда у бесконачности он даје информацију. Дакле $\mathrm{ord}_\infty(dx)=3(-2g-1)-3g(-2)=-3$. У овом случају је

$$\mathrm{div}(dx)=\sum_{k=1}^{2g+1}(\alpha_k,0)-3\infty.$$

Слично одређујемо и $\mathrm{div}(dy)$. За афине тачке $(\alpha,\beta)$ имамо два случаја, први када је $\beta=0$, тада знамо да је $\beta=y$, када је $y$ равномернизатор, а у тим тачкама је $\mathrm{ord}_{(\alpha_k,0)}(dy)=0$, и када $\beta\neq 0$, када је равномернизатор $x-\alpha$, а пошто је $d(x-\alpha)=dx$, довољно је да нађемо везу $dy$ и $dx$. Њу знамо из једначине $2ydy=f'(x)dx$, одакле је $dy=\frac{f'(x)}{2y}dx$. Пошто се у овим тачкама $y$ не анулира, можемо евентуално имати нулу и то се дешава у тачкама $(x,y)$ за које је $f'(x)=0$ (тада је $f(x)\neq 0$, тј $y\neq 0$, па је ово у реду). Остаје још испитати бесконачност, што опет води у два случаја.

Ако је $n=2g+2$ паран, тада је $\frac{1}{x}$ равномернизатор у обе бесконачности, одакле

$$dy=\frac{f'(x)}{2y}dx=-\frac{x^2f'(x)}{2y}d\left(\frac{1}{x}\right),$$

па је $\mathrm{ord}_{\infty_\pm}(dy)=(-2)-(2g+1)-(-g-1)=-2-g$. У овом случају је

$$\mathrm{div}(dy)=\sum_{\alpha:f'(\alpha)=0}(\alpha,\beta)-(g+2)\infty_--(g+2)\infty_+.$$

Ако је $n=2g+1$ непаран, имамо равномернизатор $\frac{x^g}{y}$ у једној бесконачности $\infty$. По ономе што већ знамо, када израчунамо, добијамо

$$dy=\frac{y^2f'(x)}{2gx^{g-1}y^2-x^gf'(x)}d\left(\frac{x^g}{y}\right).$$

Када средимо именилац, опет добијамо да је највећи члан $-x^{3g}$, па можемо да израчунамо $\mathrm{ord}_\infty(dy) = -2(2g+1) + 2g(-2) - 3g(-2) = -2g-2$. У овом случају је

$$\mathrm{div}(dy) = \sum_{\alpha: f'(\alpha)=0} (\alpha, \beta) - (2g+2)\infty.$$

**Пример 24.** Мало конкретније у односу на претходни пример (задржавамо ознаке и закључке), уочимо елиптичку криву

$$C : y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3).$$

По ономе што смо израчунали малопре, а и по примеру где смо рачунали дивизор координатне функције $y$ знамо

$$\mathrm{div}(dx) = (\alpha_1, 0) + (\alpha_2, 0) + (\alpha_3, 0) - 3\infty = \mathrm{div}(y).$$

Одавде је

$$\mathrm{div}\left(\frac{dx}{y}\right) = 0,$$

па је диференцијал $\frac{dx}{y}$ у исто време и регуларан и неанулирајући.

## 2.5 Род криве

**Род криве - геометријски**

**Препоручена литература:** Овде, као и у предложеној литератури, излагање је неформално и служи само да стекнемо бољу визуализацију и слику једног важног појма. Добри мотивациони текстови и слике на ову тему се могу наћи у [23], [22].

Почнимо са једним веома познатим резултатом из топологије: *Свака компактна, глатка, повезана површ је хомеоморфна сфери са коначним бројем „ручки", тј. или је сфера, или је торус са $n$ рупа, где је $n \in \mathbb{N}$.* Видећемо да алгебарске криве имају једну важну тополошку инваријанту. Када видимо једначину криве, ми је цртамо у равни. Дакле, ми криву видимо као афини реални објекат. Међутим, овај поглед и даље не даје довољно података, а из већ

познтих разлога, уместо афине криве, посматраћемо пројективну криву (пројективизација нам овде у ствари служи да компактификујемо слику), али над $\mathbb{C}$ (потребно нам је алгебарски затворено поље да бисмо избегли проблеме када полином нема све корене у пољу). У овом случају ћемо моћи да „паметним гледањем" видимо да је свака крива у $\mathbb{P}^2(\mathbb{C})$ има облик једне од ових сфера са ручкама, тј. торуса са неколико рупа. Тада *род криве* дефинишемо као број тих рупа на торусу.

Први пример ће бити један веома познат пример - права. Пошто гледамо комплексну пројективну праву, то је објекат који се састоји од $\mathbb{C}$ и једне бесконачне тачке којом компактификујемо комплексну раван, а овако добијамо сферу. Пошто сфера у себи не садржи рупе, род пројективне праве, тј. праве је 0.

Други пример су глатке конике у равни: елипсе, параболе и хиперболе. И њих ћемо такође моћи да видимо као сфере у $\mathbb{P}^2(\mathbb{C})$. На пример, афини круг $x^2+y^2=1$ се пројективно преставља као $x^2+y^2=z^2$, што се, као што смо напоменули у првој глави изоморфно пројективној правој, а над $\mathbb{C}$ смо малопре увидели да је то сфера. Дакле и конике имају род 0.

Следећи пример су елиптичке криве, тј. криве облика $y^2 = x^3+ax^2+bx+c$.

За почетак уведмо један појамм.*Решетка* у равни је је скуп $\{O+mv+nu \mid m,n\in\mathbb{Z}\}$, где су $u$ и $v$ неки линеарно независни вектори те равни, а $O$ било која тачка те равни. Када цртамо слику, стварно цртамо те векторе, дакле не узимамо само њихове крајње тачке. Најпознатија решетка је целобројна решетка, а име решетка се и види из њеног изгледа.

Може се показати (на пример, у [51]), да је елиптичка крива над $\mathbb{C}$ аналитички изоморфна количницком простору $\mathbb{C}/R$, где је $R$ нека решетка. Ово значи да идентификујемо два комплексна броја, ако је њихова разлика у тој решетки. Видимо да простор који се добије овако изгледа као паралелограм чије су ивице исто идентификоване (када из једне тачке ивице повучемо дуж паралелну другој ивици и пресечемо је са њој паралелном ивицом, добијамо тачку која је идентификована са претходном). Из топологије знамо

да је тај простор торус, који има једну ручку, одакле закључујемо да је елиптичка крива рода 1.

Ово смо могли да изведемо и на други начин, посматрањем комплексног корена. За сваку $x \in \mathbb{C}$, такво да $x^3 + ax^2 + bx + c \neq 0$, постоји тачно 2 $y \in \mathbb{C}$ таква да $y^2 = x^3 + ax^2 + bx + c$, док у случају $x^3 + ax^2 + bx + c = 0$ је једино такво $y = 0$. Ово делује да елиптичку криву можемо добити тако што две копије комплексне равни залепимо у три тачке.

Међутим, то није исправно, због особине комплексног корена (који користимо када добијамо $y$ преко $x$). Сетимо се да је за дефинисање комплексног корена било потребно да исечемо једну полуправу из 0 у комплексној равни, да бисмо спречили да можемо да обиђемо петљу око 0, јер смо тиме променили угао за $2\pi$, док је корен променио угао само за $\pi$, па је ово неконзистентно. Тако и овде приликом лепљења не смемо да дозволимо да нам иста грана корена остане сама на истој страни тачака по којима лепимо.

Нека су нуле полинома $x^3 + ax^2 + bx + c$ $x_1$, $x_2$ и $x_3$. Оне су нам проблематичне тачке, као и тача $\infty$, јер сетимо се да смо у пројективном комплексном простору, где та тачка постоји и сетимо се да је $\mathbb{P}^1(\mathbb{C}) \cong \mathbb{S}^2$. Зато, да бисмо добро дефинисали корен који нам даје $y$, морамо исећи линије на сфери које спајају $x_1$ и $x_2$, односно $x_3$ и $\infty$ на обе сфере. Приметимо да се ти исечци могу прошити до круга на сфери, одакле леплењем (и то по супротно оријентисаним кружницама тих избачених кругова) тих двеју исечених сфера добијамо торус. Овакав поступак се може наћи у [51], [23], [42], [22].

Слична слика као у претходном случају се може направити за било коју криву облика $y^2 = f(x)$, $\deg f = 2g + 1$, одакле можемо добити да слику торуса са $g$ ручки, односно таква крива је рода $g$. Модификација у случају $\deg f = 2g + 2$ је та бесконачна тачка у овом случају не прави проблем, тако да се повезује $g + 1$ пар комплексних нула, одакле треба да добијемо исту слику као и у претходном случају, односно и ове криве су рода $g$.

**Род криве - алгебарски**

У овом делу желимо да експлицитно израчунамо род алгебарске

криве $C$, за који смо стекли интуитивну слику малопре. За то ће нам бити потребан још један нови објекат који придружујемо сваком дивизору $D$ на глаткој кривој $C$ над пољем $K$.

**Дефиниција 23.** Нека је $D \in \mathrm{Div}(C)$. Простор $L(D)$, који се и назива *Риман-Рохов простор дивизора* $D$ је

$$L(D) = \{f \in \overline{K}(C)^* \mid \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

**Коментар.** За почетак, нека је $D = nP$, где је $n \in \mathbb{N}$. Услов $\mathrm{div}(f) \geq -D = -nP$ значи да $f$ може да има пол једино у тачки $P$ и то највише реда $n$. За нуле функције $f$ немамо никакву информацију. Слично, ако је $D$ позитиван дивизор, тј. $D = n_1P_1 + ...n_kP_k$, где су $n_1, \ldots, n_k$ природни бројеви, тада услов $\mathrm{div}(f) \geq -D$ даје да $f$ нема полова ван тачака $P_1, \ldots, P_k$, а у тим тачкама има пол највише реда $n_1, \ldots, n_k$. Остаје још ако дивизор $D$ садржи и тачке са негативним коефицијентом: нека је на пример $-mQ$ део дивизора $D$. Тада, између осталог, услов $\mathrm{div}(f) \geq -D$ условљава да $f$ мора имати нулу у $Q$ и то бар реда $m$. Ово важи за све тачке које се у дивизору $D$ јављају са негативним коефицијентом (има их коначно много).

**Пример 25.** Посматрајмо на пројективној правој $\mathbb{P}^1$ дивизор $D = [1,0] + [0,1]$. Тада је функција

$$f = \frac{(x-y)(x+y)}{xy} \in L(kD),$$

за сваки природан број $k$. Заиста, услов да $f \in L(kD)$ само значи да $f$ нема пол ван тачака $[1,0]$ и $[0,1]$, при чему ти полови могу бити највише реда $k$. Функција $f$ има пол у тим двема тачкама реда 1, према томе, испуњава услов да се налази у свим овим просторима. Ако посматрамо

$$\frac{1}{f} = \frac{xy}{(x-y)(x+y)},$$

ова функција се не налази ни у једном од овим простора. Иако она има нуле у тачкама $[1,0]$ и $[0,1]$, она ипак има пол у тачкама $[1,1]$ и $[-1,1]$, а то није дозвољено за функције из простора $L(kD)$.

У следећем тврђењу наводимо основне особине простора $L(D)$, за $D \in \mathrm{Div}(C)$.

**Тврђење 19.** (1) Скуп $L(D)$ је векторски простор над пољем $\overline{K}$. Његову димензију означавамо са $l(D)$.
(2) Ако је $D \leq D'$, тада $L(D) \subseteq L(D')$.
(3) $L(0)$ је скуп свих константних функција у $\overline{K}$, дакле $l(0) = 1$.
(4) Ако је $\deg(D) < 0$, тада је $L(D) = \{0\}$, па $l(D) = 0$.
(5) За $P \in C$ произвољну тачку важи $l(D + P) \leq l(D) + 1$, тј. $\dim_{\overline{K}}(L(D + P)/L(D)) \leq 1$.
(6) Ако је $D \leq D'$, тада $\dim_{\overline{K}}(L(D')/L(D)) \leq \deg(D' - D)$.
(7) $L(D)$ је коначно-димензиони векторски простор, тј. број $l(D)$ је увек коначан. Ако је $\deg(D) \geq 0$, тада $l(D) \leq \deg(D) + 1$.
(8) Ако је $D \sim D'$, тада $L(D) \cong L(D')$, па је и $l(D) = l(D')$.

**Доказ.** (1) Множење ненула константом не мења дивизор, а по познатој особини за дивизор збира функција закључујемо да и збир остаје у $L(D)$, ако су ту почетне функције, дакле $L(D)$ јесте веторски простор.
(2) Ако је $\mathrm{div}(f) \geq -D$, тада је и $\mathrm{div}(f) \geq -D'$, па $L(D) \subseteq L(D')$.
(3) Ако $f \in L(0)$, тада $f$ нема полова, дакле $f$ је константна.
(4) Нека $f \neq 0 \in L(D)$. Тада, због $\mathrm{div}(f) \geq D$ је $0 = \deg \mathrm{div}(f) \geq \deg(-D) = -\deg(D)$, одакле је $\deg(D) \geq 0$. Зато простор $L(D)$, за $\deg D < 0$ не може да садржи ни једну овакву функцију.
(5) Нека се у дивизору $D$ тачка $P \in C$ појављује $n_P$ пута. Уочимо равномернизатор у тачки $P$, нека је то функција $t \in \mathcal{O}_{C,P}$. Сада је добро дефинисано пресликавање $\phi : L(D + P) \longrightarrow K$ са $\phi(f) = (t^{n_P+1}f)(P)$. Ово је зато што $f \in L(D + P)$ има пол реда највише $n_P + 1$, па све те евентуалне полове неутралише $t^{n_P+1}$. По дефиницији овог пресликавања се види да је оно линеарно. Језгро овог пресликавања чине функције из $L(D + P)$ које немају пол реда $n_P + 1$ у $P$, дакле све функције из $L(D + P)$ чији је пол у $P$ највише $n_P$. Ово управо значи да је $\ker(\phi) = L(D)$. По теореми о изоморфизму $L(D+P)/L(D) \cong \phi(L(P+D)) \subseteq K$, па је $L(D+P)/L(D)$ највише једнодимензиони простор, што је и требало доказати.
(6) Нека је $D' = D + P_1 + ... + P_k$, где тачке $P_1$, ... , $P_k$ могу бити и исте. Означимо $D_l = D + P_1 + ... + P_l$, за $l = 0, 1, ..., k$. Применом дела под (5) $k$ пута на $D_{l+1}$ и $D_l$ (за $l = 0, 1, ..., k - 1$), закључујемо да

је $\dim_{\overline{K}}(L(D_{l+1})/L(D_l)) \leq 1$, а када надовежемо закључке, добијамо $\dim_{\overline{K}}(L(D')/L(D)) \leq k = \deg(D' - D)$.
(7) Ако је $D < 0$, онда је $L(D) = \{0\}$ свакако коначно-димензиони векторски простор. Ако је $\deg(D) \geq 0$, применимо (6) за $D-(\deg D+1)P$ ($P$ је било која тачка, једино је битно да наместимо да степен дивизора буде негативан) и $D$, тада $L(D - (\deg D + 1)P) = \{0\}$, па $\dim_{\overline{K}}(L(D)) \leq \deg(D - (D - (\deg D + 1)P)) = \deg D + 1$.
(8) Нека је $D' = D + \operatorname{div}(g)$, за неко $g \in \overline{K}(C)$. Тада је добро дефинисано пресликавање $\psi : L(D') \longrightarrow L(D)$ задато са $\psi(f) = fg$, јер ако $\operatorname{div}(f) \geq -D'$, тада $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g) \geq -D' + \operatorname{div}(g) = -D$. Ово пресликавање је јасно линеарно и бијекција, па је изоморфизам векторских простора $L(D)$ и $L(D')$.

**Тврђење 20.** За дивизор $D$ важи $l(D) > 0$ ако и само ако је $D$ линеарно еквивалентан неком позитивном дивизору.

**Доказ.** Ако је $D - \operatorname{div}(f) = D'$, за неке $f \in \overline{K}(C)$ и $D' \operatorname{Div}(C)$, тада је по претходном тврђењу $l(D) = l(D') \geq l(0) = 1$. Обрнуто, ако је $l(D) > 0$, постоји $f \neq 0 \in \overline{K}(C)$ таква да $\operatorname{div}(f) \geq -D$. Тада је $D + \operatorname{div}(f) \geq 0$, а то значи да је $D + \operatorname{div}(f)$ позитиван дивизор који је линеарно еквивалентан са $D$.

Даље следе, без доказа, три теореме од велике важности!

**Теорема 9.** (Риманова теорема) Постоји цео број $g$ такав да за све дивизоре $D \in \operatorname{Div}(C)$ важи

$$l(D) \geq \deg D + 1 - g.$$

**Теорема 10.** (Теорема Римана-Роха) Нека је $K_C$ канонски дивизор на кривој $C$. Тада постоји цео број $g$, такав да за сваки дивизор $D \in \operatorname{Div}(C)$ важи

$$l(D) - l(K_C - D) = \deg D - g + 1.$$

**Дефиниција 24.** Најмањи број $g$ из Риманове теореме, односно број $g$ из теореме Римана-Роха се назива *род криве* $C$.

Та два броја ће се поклопити (нећемо доказивати, али морају да се поклопе да би дефиниција имала смисла), и за број $g$ важи да је $g \geq 0$. То се одмах види из тога што је $l(D) \leq \deg D+1$. Наводимо неке лагане, али битне последице теореме Римана-Роха.

**Тврђење 21.** Нека су ознаке исте као и до сада.
(1) $l(K_C) = g$.
(2) $\deg K_C = 2g - 2$.
(3) Ако $\deg D > 2g - 2$, тада $l(D) = \deg D - g + 1$.
(4) Ако $\deg D \geq 2g$, тада $l(D - P) = l(D) - 1$, за све $P \in C$.

**Доказ.** (1) Ставимо $D = 0$ у једнакост Риман-Роха и добијамо $1 - l(K_C) = 1 - g$, одакле је $l(K_C) = g$.
(2) Ставимо сада $D = K_C$ у једнакост Римана-Роха. Имамо $g-1 = \deg K_C - g + 1$, а ово тачно даје $\deg K_C = 2g - 2$.
(3) Ако је $\deg D > 2g - 2$, тада $\deg(K_C - D) < 0$, па $l(K_C - D) = 0$. Када ово нестане из једначине, добијамо тражену једнакост $l(D) = \deg D - g + 1$.
(4) Ако је $\deg D \geq 2g$, тада је $\deg D, \deg(D - P) > 2g - 2$, па из (3) $l(D) = \deg D - g + 1$ и $l(D - P) = \deg(D - P) - g + 1 = (\deg D - g + 1) - 1 = l(D) - 1$.

**Пример 26.** Опишимо простор $L(K_C)$, за неки канонски дивизор $K_C = \operatorname{div}(w)$, $w \in \Omega(C)$. Важи еквиваленција да је функција $f \in L(K_C)$ ако и само ако $\operatorname{div}(f) \geq -\operatorname{div}(w)$, а ово је еквивалентно са тим да је $\operatorname{div}(fw) \geq 0$, односно да је $fw$ регуларан диференцијал. Како се сваки диференцијал из $\Omega(C)$ представља на јединствен начин у облику $fw$, за неку функцију $f$, ово додељивање $f \mapsto fw$, тј. пресликавање између $L(K_C)$ и скупа холоморфних диференцијала на $C$ је $\overline{K}(C)$-линеарно и бијективно, дакле успоставља изоморфизам између одговарајућих векторских простора. Овим закључујемо да је и (према последици теореме Римана-Роха) простор холоморфних диференцијала криве $C$ димензије $g$, рода криве $C$.

**Пример 27.** Показали смо да на пројективној правој $\mathbb{P}^1$ нема регуларних диференцијала, па по претходном примеру закључујемо

да је $l(K_C) = 0$, одакле је род пројективне праве $g = 0$. У овом случају, можемо једнакост Римана-Роха прочитати као

$$l(D) - l(-2\infty - D) = \deg D + 1.$$

Специјално, ако је за дивизор важи $\deg D > -2$, тада је

$$l(D) = \deg D + 1.$$

**Пример 28.** Посматрајмо елиптичку криву

$$C : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

над пољем $K$, где су $\alpha_k$ различити. За њу знамо да је $\operatorname{div}(\frac{dx}{y} = 0$, а ово је један од представника канонских дивизора, те у теореми и последицама Римана-Роха можемо ставити $K_C = 0$. Специјално $l(K_C) = l(0) = 1 = g$, дакле елиптичка крива је рода 1! Тада као последицу имамо и

$$l(D) = \deg D,$$

за дивизоре $D$ степена бар 1. Нека је $P \in C$, произвољна тачка. Тада је $l(P) = 1$, а како овај простор садржи све константне функције (оне немају полове нигде, а немамо услов за нуле), које чине простор димензије 1, закључујемо да је $L(P) = \langle 1 \rangle$. Подсетимо се да $x$ у $\infty$ има пол реда 2, а $y$ реда 3, док немају осталих полова.

Сада можемо да размотримо просторе $L(k\infty)$, за мале природне бројеве $k$. Знамо $l(k\infty) = k$, тако да знамо димензије тражених простора. Већ смо одредили ($P = \infty$) $L(\infty) = \langle 1 \rangle$. За $L(2\infty)$, знамо да је дводимензиони простор који садржи константне функције и функцију $x$, линеарно независну од њих, па је $L(2\infty) = \langle 1, x \rangle$. Простор $L(3\infty)$ садржи поред константних и функције $x$ и функцију $y$, а оне су све линеарно независне на кривој $C$ (имамо једначину тек за $y^2$), па је $L(3\infty) = \langle 1, x, y \rangle$. Слично се добија $L(4\infty) = \langle 1, x, y, x^2 \rangle$ и $L(5\infty) = \langle 1, x, y, x^2, xy \rangle$. Осмотримо сад простор $L(6\infty)$. Он садржи 7 различитих функција: 1, $x$, $y$, $x^2$, $xy$, $x^3$ и $y^2$.

Пошто се све оне налазе у простору димензије 6, мора постојати линеарна веза између неких од њих! Наравно, то није изненађење,

пошто је једначина криве $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, а када ово групишемо по набројаним функцијама, добијамо $\overline{K}$-линеарну везу између неких од тих функција.

**Пример 29.** Постоји начин да окарактеришемо све канонске дивизоре. Знамо да сваки канонски дивизор $K_C$ задовољава $\deg K_C = 2g - 2$ и $l(K_C) = g$. Важи и обрнуто, ако за дивизор $D$ важи $\deg D = 2g - 2$, $l(D) = g$, онда је он канонски дивизор!

Убацимо прво $D$ у једнакост Римана-Роха, одакле је $g - l(K_C - D) = 2g - 2 - g + 1$, тј. $l(K_C - D) = 1$. Сада убацимо $K_C - D$ у једнакост Римана-Роха, одакле је $1 - g = \deg(K_C - D) - g + 1$, па је $\deg(K_C - D) = 0$. Из услова $l(K_C - D) = 1$ закључујемо да постоји функција $f \in \overline{K}(C)$ таква да је $\operatorname{div}(f) \geq D - K_C$. Али, како је $\deg(\operatorname{div}(f)) = 0$ и $\deg(D - K_C) = 0$, мора важити једнакост $\operatorname{div}(f) = D - K_C$. Сада је $D = \operatorname{div}(f) + K_C = \operatorname{div}(f) + \operatorname{div}(w) = \operatorname{div}(fw)$, за неки диференијал $w$, а тада је $fw$ опет диференцијал, што управо значи да је $D$ канонски дивизор.

Ако је $g > 0$, тада је $l(D) > 0$, па знамо да је $D$ онда линеарно еквивалентан неком позитивном дивизору, одакле можемо да закључимо да за $g > 0$ постоји позитиван канонски дивизор. За $g = 0$ знамо да овако нешто не мора да важи (пример: $\mathbb{P}^1$).

**Пример 30.** Нека је : $y^2 = f(x)$ хиперелиптичка крива (тј. њен афини део), при чему је $f$ непарног степена. Она има јединствену бесконачност $\infty$. Желимо да опишемо просторе $L(k\infty)$, где је $k \in \mathbb{N}_0$.

Дакле, тражимо функције које су регуларне у свим афиним тачкама за почетак. Ако узмемо било коју неполиномску рационалну функцију из $\overline{K}(C)$, она ће имати неконстантан именилац, који ће се сигурно анулирати у некој тачки $(x_0, y_0)$, јер ово све посматрамо над алгебарски затвореним пољем $\overline{K}$. Полином у имениоцу има бар једну неодређену од $x$ и $y$, па када фиксирамо ону другу неодређену, добијамо полином по првој неодређеној који има нулу у $\overline{K}$. Према томе, остају једино полиномске функције, тј. елементи афиног координатног прстена $K[x, y]$ (при чему ово сечемо по релацији $y^2 - f(x)$).

Због тога, $y^2$ можемо представити као полином по $x$, па је довољно да посматрамо функције 1, $x$, $x^2$, ... , $y$, $xy$, $x^2y$, ... Међу овим функцијама нема линеарно зависних, тако да оне чине

базу над пољем $\overline{K}$. Такође, у примеру број 3 смо видели да је $\mathrm{ord}_\infty(x) = -2$ и $\mathrm{ord}_\infty(y) = -2g-1$. Сада лако рачунамо редове полова набројаних функција: $\mathrm{ord}_\infty(x^n) = -2n$ и $\mathrm{ord}_\infty(x^n y) = -2n - 2g - 1$.

Сада лако можемо наћи базе простора $L(k\infty)$. Већ знамо $L(0) = \langle 1\rangle$. Међутим, исто ће да важи и за $L(\infty)$, јер координатне функције имају пол у $\infty$ бар 2, док рационалне функције имају пол негде у афином делу. Дакле, $L(\infty) = \langle 1\rangle$. На даље неко време можемо убацивати степене функције $x$, која има пол реда два, према томе два узастопна броја $k$ ће давати исти простор докле год не пређемо $g$: $L(2\infty) = L(3\infty) = \langle 1, x\rangle$, $L(4\infty) = L(5\infty) = \langle 1, x, x^2\rangle$, ... , $L(2n\infty) = \langle 1, x, ..., x^n\rangle$, кад год $n \leq g$ и $L((2n+1)\infty) = \langle 1, x, ..., x^n\rangle$ кад год $n < g$. У неком тренутку долазимо до $k = 2g+1$, где се први пут појављује и $y$: $L((2g+1)\infty) = \langle 1, x, ..., x^g, y\rangle$, $L((2g+2)\infty) = \langle 1, x, ..., x^g, x^{g+1}, y\rangle$. Сада је јасно како се граде ови већи простори, $L(2n\infty) = \langle 1, x, ..., x^g, ..., x^n, y, xy, ..., x^{n-g-1}y\rangle$, кад год $n > g$ и $L((2n+1)\infty) = \langle 1, x, ..., x^g, ..., x^n, y, xy, ..., x^{n-g-1}y, x^{n-g}y\rangle$, кад год $n \geq g$. Сада можемо да закључимо вредности бројева $l(n\infty)$. Резултати:

$$L(n\infty) = \begin{cases} \{0\}, & n < 0 \\ \left\langle 1, x, ..., x^{[\frac{n}{2}]}\right\rangle, & 0 \leq n \leq 2g \\ \left\langle 1, x, ..., x^{[\frac{n}{2}]}, y, xy, ..., x^{[\frac{n-1}{2}]-g}y\right\rangle, & 2g+1 \leq n \end{cases} \tag{1}$$

$$l(n\infty) = \begin{cases} 0, & n < 0 \\ [\frac{n}{2}] + 1, & 0 \leq n \leq 2g \\ n - g + 1, & 2g+1 \leq n \end{cases} \tag{2}$$

Приметимо да за $n \geq 2g+1$ важи $l(n\infty) = n - g + 1$, док за $n = 2g$ је $l(n\infty) = g + 1 = n - g + 1$ и за $n = 2g-1$ $l(n\infty) = g = n - g + 1$ што је у складу са последицом теореме Римана-Роха да је $l(D) = \deg D - g + 1$, за $\deg D > 2g - 2$.

**Пример 31.** На начин као у претходном примеру не можемо испитати просторе $L(k\infty_s)$ и $L(k\infty_{-s})$, када је $\deg(f) = 2g+2$ паран, а $k \in \mathbb{N}_0$. Међутим, оно што можемо да урадимо јесте да испитамо просторе $L(k(\infty_s + \infty_{-s}))$. Овај задатак је веома сличан као задатак из претходног примера, одакле на исти начин закључујемо да ови простори могу да садрже само функције 1, $x$, $x^2$, ... , $y$, $xy$, ... На

исти начин као у претходном примеру и одређујемо ове просторе, а овде дајемо само коначан резултат:

$$L(n(\infty_s + \infty_{-s})) = \begin{cases} \{0\}, & n < 0 \\ \langle 1, x, ..., x^n \rangle, & 0 \leq n \leq g \\ \langle 1, x, ..., x^n, y, xy, ..., x^{n-g-1}y \rangle, & g+1 \leq n \end{cases} \quad (3)$$

$$l(n(\infty_s + \infty_{-s})) = \begin{cases} 0, & n < 0 \\ n+1, & 0 \leq n \leq g \\ 2n-g+1, & g+1 \leq n \end{cases} \quad (4)$$

Пошто је $\deg(n(\infty_s + \infty_{-s})) = 2n$, можемо за $n \geq g$ (ово је еквивалентно са $\deg D > 2g-2$) да проверимо тачност последице теореме Римана-Роха. За $n \geq g+1$ је ово очигедно, док за $n = g$ имамо $g+1 = 2g-g+1$, што је такође тачно.

**Теорема 11.** (Хурвицова теорема) Нека је $\phi : C_1 \longrightarrow C_2$ неконстантно сепарабилно пресликавање глатких кривих, рода $g_1$ и $g_2$, редом. Тада важи неједнакост

$$2g_1 - 2 \geq (\deg \phi)(2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1).$$

У овој неједнакости једнакост важи ако и само ако је испуњен један од следећа два услова:
(1) $\mathrm{char}(K) = 0$; (2) $\mathrm{char}(K) = p$, али $p \nmid e_\phi(P)$, ни за једно $P \in C_1$.

Видимо да у збир на десној страни улазе само рамификоване тачке и када будемо примењивали Хурвицову теорему, само ћемо обратити пажњу на њих. Има смисла поставити питање зашто је тај збир коначан и зато наводимо још једно тврђење, без доказа, које нам даје одговор на то питање.

**Тврђење 22.** Нека је $\phi : C_1 \longrightarrow C_2$ неконстантно сепарабилно пресликавање глатких кривих. За скоро све тачке $Q \in C_2$ (сем можда за њих коначно много) важи $\#\phi^{-1}(Q) = \deg_s(\phi)$.

Ознака $\#\phi^{-1}(Q)$ је уобичајена ознака за број тачака скупа $\phi^{-1}(Q)$. У Хурвицовој теореми захтевамо да пресликавање буде сепарабилно, одакле је $\deg(\phi) = \deg_s(\phi)$. Како знамо формулу

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi,$$

за скоро све $Q \in C_2$ ће се на левој страни наћи тачно $\deg \phi$ тачака, одакле све оне морају бити нерамификоване. Само за коначно тачака $Q \in C_2$ и према томе за коначно тачака $P \in C_1$ ће важити $e_\phi(P) > 1$. Дакле, збир на десној страни је коначан.

**Пример 32.** Желимо коначно да се уверимо да хиперелиптичка крива, задата једначином у стандардном афином делу $y^2 = f(x)$, $\deg(f) \in \{2g+1, 2g+2\}$ је рода $g$, као што смо видели са слике у 2.2. Користићемо пресликавање из примера 9 и податке које смо тамо открили. Дакле, $\phi : C \longrightarrow \mathbb{P}^1$ задајемо са $\phi(x, y) = x$.

Пошто смо захтевали да за поље $K$ важи $\mathrm{char}(K) \neq 2$, пресликавање је сепарабилно и сви индекси рамификације овог пресликавања су 1 или 2 у Хурвицовој теореми важи једнакост. Још знамо да је $\deg \phi = 2$ и $g(\mathbb{P}^1) = 0$. Када ово заменимо у закључак теореме, добијамо једнакост

$$2g(C) - 2 = 2(0 - 2) + \sum_{P \in C} (e_\phi(P) - 1).$$

Као и сваки пут до сада, морамо да разликујемо два случаја.

Нека је прво $\deg(f) = 2g + 1$. Имамо једну бесконачност $\infty$, која је рамификована, тј. $e_\phi(\infty) = 2$ и имамо још $2g + 1$ рамификованих тачака, то су оне које садрже нуле полинома $f$, тј. тачке облика $(\alpha, 0)$. У свакој од тих тачака важи $e_\phi((\alpha, 0)) = 2$. Све остале тачке су нерамификоване, па не улазе у збир. Сада када ово вратимо у једнакост, долазимо до траженог закључка

$$2g(C) = -2 + 2g + 1 + 1,$$

односно $g(C) = g$.

Нека је $\deg(f) = 2g+2$. Сада имамо две бесконачности које нису рамификоване, тако да једино имамо $2g+2$ рамификованих афиних тачака облика $(\alpha, 0)$ и свака од њих је индекса рамификације 2. Овај случај нам још брже даје једнакост

$$2g(C) = -2 + 2g + 2,$$

тј. $g(C) = g$ и у овом случају. Ево још једног оправдања зашто смо смели одмах у дефиницији хиперелиптичке криве да напишемо да је рода $g$. Приметимо и да нигде нисмо користили да је $g \geq 2$, овај доказ потпуно ради и за $g = 1$, што даје још један показатељ да једначина облика $y^2 = f(x)$, где је $f$ трећег или четвртог степена формира криву рода 1, односно баш елиптичку криву.

За крај ове главе наводимо једну теорему која ће нам бити корисна касније. Знамо да је хиперелиптичка крива $C : y^2 = f(x)$, при чему $\deg f \in \{2g+1, 2g+2\}$ рода $g$. Тада је $l(K_C) = g$. Одавде знамо да је простор регуларних диференцијала димензије $g$. Теорема која следи нам даје базу тог векторског простора.

**Теорема 12.** Нека је $C : y^2 = f(x)$ хиперелиптичка крива рода $g$ над пољем $K$. Тада је скуп

$$\left\{ \frac{1}{2y}dx, \frac{x}{2y}dx, ..., \frac{x^{g-1}}{2y}dx \right\}$$

база векторског простора реглуарних диференцијала над пољем $\overline{K}$. Другим речима, сваки регуларан диференцијал на кривој $C$ се записује на јединствен начин у облику $\dfrac{p(x)dx}{2y}$, за неки полином $p$ степена највише $g-1$.

**Доказ.** Означимо са $D_\infty$ дивизор у бесконачности функције $x$. То значи да је $D_\infty = 2\infty$ у непарном случају, односно $D_\infty = \infty_s + \infty_{-s}$ у парном случају. Означимо и $w_0 = \frac{dx}{2y}$. Пошто смо већ одредили $\operatorname{div}(dx)$ и $\operatorname{div}(y)$, када уврстимо те вредности знамо и $\operatorname{div}(w_0) = \operatorname{div}(dx) - \operatorname{div}(y) = (g-1)D_\infty$. Сваки диференцијал можемо да запишемо у облику $w = \phi w_0$, за неко $\phi \in \overline{K}(C)$, а по ономе што смо раније утврдили, овај диференцијал је регуларан ако и

само ако $\phi \in L((g-1)D_\infty)$. Међутим, и ове просторе смо већ описали, а у оба случаја је $L((g-1)D_\infty) = \langle 1, x, ..., x^{g-1} \rangle$. Како су ове функције линеарно независне, има их $g$, а сад смо утврдили да се $\frac{1}{2y}dx, \frac{x}{2y}dx, ..., \frac{x^{g-1}}{2y}$ све налазе у простору регуларних диференцијала, који је димензије $g$, закључујемо да оне формирају базы тог простора над $\overline{K}$.

# 3 $p$-адски бројеви и њихове примене

## 3.1 Увод у $p$-адске бројеве

**Препоручена литература:** Литература за $p$-адске бројеве је нашироко распрострањена, за детаљно изучавање су познате књиге [25] и [29], док су веома згодни и неки краћи материјали, као што су [2], [44], [57], [41], [53]. Овде само кратко наводимо основна својства $p$-адских валуација и конструкцију $p$-адских бројева. Доказе наведених тврђења нећемо наводити, а могу се наћи у презентованој литератури.

Подсетимо се да је *апсолутна вредност* на пољу $K$ пресликавање

$$|\ |: K \longrightarrow \mathbb{R}_{\geq 0}$$

са следећим својствима
(1) $|x| = 0$ ако и само ако $x = 0$;
(2) $|xy| = |x||y|$, за све $x, y \in K$;
(3) $|x + y| \leq |x| + |y|$, за све $x, y \in K$.

На пољу $\mathbb{Q}$ осим стандардне апсолутне вредности, постоје и *$p$-адске апсолутне вредности*, које означавамо са $|\cdot|_p$, за сваки прост број $p$ и дефинишу се на следећи начин. Сваки рационалан број $x \neq 0$ се може записати у облику $x = p^m \cdot \frac{a}{b}$, при чему $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, $p \nmid ab$. Тада

$$|x|_p = p^{-m},$$

док стављамо $|0|_p = 0$.

**Пример 33.** Овакве апсолутне вредности се брзо рачунају, за $360 = 2^3 \cdot 3^2 \cdot 5$ је $|360|_2 = \frac{1}{8}$, $|360|_3 = \frac{1}{9}$, $|360|_5 = \frac{1}{5}$, док за остале просте бројеве $p$ је $|360|_p = 1$. Слично

$$\left|\frac{28}{99}\right|_2 = \frac{1}{4}, \quad \left|\frac{28}{99}\right|_3 = 9, \quad \left|\frac{28}{99}\right|_7 = \frac{1}{7}, \quad \left|\frac{28}{99}\right|_{11} = 11.$$

Треба проверити да овако дефинисане апсолутне вредности заиста то и јесу. То је рутински посао, али долазимо до нечега

занимљивог. У провери рутински утврђујемо да својства (1) и (2) важе, док за својство (3) важи и више! Наиме, важи
(3') $|x+y|_p \leq \max\{|x|_p, |y|_p\}$, за све $x, y \in \mathbb{Q}$.

Овакве апсолутне вредности се зову *неархимедске апсолутне вредности*. Разлог је јасан, у њима не важи Архимедово својство, на пример, за $a = 1$ и $M = 2$ неће постојати $n \in \mathbb{N}$, такво да је $|na|_p > M$! И ове неједнакости видимо да $|na|_p = |n|_p \leq 1$, за све $n \in \mathbb{N}$.

**Пример 34.** Из дефиниције апсолутне вредности $|\cdot|$ се лако изводе својства да је

$$|1| = 1, \qquad |-1| = 1, \qquad |-x| = |x|,$$

као и да $|x^n| = 1$ повлачи да је $|x| = 1$, одакле следи да за апсолутну вредност на коначном пољу важи да је $|x| = 1$, за све $x \neq 0$.

Једно необично својство ове $p$-адске апсолутне вредности је следеће, ако $|x|_p \neq |y|_p$, тада

$$|x+y|_p = \max\{|x|_p, |y|_p\}.$$

Када имамо апсолутну вредност $|\cdot|$ на пољу $K$, тада можемо да дефинишемо и метрику на $K$ са $d(x,y) = |x-y|$, а директно се може проверити да је овако заиста дефинисана метрика. Посебно је занимљива ова $p$-адска метрика, јер ту важе две интересантне ствари.
(1) *Сваки троугао је једнакокрак, тј. за било која три $x, y, z \in \mathbb{Q}$, бар два броја из скупа $\{d(x,y), d(y,z), d(z,x)\}$ су једнака!*
(2) *Свака тачка отворене лопте је њен центар!*

Сетимо се да је једна од дефиниција да су две метрике на истом простору *еквивалентне* ако индукују исту топологију (тј. ако је отворен скуп у првој метрици, отворен и у другој и обрнуто). Стога, кажемо да су и две норме на истом простору *еквивалентне* ако су метрике које дефинишемо помоћу њих еквивалентне.

Желимо да призовемо у помоћ анализу, а за анализу су нам потребни метрички простори које смо направили. Нема потребе да

одвојено посматрамо просторе са еквивалентним метрикама. Да ли постоје још неке апсолутне вредности на $\mathbb{Q}$? Постоје,*али оне су еквивалентне некој од наведених, са изузетком тривијалне апсолутне вредности, за коју је* $|x| = 1$*, за све* $x \in \mathbb{Q}^*$! Ово тврђење се назива теорема Островског. Дакле, пронашли смо све апсолутне вредности које су нам од интереса када желимо да радимо анализу у пољу $\mathbb{Q}$, , међу којима је тачно једна *архимедска* (где важи Архимедова аксиома), то је стандардна апсолутна вредност, док су све $p$-адске неархимедске.

Ако желимо да се бавимо анализом у метричком простору, желимо да Кошијеви низови конвергирају, тј. да је метрички простор *комплетан*. Као што знамо из реалне анализе, $\mathbb{Q}$ није комплетан у односу на стандардну апсолутну вредност, а његово комплетирања је управо поље $\mathbb{R}$. Остаје да проверимо да је $\mathbb{Q}$ комплетан у односу на $p$-адске апсолутне вредности. И ту је одговор не. Даћемо пример за случај $p = 3$, одакле се лако може извести доказ за остале просте бројеве $p$.

Одаберимо број 7, то је цео број, који није потпун квадрат, али који је квадратни остатак модуло 3 и није дељив са 3. Низ конструишемо индуктивно, први члан $x_0$ бирамо тако да је $x_0^2 \equiv 7 \pmod 3$, а ако знамо број $x_{n-1}$, тада је $x_n$ цео број са следећим својствима

$$x_n \equiv x_{n-1} \pmod{3^n}, \qquad x_n^2 \equiv 7 \pmod{3^{n+1}}.$$

Већ са знањем елементарне теорије бројева знамо да овакав низ постоји, а наведимо овде првих неколико чланова - 1, 4, 13, 13, 175, ... Тада важи

$$|x_m - x_n|_3 \leq \max\{|x_m - x_{m-1}|_3, ..., |x_{n+1} - x_n|_3\} \leq$$

$$\leq \max\{3^{-m}, 3^{-m+1}, ..., 3^{-n-1}\} = 3^{-n-1},$$

одакле је овај низ Кошијев. Такође

$$|x_n^2 - 7|_3 \leq 3^{-n-1},$$

одакле, ако овај низ конвергира, његов лимес мора бити $\sqrt{7}$, а то је број који није рационалан. Према томе, ово је пример Кошијевог низа који не конвергира.

Стога, пролазимо добро познати процес комплетирања неког метричког простора, што овде прескачемо, одакле, кренувши од $(\mathbb{Q}, |\cdot|_p)$, долазимо до поља $\mathbb{Q}_p$, са својом апсолутном вредношћу, коју исто означавамо са $|\cdot|_p$ и она је проширење $p$-адске апсолутне вредности на $\mathbb{Q}$. Проширена апсолутна вредност је и даље неархимедска са истим својствима као и до сада. Чак је и скуп могућих апсолутних вредности исти као и над $\mathbb{Q}$, тј.

$$\{|x|_p \mid x \in \mathbb{Q}_p\} = \{|x|_p \mid x \in \mathbb{Q}\} = \{p^m \mid m \in \mathbb{Z}\} \cup \{0\}.$$

Такође, познато је да у процесу комплетирања почетно поље остаје густо у новодобијеном, тако да је $\mathbb{Q}$ густо у $\mathbb{Q}_p$.

Из неархимедског својства $|\cdot|_p$ следи да је

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x| \leq 1\}$$

прстен, тачније, то је прстен *p-адских целих бројева*. Слично,

$$\mathfrak{M}_p = p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x| < 1\}$$

је идеал у прстену $\mathbb{Z}_p$, то је јединствен максимални идеал у том прстену, одакле закључујемо да је $\mathbb{Z}_p$ локални прстен. Ако нас занима који рационални бројеви су у овом прстену, лако се види

$$\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}.$$

Прстен $\mathbb{Z}_p$ се може лепо описати, захваљујући томе да инклузија $\mathbb{Z} \longrightarrow \mathbb{Z}_p$ има густу слику, тј. за свако $x \in \mathbb{Z}_p$ и $n \in \mathbb{N}$, постоји $\alpha \in \mathbb{Z}$, $0 \leq \alpha \leq p^n - 1$ (и то јединствено!), такво да

$$|x - \alpha|_p \leq p^{-n}.$$

Као последицу овога, за свако $x \in \mathbb{Z}_p$ постоји јединствен Кошијев низ $\alpha_n \in \mathbb{Z}$ који конвергира ка $x$ са следећим својствима
(1) $0 \leq \alpha_n \leq p^n - 1$;

(2) За свако $n \in \mathbb{N}$ важи $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.

Одавде закључујемо да се сваки $p$-адски цео број $x$ јединствено записује у следећм облику

$$x = \sum_{n=0}^{\infty} a_n p^n,$$

при чему за све $n$ важи $0 \leq a_n \leq p$. Са друге стране, овај запис можемо видети и као уређени скуп бројева

$$(b_0, b_1, b_2, ..., b_n....) \qquad b_n \equiv b_{n-1} \pmod{p^n}.$$

Овако добијамо $p$-адске целе бројеве као инверзни лимес прстена $\mathbb{Z}/p^n\mathbb{Z}$ и хомоморфизама

$$\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z}, \qquad x \pmod{p^n} \mapsto x \pmod{p^{n-1}}.$$

Још се доказује да је $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$, што значи да за свако $x \in \mathbb{Q}_p$, постоји $m \in \mathbb{Z}$ такво да $p^m x \in \mathbb{Q}_p$, одакле се $x$ може развити као

$$x = \sum_{n=-m}^{\infty} a_n p^n.$$

Видимо аналогију са познатим развојима, $p$-адски цели бројеви се развијају у Тејлоров ред по $p$, а $p$-адски бројеви уопштено се развијају у (коначан) Лоранов ред. Наравно, јасно је да ови редови конвергирају.

Што се тиче тополошких својстава, у $\mathbb{Q}_p$ је свака затворена лопта која не садржи само једну тачку уједно и отворена лопта и обрнуто (због дискретности скупа вредности које може да узме апсолутна вредност), одакле следи да је $\mathbb{Q}_p$ потпуно неповезан простор, тј. компонента повезаности сваке тачке $x \in \mathbb{Q}_p$ је само тачка. Пошто је јасно да можемо раздвојити различите тачке у $\mathbb{Q}_p$, то је и Хаусдорфов простор. Знамо и то да је прстен $\mathbb{Z}_p$ компактан, док је поље $\mathbb{Q}_p$ локално компактно.

Ипак желимо да радимо и алгебру поред анализе, а ту нам смета што поље $\mathbb{Q}_p$ није алгебарски затворено. То се може лако проверити, за одређени прост број $p$ узмимо било који квадратни неостатак $a$ по модулу $p$ и тада број $\sqrt{a}$ не постоји у $\mathbb{Q}_p$, тј. полином $x^2 - a$ нема корена у пољу $\mathbb{Q}_p$. Из алгебре знамо да за свако поље $K$ постоји (јединствено до на изоморфизам) његово алгебарско затворење $\overline{K}$. Одатле и постоји поље $\overline{\mathbb{Q}_p}$. Међутим, опет се јавља стара невоља, ово поље није комплетно! На срећу, комплетирање овог поља, које називамо $\mathbb{C}_p$ остаје и алгебарски затворено, према томе, ово је минимално раширење поља $\mathbb{Q}_p$ које је у исто време и алгебарски затворено и комплетно. Зато овде користимо ознаку $\mathbb{C}_p$, по аналогији са $\mathbb{C}$, а не већ код $\overline{\mathbb{Q}_p}$. И апсолутна вредност $|\cdot|_p$ се на стандардан начин проширује са $\mathbb{Q}_p$ на $\mathbb{C}_p$. Поновимо још једном, ово се све може наћи у [25] и [29].

## 3.2 Важна својства $p$-адских бројева

Након увода, у којем нисмо баш видели теорију бројева, коначно долазимо до својства $p$-адских бројева због којих су они тако значајни. Томе највише доприноси невероватно корисна **Хенселова лема** (овај математичар је иначе и творац $p$-адских бројева) и из поштовањ према теореми и њеним многобројним применама навешћемо многе верзије иако би било математички коректно да шкрто само напоменемо најопштији облик. Почећемо са једним примером.

**Пример 35.** Као што смо нагласили при крају прошлог излагања, ако је $a$ квадратни неостатак по модулу $p$ и тада број $\sqrt{a}$ не постоји у $\mathbb{Q}_p$, тј. полином $x^2 - a$ нема корена у пољу $\mathbb{Q}_p$. Ако је $x^2 = a$, тада је $|x|_p \leq 1$, јер је $|a|_p \leq 1$, па је $x \in \mathbb{Z}_p$, тј.

$$x = \sum_{n=0}^{\infty} a_n p^n.$$

Ако прихватимо (а јесте) да множимо бројеве онако како бисмо очекивали, тада квадрирањем добијамо

$$a = \left( \sum_{n=0}^{\infty} a_n p^n \right)^2 \equiv a_0^2 \pmod{p},$$

а ово онда даје да је $a$ квадратни остатак модуло $p$, што је контрадикција.

Са друге стране, ако је $p \neq 2$, $a$ квадратни остатак модуло $p$ и $p \nmid a$, тада заиста постоји $x \in \mathbb{Z}_p$ такво да $x^2 = a$. Можемо индуктивно да добијемо коефицијенте $a_n$ у развоју

$$x = \sum_{n=0}^{\infty} a_n p^n.$$

Бирамо $a_0$ из скупа $\{1, 2, ..., p-1\}$ такво да $a_0^2 \equiv a \pmod{p}$. Даље, мора бити

$$2a_0a_1 + p_1 \equiv 0 \pmod{p},$$

где $p_1$ означава пренос, а пошто $a_0 \neq 0$, можемо одредити и $a_1$ и то јединствено. Настављајући овај процес (увек ћемо уз нови члан имати $2a_0a_n$), одређујемо јединствено $a_n$, па добијамо тражено $x$. Формализацију овог примера видимо у следећој теореми.

**Теорема 13.** Нека је

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in \mathbb{Z}_p[x].$$

Претпоставимо да постоји $a_0 \in \mathbb{Z}_p$ такав да

$$f(a_0) \equiv 0 \pmod{p}, \qquad f'(a_0) \not\equiv 0 \pmod{p}.$$

Овде је $f'$ формални извод полинома $f$. Тада постоји јединствено $a \in \mathbb{Z}_p$ такво да

$$f(a) = 0, \qquad a \equiv a_0 \pmod{p}.$$

**Пример 36.** Сада можемо и формално доказати други део претходног примера, пошто једначина $f(x) = x^2 - a$ има решења $a_0$ модуло $p$ у $\mathbb{Z}$, па самим тим и у $\mathbb{Z}_p$ и при томе је $f'(a_0) = 2a_0 \not\equiv 0 \pmod{p}$, ово решење се јединствено подиже у решење $x \in \mathbb{Z}_p$. Приметимо да једначина

$$x^2 \equiv a \pmod{p}$$

има два решења у скупу $\{1, 2, ..., p-1\}$, одакле због јединствености подизања, постоји тачно два решења једначине $x^2 = a$ у $\mathbb{Z}_p$, као што је и очекивано.

Одавде можемо да закључимо да следећи бројеви постоје у одговарајућим прстенима (иако је неформалан запис, пошто корен није једнозначна функција, зна се на шта се мисли)

$$\sqrt{-2} \in \mathbb{Z}_3, \quad \sqrt{-1} \in \mathbb{Z}_5, \quad \sqrt{2} \in \mathbb{Z}_7, \quad \sqrt{2016} \in \mathbb{Z}_{11}.$$

Међутим, ова теорема има мало ограничености у примени. Не можемо ништа за закључимо о $p$-тим коренима у пољу $\mathbb{Q}_p$, на пример (обичним) коренима у $\mathbb{Q}_2$. Напоменимо да је услов теореме заиста битан, морамо да будемо пажљиви, јер нам ова теорема не даје постојање $\sqrt{3}$ у $\mathbb{Q}_3$, јер то ни не постоји. За било које решење једначине $x^2 \equiv 3 \pmod 3$ важи $2x \equiv 3 \equiv 0 \pmod 3$, што значи да не смемо применити теорему.

Овај поступак је и добар да се докаже да $\sqrt{3} \notin \mathbb{Q}_3$, чак $\sqrt{3} \notin \mathbb{Z}_3$. Заиста, прва цифра развоја мора броја $x = \sqrt{3}$ бити 0, али онда $3 \mid x$, па $9 \mid x^2 = 3$, што је контрадикција.

Следи нова верзија теореме.

**Теорема 14.** Нека је $f(x) \in \mathbb{Z}_p[x]$. Нека постоји $a_0 \in \mathbb{Z}_p$, тако да важи

$$|f(a_0)|_p < |f'(a_0)|_p^2.$$

Тада постоји јединствено $a \in \mathbb{Z}_p$, тако да важи

$$f(a) = 0 \qquad\qquad |a - a_0|_p < |f'(a_0)|_p.$$

Прецизније, тада важи и

(1) $|a - a_0|_p = \left|\dfrac{f(a_0)}{f'(a_0)}\right|_p$; (2) $|f'(a)|_p = |f'(a_0)|_p$.

**Коментар.** Јасно се види да је ова верзија теореме уопштење претходне, ако је $f(a_0) = 0$ и $p \nmid f'(a_0)$, тада је услов испуњен, а закључак следи из $|a - a_0|_p < 1$, што значи да $p \mid a - a_0$.

**Пример 37.** Сада можемо да испитамо и који непарни цели бројеви $a$ су квадрати у $\mathbb{Q}_2$. Свакако је да то не могу бити они $a \not\equiv 1$

(mod 8), јер то не важи ни у $\mathbb{Z}$, па можемо посматрати само прве три цифре развоја где добијамо контрадикцију. Претходна теорема нам ипак даје да бројеви $a \equiv 1 \pmod 8$ заиста јесу квадрати у $\mathbb{Q}_2$. Ако посматрамо полином $f(x) = x^2 - a$, тада $f(1) = 1 - a$ је дељиво са 8, док је $f'(1) = 2$, па је

$$|f(1)|_2 < |f'(1)|_2,$$

одакле, по претходном закључујемо да постоји неко $x \in \mathbb{Z}_2$, такво да $x^2 = a$. Ове резултате можемо спојити у следећи закључак.

Нека је $a = p^n \cdot u \in \mathbb{Q}_p$, при чему $u \in \mathbb{Z}_p^*$, $n \in \mathbb{Z}$. Тада је $a$ потпун квадрат у $\mathbb{Q}_p$ ако и само ако $2 \mid n$ и ако за непарне $p$, редукција $u$ модуло $p$ је квадрат у $\mathbb{F}_p$, док за $p = 2$ је услов $u \equiv 1 \pmod 8$.

Важи и слична варијанта теореме за полиноме више променљивих.

**Теорема 15.** Нека је $F(x_1, ..., x_n) \in \mathbb{Z}_p[x_1, ..., x_n]$. Нека постоји индекс $1 \leq i \leq n$ и тачка $(a_1, ..., a_n) \in \mathbb{Z}_p^n$ таква да је

$$|F(a_1, ..., a_n)|_p < \left| \frac{\partial F}{\partial x_i}(a_1, ..., a_n) \right|_p^2.$$

Тада $F$ има корен у $\mathbb{Z}_p^n$.

**Пример 38.** Посматрајмо једначину $2x^2 = 1 - 31y^4$. Тада она има решења у $\mathbb{Q}_2$, јер има решење по модулу 32, узмимо $(x, y) = (1, 1)$. Зашто гледамо модул 32? Ако означимо $F(x, y) = 2x^2 - 1 + 31y^4$, видимо да је

$$\left| \frac{\partial F}{\partial x}(1, 1) \right|_2 = \left| \frac{\partial F}{\partial y}(1, 1) \right| = |4|_2 = \frac{1}{4}.$$

Ово се квадрира у теореми, па нам треба прецизност већа од $2^4$, а најмања таква се добија када посматрамо по модулу $2^5$.

За крај, постоји и полиномска верзија Хенселове леме и то је последња коју наводимо.

**Теорема 16.** Нека је $f(x) \in \mathbb{Z}_p[x]$. Претпоставимо да постоје полиноми $g_1(x), h_1(x) \in \mathbb{Z}_p[x]$ такви да

(1) $g_1(x)$ је моничан;
(2) $g_1(x)$ и $h_1(x)$ су узајамно прости модуло $p$, тј. њихове редукције генеришу $\mathbb{F}_p[x]$;
(3) $f(x) \equiv g_1(x)h_1(x) \pmod{p}$ (коефицијент по коефицијент).
Тада постоје полиноми $g(x), h(x) \in \mathbb{Z}_p[x]$ такви да
(1) $g(x)$ је моничан;
(2) $g(x) \equiv g_1(x) \pmod{p}$ и $h(x) \equiv h_1(x) \pmod{p}$;
(3) $f(x) = g(x)h(x)$.

Између осталог, коришћењем Хенселових лема се доказује чувена **теорема Хасе-Минковског** позната као *локално-глобални принцип. Нетривијално решење* у овом случају је решење различито од оног које чине све нуле.

**Теорема 17.** Нека је $F(x_1, .., x_n) \in \mathbb{Q}[x_1, ..., x_n]$ квадратна форма, тј. хомоген полином степена 2. Једначина

$$F(x_1, ..., x_n) = 0$$

има нетривијална решења у $\mathbb{Q}$ ако и само ако има нетривијална решења у свим $\mathbb{Q}_p$ и $\mathbb{R}$.

Уз помоћ конгруенција и Хенселове леме се лако проверава да ли ће квадратна форма имати решења у $\mathbb{Q}_p$, док се за $\mathbb{R}$ то рутински провери. Интересантнији су случајеви већег степена.

**Пример 39.** Један од најчувенијих примера је једначина $3x^3+4y^3+5z^3 = 0$ која има нетривијална решења у свим $\mathbb{Q}_p$ и у $\mathbb{R}$, али нема нетривијална решења у $\mathbb{Q}$, то је Селмеров пример, а он је ту тврдњу доказао у [43]. Овај пример се може наћи и у чланку [17].

Још један пример је једначина

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

која има решења у свим $\mathbb{Q}_p$ и у $\mathbb{R}$ (очигледно!), а нема у $\mathbb{Q}$ (очигледно!). Средњи фактор се анлуира у $\mathbb{Q}_2$, док се први фактор анулира у $\mathbb{Q}_{17}$. За остале просте $p$ закључак следи из чињенице да су узајамно прости са бројевима 2, 17 и 34, а ова три броја не могу бити истовремено квадратни неостаци по модулу $p$.

## 3.3 Занимљиви $p$-адски резултати за број тачака на кривама

Сада ћемо се посветити уводу у презентацију улоге $p$-адских бројева у Диофантовим једначинама. Као што смо навели у првој глави, предност $\mathbb{Q}_p$ у односу на $\mathbb{Q}$ је у томе што је могуће много лакше решити једначине. На пример, уз неке мале услове, довољно је проверити да једначина има решења по модулу $p$, да би имала решење у $\mathbb{Q}_p$, док то свакако не важи за $\mathbb{Q}$. Ускоро стижемо и до тога.

**Дефиниција 25.** Посматрајмо хиперелиптичку криву $C : y^2 = F(x, z)$, над $\mathbb{Q}_p$, али тако да $F$ има коефицијенте у $\mathbb{Z}_p$. Тада можемо редуковати све коефицијенте полинома $F$ по модулу $p$ и тиме добити полином $\overline{F}(x, z)$, са коефицијентима у $\mathbb{F}_p$. Овај полином се назива *редукција полинома $F$ по модулу $p$*. Ако је $\overline{F}$ бесквадратан, онда кажемо да $C$ има *добру редукцију*. Крива $y^2 = \overline{F}(x, z)$ је глатка ако и само ако је полином $F$ бесквадратан (видети почетак дела 2.2). То је и разлог за назив добра редукција, крива има добру редукцију ако се редукује у глатку криву. Ако је још и $C$ дефинисана над $\mathbb{Q}$, при чему $F \in \mathbb{Z}[x, z]$, тада кажемо да $C$ има *добру редукцију у $p$* или *добру редукцију по модулу $p$* ако има добру редукцију када је посматрамо као криву над $\mathbb{Q}_p$. У супртоном, кажемо да $C$ има *лошу редукцију* (*у $p$*, ако је гледамо над $\mathbb{Q}$).

Присетимо се да, за полином $f(x)$ важи да има бар један вишеструки корен ако и само ако је његова дискриминанта $\operatorname{disc}(f) = 0$. А ако дехомогенизујемо ову нашу једначину, тј. посматрамо афини облик $y^2 = f(x)$, тада знамо да је она несингуларна (тј. глатка) ако и само ако $\operatorname{disc}(f) \neq 0$. Сада применом овог истог тврђења, само над пољем $\mathbb{F}_p$, над којим редукција има коефицијенте, долазимо до закључка да $f$ има добру редукцију (у $p$) ако и само ако $p \nmid \operatorname{disc}(f)$.

Према томе, за почетну једначину, $y^2 = F(x, z)$, провера је иста, само што узимамо $\operatorname{disc}(F)$ као дискриминанту бинарне форме $F$ и проверавамо да ли $p \mid \operatorname{disc}(F)$. Ако је почетна крива глатка, тј. $\operatorname{disc}(F) \neq 0$, и ако $F \in \mathbb{Z}[x, z]$, тада ће бити $\operatorname{disc}(F) \in \mathbb{Z}\backslash\{0\}$, одакле видимо да само коначан број простих бројева може делити $\operatorname{disc}(F)$, што значи да глатка крива $C$ има лошу редукцију само за коначно много простих бројева $p$.

Ако крива $C$, рода $g$, над $\mathbb{Q}_p$ (или $\mathbb{Q}$) има добру редукцију (у $p$), тада је њена редукција, коју означавамо са $\overline{C}$ опет хиперелиптичка крива рода $g$. Овако означавамо криву добијену редукцијом, чак и ако је то лоша редукција.

Сваку тачку $P = [x_0, y_0, z_0] \in C(\mathbb{Q}_p)$ можемо редуковати. Можемо скалирати координате, тако да $x_0, z_0 \in \mathbb{Z}_p$. Онда мора бити и $y_0 \in \mathbb{Z}_p$, што се види из једначине криве. Такође, из једначине криве, видимо и то да ако су $x_0$ и $z_0$ оба дељива са $p$, да то мора бити и $y_0$ и онда поделимо све са $p$. Овим поступком се можемо постарати да $x_0, y_0, z_0 \in \mathbb{Z}_p$ и да $p$ не дели оба од $x_0$ и $z_0$. Онда је $\overline{P} = [\overline{x_0}, \overline{y_0}, \overline{z_0}] \in \overline{C}(\mathbb{F}_p$ добро дефинисана тачка, јер нису у исто време $\overline{x_0} = \overline{z_0} = 0$. Стога, имамо добро дефинисано *редуктивно пресликавање*

$$\rho_p : C(\mathbb{Q}_p) \longrightarrow \overline{C}(\mathbb{F}_p), \quad P \mapsto \overline{P}.$$

Следеће тврђење је веома корисно у анализи $p$-адских тачака на кривама и показује једну од моћи Хенселове теореме.

**Тврђење 23.** Нека је $C : y^2 = F(x, z)$ глатка хиперелиптичка крива над $\mathbb{Q}_p$, таква да $F \in \mathbb{Z}_p[x, z]$. Нека њена редукција $\overline{C} : y^2 = \overline{F}(x, z)$ над $\mathbb{F}_p$ садржи глатку тачку $Q$, тада постоји тачка $P \in C(\mathbb{Q}_p)$ чија је редукција $\overline{P} = Q$.

**Доказ.** Доказујемо ово тврђење за било коју афину криву, а јасно је да можемо гледати само афине делове, како бисмо доказали тврђење за пројективне криве. Без губљења општости, можемо претпоставити да је тачка $Q = (0, 0)$, што постижемо дозвољеном променом координата - транслацијом. Такође, један од парцијалних извода у $Q$ не сме бити нула, због глаткости, па и то без губљења општости (иначе заменимо координате), можемо претпоставити да је парцијални извод по $y$. Дакле, нека $p \mid \dfrac{\partial f}{\partial y}(0, 0)$. Онда, множењем свега са $p$-адским инвертибилним елементом, можемо чак претпоставити да је $\dfrac{\partial f}{\partial y}(0, 0) = 1$. Тада је

$$g(y) = f(0, y) = pa_0 + y + a_2y^2 + ... + a_ny^n,$$

при чему $a_0, a_2, ..., a_n \in \mathbb{Z}_p$, одакле редукција полинома $g$ по модулу $p$ има прост корен $y = 0$. Применом Хенселове леме, закључујемо да постоји корен полинома $g$ $y_0 \in p\mathbb{Z}_p$. Тада се тачка $P = (0, y_0) \in C(\mathbb{Q}_p)$ редукује на тачку $Q$. Овим је доказ завршен.

Следећу теорему наводимо без доказа. Познатија (и прва верзија) је Хасеова теорема, која важи за елиптичке криве (тада је $g = 1$), а уопштио је Вејл касније на криве произвољног рода.

**Теорема 18.** (Хасе - Вејлова теорема) Нека је $C$ глатка, апсолутно несводљива пројективна крива, рода $g$, над коначним пољем $\mathbb{F}_q$, са $q$ елемената. Тада

$$|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}.$$

Као последицу, имамо следеће тврђење.

**Тврђење 24.** Нека је $C : y^2 = F(x, z)$ хиперелиптичка крива, рода $g$ и нека је $p > 4g^2 - 2$ прост број за који $C$ има добру редукцију. Тада је $C(\mathbb{Q}_p) \neq \emptyset$.

**Доказ.** Крива $\overline{C}$, редукција $C$ по модулу $p$ је из услова хиперелиптицка крива рода $g$, глатка, апсолутно несводљива и пројективна. Прво доказујемо да је $\overline{C}(\mathbb{F}_p) \neq \emptyset$. По Хасе-Вејловој теореми, $\#\overline{C}(\mathbb{F}_p) \geq p+1-2g\sqrt{p}$. Довољно је да докажемо да је $p+1-2g\sqrt{p} > 0$, за $p > 4g^2-2$. Пребацивањем $2g\sqrt{p}$ на другу страну и квадрирањем добијамо $p^2 + 2p + 1 > 4g^2p$, а ово је тачно због низа неједнакости $p^2 + 2p + 1 > p^2 + 2p = p(p + 2) > 4g^2p$. Сада знамо да постоји тачка $Q \in \overline{C}(\mathbb{F}_p)$. Сада по тврђењу 23, постоји тачка $P \in C(\mathbb{Q}_p)$, која се редукцијом модуло $p$ слика у $Q$, одакле закључујемо $C(\mathbb{Q}_p) \neq \emptyset$.

Важно је напоменути да је услов да крива има добру редукцију модуло $p$ заиста битан. Ево и примера зашто. Нека је $f \in \mathbb{Z}[x]$ моничан полином, степена $2g + 2$, чија редукција модуло $p$ је несводљив полином. Посматрајмо криву $C : y^2 = pf(x)^2$. Тада за сваки $\xi \in \mathbb{Z}_p$ важи $p \nmid f(\xi)$ (иначе би редукција $f$ по модулу $p$ имала нулу - први члан развоја $\xi$, а онда тај полином не би био несводљив). Тада $\mathrm{ord}_p(pf(\xi)) = 1$, па тај број не може бити потпун квадрат у $\mathbb{Q}_p$, дакле у овом случају нема решења. Ако $\xi \in \mathbb{Q}_p \backslash \mathbb{Z}_p$,

тада ће бити $\mathrm{ord}_p(f(\xi)) = -k(2g+2)$, јер ће члан $x^{2g+2}$ да доминира (остаће тај степен у имениоцу). Опет је $\mathrm{ord}_p(pf(\xi))$ непаран број, тако да ни у овом случају $pf(\xi)$ није потпун квадрат и нема решења. Стога, $C(\mathbb{Q}_p) = \emptyset$.

Присетимо се да ако је $C(\mathbb{Q}_p) = \emptyset$ или $C(\mathbb{R}) = \emptyset$, тада је и $C(\mathbb{Q}) = \emptyset$. Провера „локалних" тачака може дати да не постоје рационалне тачке на некој кривој, ако нађемо неко од поља $\mathbb{Q}_p$ или $\mathbb{R}$ такво да крива нема тачака у том пољу. Претходно тврђење је значајно због тога што нам каже да треба да проверимо „само" коначно много оваквих поља, јер крива $C$ може да има лошу редукцију само за коначно много простих бројева $p$. Зато наводимо једну дефиницију и корисну теорему након ње.

**Дефиниција 26.** Крива $C$ над $\mathbb{Q}$ *има локалне тачке свуда* ако $C(\mathbb{R}) \neq \emptyset$ и $C(\mathbb{Q}_p) \neq \emptyset$, за све просте бројеве $p$.

**Теорема 19.** Нека је $C$ хиперелиптичка крива рода $g$ над $\mathbb{Q}$, дата једначином $y^2 = F(x, z)$, где је $F \in \mathbb{Z}[x, z]$. Тада можемо проверити у коначно много корака да ли $C$ има локалне тачке свуда или не.

**Доказ.** Из претходног текста, знамо да је довољно да проверимо само коначно много простих бројева $p$. Прво одређујемо $\overline{C}(\mathbb{F}_p)$. Ако је $\overline{C}(\mathbb{F}_p) = \emptyset$, одмах знамо да је одговор на питање одричан (јер се свака тачка из $\mathbb{Q}_p$ се редукује на тачку у $\mathbb{F}_p$). Ако $\overline{C}(\mathbb{F}_p)$ садржи глатку тачку, тада знамо да је $C(\mathbb{Q}_p) \neq \emptyset$, по тврђењу 23. Остаје још да проверимо случај када за неко $p$ имамо тачке у $\overline{C}(\mathbb{F}_p)$ које нису глатке.

Афином променом координата (транслацијом) можемо да претпоставимо да тачка $Q = (0, \overline{\eta})$, тачка на афином делу криве $y^2 = f(x)$ није глатка. Доказаћемо тврђење за $p \neq 2$ (за $p = 2$ доказ иде слично са више посла). Тада због $\dfrac{\partial y^2}{\partial y} = 0$, следи да је $\overline{\eta} = 0$, такође $f$ мора имати бар двоструку нулу за $x = 0$. Дакле, једначина је облика

$$y^2 = pa_0 + pa_1x + a_2x^2 + ... + a_{2g+2}x^{2g+2} (= f(x)),$$

при чему $a_j \in \mathbb{Z}$, $0 \leq j \leq 2g+2$, и $a_{2g+2}$ може бити 0, уколико је реч о непарном степену.

Ако $p \nmid a_0$, тада је јасно да је $\mathrm{ord}_p(f(\xi)) = 1$, за све $\xi \in p\mathbb{Z}_p$, а онда се ова тачка (у ствари $x$-координата) не подиже у решење у $\mathbb{Q}_p$, јер би она морала живи у $p\mathbb{Z}_p$, јер је њена редукција модуло $p$ једнака 0.

Ако $p \mid a_0$, тј. $a_0 = pa_0'$ у $\mathbb{Z}_p$, тада мењамо $f$ са

$$f_1(x) = \frac{f(px)}{p^2} = a_0' + a_1 x + a_2 x^2 + pa_3 x^3 + ... + p^{2g} a_{2g+2} x^{2g+2}.$$

Даље, решавање настављамо тако што тражимо $\xi \in \mathbb{Z}_p$, такво да је $f(\xi)$ квадрат у $\mathbb{Z}_p$. Дакле, пребацили смо проблем на другу криву $C_1 : y^2 = f_1(x)$, изоморфну почетној. Сада настављамо процес и испоставља се да ће се процес у неком тренутку зауставити (може се пажљивим поступком показати да ако се процес не зауставља, тада $f$ има двоструки корен, што значи да крива није глатка, што је контрадиција), што значи да можемо да одредимо да ли се тачка $Q$ подиже у решење у $\mathbb{Q}_p$ или не.

## 3.4 Анализа $p$-адских степених редова

За почетак, као што смо радили и у реалној анализи, пре редова, испитујемо својства низова. У ствари, овде нам треба само једно својство, које не важи у реалној анализи, те је ово још један показатељ предности $p$-адске анализе. Нека $|\cdot|$ означава апсолутну вредност на одговарајућем пољу.

**Тврђење 25.** Низ $(a_n) \in \mathbb{Q}_p$ (или $(a_n) \in \mathbb{C}_p$) је Кошијев, дакле конвергентан, ако и само ако је

$$\lim_{n\to\infty} |a_{n+1} - a_n| = 0.$$

**Доказ.** Смер са лева на десно важи увек и то је јасно по неједнакости троугла

$$|a_{n+1} - a_n| \leq |a_{n+1} - \lim_{n\to\infty} a_n| + |\lim_{n\to\infty} a_n - a_n|.$$

Суштина је у смеру здесна на лево, јер ту користимо неархимедско својство, за $m > n$ важи

$$|a_m - a_n| = |a_m - a_{m-1} + a_{m-1} - a_{m-2} + ... + a_{n+1} - a_n| \leq$$

$$\leq \max\{|a_m - a_{m-1}|, |a_{m-1} - a_{m-2}|, ..., |a_{n+1} - a_n|\},$$

а ова вредност је довољно мала за довољно велике $n$ из претпоставке тврђења.

Сада наводимо следеће важно тврђење које опет користи специфичност неархимедске метрике.

**Тврђење 26.** Нека је низ $(a_n) \in \mathbb{Q}_p$ (или $(a_n) \in \mathbb{C}_p$) Кошијев, тј. конвергентан, такав да $A = \lim_{n\to\infty} a_n \neq 0$. Тада је низ $|a_n|$ константан почев од неког $n_0$ и при томе важи $|a_n| = |A|$, за $n > n_0$.

**Доказ.** За почетак докажимо да постоји неко $n_0 \in \mathbb{N}$ и $c > 0$, такво да је $|a_n| > c$, за све $n > n_0$. Уочимо било који број $0 < \varepsilon < |A|$ и тада по дефиницији лимеса постоји $n_0 \in \mathbb{N}_0$ такво да $|A - a_n| < \varepsilon$, за све $n > n_0$. Применом (обичне) неједнакости троугла добијамо $|A| - |a_n| \leq |A - a_n| < \varepsilon$, за $n > n_0$, односно $A - \varepsilon < |a_n|$, за све $n > n_0$, што је и требало доказати.

Са друге стране, за изабрано $c$ малопре важи да постоји неко $m_0 \in \mathbb{N}$, такво да за све $n, m > m_0$ важи $|a_n - a_m| < c$, јер је низ Кошијев. Тада је за све такве $m$ и $n$ $|a_n - a_m| < \max\{|a_n|, |a_m|\}$, при чему треба да приметимо да је то строга неједнакост, која се у неархимедској метрици може десити једино када $|a_n| = |a_m|$. Дакле, почев од неког $n_0$ важи да је низ $|a_n|$ константан, нека је та вредност $L$.

Сада пуштањем лимеса на неједнакости $|A| - |a_n| \leq |A - a_n|$ и $|a_n| - |A| \leq |A - a_n|$, добијамо $|A| - L \leq 0$ и $L - |A| \leq 0$, одакле мора бити и $L = |A|$, што завршава доказ овог тврђења.

Као директну последицу претходна два тврђења, имамо одговарајуће тврђење за редове у $\mathbb{Q}_p$ (односно $\mathbb{C}_p$).

**Тврђење 27.** Ред $\sum_{n=1}^{\infty} a_n$ конвергира ако и само ако $\lim_{n\to\infty} a_n = 0$. У том случају

$$\left|\sum_{n=1}^{\infty} a_n\right| \leq \max_{n\in\mathbb{N}} |a_n|.$$

**Доказ.** Први део је јасан из почетног тврђења, док други део ипак захтева проверу. Ако $\lim_{n\to\infty} a_n = 0$, тада су за било које $\varepsilon$ сви чланови низа, почев од неког $n_0$ мањи од њега. Ставимо $\varepsilon = |a_1|$, одакле је $\max_{n\in\mathbb{N}} |a_n| = \max\{|a_1|, |a_2|, ...|a_{n_0}|\}$, дакле постоји индекс $N$ такав да је $\max_{n\in\mathbb{N}} |a_n| = |a_N|$. Са друге стране, из претходног тврђења, знамо да низ парцијалних сума овог реда, почев од неког $m_0$ мора имати исту апсолутну вредност, одакле ту вредност има и збир целог реда, тј.

$$\left|\sum_{n=1}^{\infty} a_n\right| = \left|\sum_{n=1}^{m_0} a_n\right|.$$

Тада је

$$\left|\sum_{n=1}^{m_0} a_n\right| \leq \max\{|a_1|, |a_2|, ..., |a_{m_0}|\} \leq |a_N|,$$

одакле следи тражена неједнакост.

Наводимо сада неколико примера да увидимо разлику између конвергенције низова и редова у $\mathbb{R}$ и у $\mathbb{Q}_p$.

**Пример 40.** Низ $a_n = n!$ конвергира у сваком $\mathbb{Q}_p$ и то конвергира ка 0, што се јасно види из формуле за степен $p$ који дели $n!$, док у $\mathbb{R}$ очигледно не важи, јер овај низ тежи $+\infty$. Такође, ред $\sum_{n=1}^{\infty} n!$ конвергира у свим $\mathbb{Q}_p$, док у $\mathbb{R}$ нема смисла да тако нешто помислимо.

**Пример 41.** Низ $a_n = p^n$ конвергира ка 0 у $\mathbb{Q}_p$, док у $\mathbb{R}$ овај низ тежи $+\infty$. Овај низ не конвергира ни у једном другом $\mathbb{Q}_q$, $q \neq p$. Иако ова чињеница делује очигледно, ипак морамо нешто да напишемо

да бисмо је доказали.

Ту ћемо се помоћи елементарном теоријом бројева. Нека је $t$ поредак броја $p$ по модулу $q$ и нека $q^u \mid\mid p^t - 1$. Тада $q^{u+v} \mid p^k - 1$ ако и само ако $t \cdot q^v \mid k$. Одавде можемо да закључимо да низ $p^n$ није Кошијев у $\mathbb{Q}_q$, јер за $m > n$ важи

$$|p^m - p^n| = |p^n||p^{m-n} - 1| = |p^{m-n} - 1|,$$

а да би тај низ био Кошијев, мора $p^{m-n}-1$ бити дељиво са произвољно великим степеном $q$, међутим као што смо видели, тада се и $m$ и $n$ морају разликовати за велики број, па је то неизводљиво.

Сетимо се збира геометријске прогресије (када конвергира) $1 + x + x^2 + ... = \dfrac{1}{1-x}$. Тако ће се и овде испоставити $\displaystyle\sum_{n=1}^{\infty} p^n = \frac{1}{1-p}$. Доказ иде исто као и осталим случајевима

$$\left|\sum_{k=1}^{n} p^k - \frac{1}{1-p}\right| = \left|\frac{1-p^{n+1}}{1-p} - \frac{1}{1-p}\right| = \frac{|p^{n+1}|}{|1-p|} \to 0.$$

**Пример 42.** Низ $a_n = \dfrac{1}{n}$ је пример конвергентног реда, чији ред $\displaystyle\sum_{n=1}^{\infty} a_n$ не конвергира у $\mathbb{R}$. Као што видимо такав случај не може да наступи у $\mathbb{Q}_p$. Низ $a_n$, међутим, не конвергира у $\mathbb{Q}_p$, за било који прост број $p$. Један од разлога из којих то можемо да закључимо је и тај да постоје чланови који константно увећацају апсолутну вредност, јер $|a_{p^n}| = p^n$, а конвергентан низ, као што смо видели мора имати констатну апсолутну вредност почев од неког елемента или конвергира ка 0, што овде није случај, јер написане апсолутне вредности не теже 0. Дакле, имамо и низ који конвергира у $\mathbb{R}$, који не конвергира ни у једном $\mathbb{Q}_p$. Ако желимо да добијемо такав ред, довољно је да узмемо низ $b_n = \dfrac{1}{n^2}$.

**Пример 43.** Низ $a_n = \dfrac{n!}{(n!)! + 1}$ је низ који конвергира ка 0 у свим $\mathbb{Q}_p$, јер је бројилац овог разломка дељив са произвољно великим

степеном $p$, за довољно велико $n$, док именилац сигурно не може бити дељив са $p$, почев од неког члана, док је јасно да и у $\mathbb{R}$ овај низ конвергира ка 0. Слично је и са редовима $\sum_{n=1}^{\infty} a_n$ који конвергирају у свим наведеним пољима.

**Пример 44.** За крај овог низа примера, наведимо пример низа у $\mathbb{Q}_p$ (сада је $p$ фиксирано) који конвергира, али не ка 0. Уочимо $a_n = (1+p)^{p^n}$. Применимо помоћно тврђење из примера 41 - $p \mid\mid p+1-1$, одакле $p^{n+1} \mid (p+1)^{p^n} - 1$, што значи да је $|a_n - 1| \leq p^{-n-1}$ (заправо важи једнакост), одакле следи $\lim_{n\to\infty} a_n = 1$.

Наведимо без доказа (а лако се доказују, стандардним методама) два тврђења која важе у реалној анализи, па се преносе овде.

**Тврђење 28.** Нека је $(a_n) \in \mathbb{Q}_p$ (или $(a_n) \in \mathbb{C}_p$). Тада апсолутна конвергенција повлачи обичну конвергенцију, тј. ако $\sum_{n=1}^{\infty} |a_n|$ конвергира (у $\mathbb{R}$), тада и ред $\sum_{n=1}^{\infty} a_n$ у $\mathbb{Q}_p$ (односно $\mathbb{C}_p$).

**Тврђење 29.** Нека $a_{ij} \in \mathbb{Q}_p$ ($a_{ij} \in \mathbb{C}_p$) су такви да за свако $\varepsilon > 0$ постоји $n_0 \in \mathbb{N}$ такав да

$$\max(i,j) > n_0 \implies |a_{ij}| < \varepsilon.$$

Тада можемо заменити поредак сабирања, тј.

$$\sum_{i=1}^{\infty} \left( \sum_{j=1}^{\infty} a_{ij} \right) = \sum_{j=1}^{\infty} \left( \sum_{i=1}^{\infty} a_{ij} \right),$$

дакле, оба реда конвергирају и збир им је исти.

Прелазимо на $p$-адске степене редове. Наравно, то су редови облика

$$f(x) = \sum_{n=1}^{\infty} a_n x^n$$

при чему $a_n \in \mathbb{Q}_p$ (или $a_n \in \mathbb{C}_p$) и они конвергирају за све $x \in \mathbb{Q}_p$ ($x \in \mathbb{C}_p$) за које је $\lim\limits_{n\to\infty} |a_n x^n| = 0$. Одавде брзо можемо да увидимо да важи исто као и у до сада познатим случајевима, да је *полупречник конвергенције степеног реда*

$$R = \frac{1}{\limsup \sqrt[n]{|a_n|}}.$$

**Тврђење 30.** Нека је $f(x) = \sum\limits_{n=1}^{\infty} a_n x^n$ степени ред у $\mathbb{Q}_p$ (или $\mathbb{C}_p$), чији је полупречник конвергенције (који може бити и 0 и $\infty$)

$$R = \frac{1}{\limsup \sqrt[n]{|a_n|}}.$$

(1) Ако $R = 0$, тада $f(x)$ конвергира само за $x = 0$.
(2) Ако $R = \infty$, тада $f(x)$ конвергира за све $x \in \mathbb{Q}_p$ (или $x \in \mathbb{C}_p$)
(3) Ако $0 < R < \infty$, тада $f(x)$ конвергира за све $|x| < R$ и дивергира за све $|x| > R$.
(4) За $|x| = R$, $f(x)$ конвергира ако и само ако $\lim\limits_{n\to\infty} |a_n| R^n = 0$.

Приметимо још једну разлику у односу на анализу на коју смо навикли. У реалној или комплексној анализи степени ред на граници круга конвергенције не мора да стално конвергира или да стално дивергира, међутим овде је управо то случај, или конвергира за све те тачке, или дивергира свуда на граници.

**Пример 45.** За степени ред $f(x) = \sum\limits_{n=1}^{\infty} a_n x^n \in \mathbb{Z}_p[[x]]$ важи да конвергира на $p\mathbb{Z}_p$. Ово се одмах види, из услова је $|x| < 1$ и $|a_n| \leq 1$, одакле је $\lim_{n\to\infty} |a_n x^n| = 0$.

**Пример 46.** Степени ред $\sum\limits_{n=1}^{\infty} p^n x^n$ има полупречник конвергенције $p$, одакле знамо да конвергира за $|x| < p$ и дивергира за $|x| > p$. Дивергира и за $|x| = p$, јер је тада апсолутна вредност општег члана реда 1.

Слично, степени ред $\sum_{n=1}^{\infty} \frac{x^n}{p^n}$ полупречник конвергенције $\frac{1}{p}$ и конвергира ако и само ако $|x| < \frac{1}{p}$.

**Пример 47.** Сећамо се познатих развоја у реалној анализи $\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$ и $\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$. И овде можемо да дефинишемо исто, докле год ови редови конвергирају, дакле треба одредити полупречнике конвергенције за наведене развоје.

Прво одређујемо за логаритам - треба израчунати

$$\limsup \sqrt[n]{\left|\frac{1}{n}\right|} = \limsup p^{\frac{\operatorname{ord}_p n}{n}} = 1,$$

јер низ $\frac{\operatorname{ord}_p n}{n}$ тежи 0, због чињенице да је $\operatorname{ord}_p n \leq \log_p n$. Само треба проверити шта се дешава за $|x| = 1$, а тада $\left|(-1)^n \frac{x^n}{x}\right| = \left|\frac{1}{n}\right| \geq 1$, па ред дивергира. Закључак је да степени развој логаритма конвергира за $|x| < 1$, те је за такве $x$ та функција добро дефинисана. Ако радимо над $\mathbb{Q}_p$, тада је $\log : 1 + p\mathbb{Z}_p \longrightarrow \mathbb{Q}_p$.

Сада ћемо да урадимо исти посао за експоненцијалну функцију. У $\mathbb{R}$ добро знамо да овај степени ред конвергира за све $x$, због $n!$ у имениоцу, међутим овде нам то мало отежава посао. Означимо

$$S_n = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] = \sum_{k=1}^{[\log_p n]} \left[\frac{n}{p^k}\right].$$

Са једне стране је

$$S_n \leq \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p(1-\frac{1}{p})} = \frac{n}{p-1},$$

док са друге стране

$$S_n = \sum_{k=1}^{\infty} \left(\frac{n}{p^k} - \left\{\frac{n}{p^k}\right\}\right) \geq \sum_{k=1}^{\infty} \frac{n}{p^k} - \log_p n =$$

$$= \frac{n\left(1 - \frac{1}{p^{[\log_p n]}}\right)}{p-1} - \log_p n.$$

Поделимо са $n$ обе неједнакости и пустимо да $n$ тежи бесконачно, одакле по теореми два полицајца и лопову добијамо

$$\lim_{n\to\infty} \frac{S_n}{n} = \frac{1}{p-1}.$$

Сада је лако одредити полупречник конвергенције

$$R = \frac{1}{\limsup \sqrt[n]{\left|\frac{1}{n!}\right|}} = \frac{1}{\limsup p^{\frac{S_n}{n}}} = p^{-\frac{1}{p-1}}.$$

Сличним рачуном се проверава да за $|x| = p^{-\frac{1}{p-1}}$ ред дивергира одакле степени ред експоненцијалне функције конвергира само за $|x| < p^{-\frac{1}{p-1}}$, што је значајна разлика у односу на оно са чим смо се до сада сретали. Приметимо да и $\exp(x)$ конвергира на мањем скупу него $\log(1+x)$!

Сетимо се и познатих идентитета који важе за ове функције

$$\log((1+x)(1+y)) = \log(1+x) + \log(1+y),$$

$$\exp(x+y) = \exp(x)\exp(y),$$

$$\log(\exp(x)) = 1 + x.$$

И овде важе ови идентитети на доменима где су дефинисани. То се испоставља из следећег разлога, ови идентитет важе над $\mathbb{R}$ што значи када развијемо у степени ред обе стране једнакости морамо да добијемо идентички исте степене редове! Зато само треба проверити када су над $p$-адским пољима дефинисани идентитети, а то се брзо проверава да су у сва три идентитета домени на левој и десној страни исти, у првом $|x| < 1$, $|y| < 1$, у другом $|x| < p^{-\frac{1}{p-1}}$, $|y| < p^{-\frac{1}{p-1}}$, у трећем $|x| < p^{-\frac{1}{p-1}}$. Међутим, ако желимо обрнуту једнакост која каже да су логаритамска и експоненцијална функција инверзне, тј.

$$\exp(\log(1+x)) = 1 + x,$$

ипак није довољно да посматрамо $|x| < 1$, јер лева страна не мора да буде дефинисана. Испоставља се да је довољно онакве $x$ за које је дефинисана експоненцијална функција, тј. $|x| < p^{-\frac{1}{p-1}}$.

**Пример 48.** Једна занимљива примена ових степених редова је на задатак из елементарне теорије бројева. Следи текст задатка.

Нека је $M$ било који природан број. Доказати да постоји природан број $n$ такав да је бројилац сведеног разломка

$$2 + \frac{2^2}{2} + ... + \frac{2^n}{n}$$

дељив са $2^M$.

Видимо да овај број доста подсећа на развој логаритма. Из формуле за овакве бројеве је јасно да треба да убацимо $x = -2$, што значи да нам поље у којем је $|-2| < 1$. То наравно важи у $\mathbb{Q}_2$, а и логично је да посматрамо то поље, јер тражимо дељивост са произвољно великим $2^M$, односно да број буде што мањи у овом пољу. По својству логаритма $2\log(-1) = \log 1 = 0$, тј. $\log(-1) = 0$. Дакле ред

$$\log(1 + (-2)) = \sum_{n=1}^{\infty} -\frac{2^n}{n}$$

конвергира ка 0 у $\mathbb{Q}_2$, а ово специјално значи да нека његова парцијална сума мора бити норме мање од $2^{-M}$, тј. да је бројилац дељив са $2^M$, што је и требало доказати.

**Пример 49.** Слично као и претходне функције, можемо развити и

$$(1 + x)^\alpha = \sum_{n=1}^{\infty} \binom{\alpha}{n} x^n.$$

Посматраћемо само случај када $\alpha \in \mathbb{Z}_p$. Доказаћемо да овај ред конвергира за $|x| < 1$, што је коначно неки очекиван резултат, али морамо да будемо пажљиви, у неким случајевима је полупречник конвергенције и већи, а у неким не, при чему нећемо то овде дискутовати. Довољно је да докажемо да је

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)...(\alpha-n+1)}{n!} \in \mathbb{Z}_p.$$

Посматрајмо полином

$$P(x) = \frac{x(x-1)...(x-n+1)}{n!}.$$

Полином је непрекидна функција (пошто имамо $p$-адску метрику, можемо да говоримо о непрекидним функцијама). Знамо да је за $\alpha \in \mathbb{Z}$, $P(\alpha) \in \mathbb{Z}$. Такође, знамо и да је затворење (у односу на $p$-адску метрику) скупа $\mathbb{Z}$ скуп $\mathbb{Z}_p$, одакле непрекидна функција мора сликати затоврење домена у затворење слике, тј. $P : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$, што смо и желели да покажемо.

**Пример 50.** Некада морамо бити пажљиви са $p$-адским степеним редовима, јер могу да конвергирају другачије у $\mathbb{R}$ и $\mathbb{Q}_p$. На пример, пођимо од једнакости $\left(1+\frac{7}{9}\right)^{\frac{1}{2}} = \frac{4}{3}$. Радићемо у пољу $\mathbb{Q}_7$. Тада $\frac{1}{2} \in \mathbb{Z}_7$ и $\left|\frac{7}{9}\right| < 1$, одакле можемо да применимо претходни пример и да развијемо корен у степени ред

$$\frac{4}{3} = \left(1+\frac{7}{9}\right)^{\frac{1}{2}} = 1 + \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} \left(\frac{7}{9}\right)^n \in 1 + 7\mathbb{Z}_7.$$

Али,

$$\left|\frac{4}{3} - 1\right| = \left|\frac{1}{3}\right| = 1,$$

а по претходном би требало да буде

$$\left|\frac{4}{3} - 1\right| < 1!$$

Где је грешка? Испоставља се да иако овај ред конвергира у $\mathbb{R}$ и у $\mathbb{Q}_7$, то не мора бити исти број! У $\mathbb{R}$, овај ред јасно конвергира ка $\frac{4}{3}$, међутим у $\mathbb{Q}_7$, овај ред конвергира ка другом корену једначине $x^2 - \frac{16}{9} = 0$ - ка $-\frac{4}{3}$. Разлог се види из претходног текста, то је корен ове једначине, који је у $1 + 7\mathbb{Z}_7$, за $\frac{4}{3}$ смо видели да то не

важи, док за $-\frac{4}{3}$ заиста важи

$$\left|-\frac{4}{3}-1\right| = \left|\frac{7}{3}\right| = \frac{1}{7}.$$

Након ових занимљивих примера, који позивају на опрез, враћамо се нечему што нам треба у доказу главне (Колеманове) теореме. Желимо да анализирамо број нула степених редова у $\mathbb{Q}_p$. При неким посебним условима (који ће за наше потребе бити испуњени), имамо следећу теорему.

**Теорема 20.** Нека је $l(t) \in \mathbb{Q}[[t]]$ степени ред, такав да његов формални извод $w(t) \in \mathbb{Z}[[t]]$, тј. да има коефицијенте у $\mathbb{Z}_p$. Нека је слика $w(t)$ у $\mathbb{F}_p[[t]]$ облика $\overline{w}(t) = up^m + ...$, за неко $u \in \mathbb{F}_p^*$. Тада $l(t)$ конвергира на $p\mathbb{Z}_p$. Ако $p > m+2$, тада $l(t)$ има највише $m+1$ нулу у $p\mathbb{Z}$.

**Доказ теореме.** Ово је приступ из лекција професора Штола [53]. Занимљив је из разлога што доказујемо још нека корисна тврђења успут. Кренимо од првог тврђења.

**Тврђење 31.** Нека је $0 \neq l(t) = \sum_{n=0}^{\infty} a_n t^n \in \mathbb{Q}[[t]]$, такав да $\lim_{n\to\infty} a_n = 0$ у $p$-адској метрици. Нека је $v_0 = \min\{\mathrm{ord}_p(a_n) \mid n \in \mathbb{N}_0\}$ и $N = \max\{n \in \mathbb{N}_0 \mid \mathrm{ord}_p(a_n) = v_0\}$. Тада постоји константа $c \in \mathbb{Q}_p^*$, монични полином $q \in \mathbb{Z}_p[t]$, степена $N$ и степени ред $h(t) = \sum_{n=0}^{\infty} b_n t^n \in 1 + pt\mathbb{Z}_p[[t]]$, са $\lim_{n\to\infty} b_n = 0$ у $p$-адској метрици, тако да важи

$$l(t) = cq(t)h(t).$$

**Доказ.** Ради једноставности, можемо да скалирамо степени ред са $a_N^{-1}$ и да претпоставимо да је $v_0 = 0$ и $a_N = 1$. Тада је $l(t) \in \mathbb{Z}_p[[t]]$. Услов $\lim_{n\to\infty} a_n = 0$ користимо да закључимо да је слика $l_m(t)$ степеног реда $l(t)$ редукцијом у $\mathbb{Z}/p^m\mathbb{Z}[[t]]$ полином, јер ће, почев

од неког члана сви коефицијенти $a_n$ бити дељиви са $p^m$. Такође, тај услов нам аутоматски даје конвергенцију овог реда на $\mathbb{Z}_p$.

Идеја нам је да конструишемо низове:
(1) константи $c_m \in (\mathbb{Z}/p^m\mathbb{Z})^*$;
(2) моничних полинома $q_m(t) \in \mathbb{Z}/p^m\mathbb{Z}[t]$, степена $N$;
(3) полинома $h_m(t) \in \mathbb{Z}/p^m\mathbb{Z}[t]$, при чему $h_m(t) \equiv 1 \pmod{pt}$,
који задовољавају

$$l_m(t) = c_m q_m(t) h_m(t)$$

и тако да се тројка $(c_{m+1}, q_{m+1}(t), h_{m+1}(t))$ редукцијом по модулу $p^m$ редукује на тројку $(c_m, q_m(t), h_m(t))$.

Тада, по добро познатом поступку конструкције $p$-адских бројева, инверзним лимесом, долазимо до јединствене константе $c \in \mathbb{Z}^*$, $q(t) \in \mathbb{Z}_p[t]$, моничан полиноом степена $N$ и $h(t) \in 1 + pt\mathbb{Z}_p[[t]]$, такви да се редукцијом по модулу $p^m$ добијају баш $(c_m, q_m(t), h_m(t))$ и важи

$$l(t) = cq(t)h(t).$$

Овај поступак, очекивано, спроводимо математичком индукцијом. За базу индукције, тј. $m = 1$, узмимо $c_1 = 1$, $q_1(t) = l_1(t)$ и $h_1(t) = 1$. Једино што треба проверити је да ли $q_1(t)$ задовољава услове, а то јесте из разлога што је $a_N = 1$ и сви коефицијенти после $N$-тог места су дељиви са $p$, по услову тврдјења, па је $l_1(t)$ моничан полином $N$-тог степена. Претпоставимо да смо конструисали $(c_m, q_m(t), h_m(t))$, за неко $m \in \mathbb{N}$ и желимо да конструишемо $(c_{m+1}, q_{m+1}(t), h_{m+1}(t))$. Уочимо произвољно подизање $(\tilde{c}_{m+1}, \tilde{q}_{m+1}(t), \tilde{h}_{m+1}(t))$ уређене тројке $(c_m, q_m(t), h_m(t))$ по модулу $\mathbb{Z}/p^{m+1}\mathbb{Z}$ (тј. редукција прве тројке по модулу $p^m$ даје другу тројку), али да је $\tilde{q}_{m+1}(t)$ моничан степена $N$ и $\tilde{h}_{m+1}(t) \equiv 1 \pmod{pt}$. За тражене $(c_{m+1}, q_{m+1}(t), h_{m+1}(t))$ важи да се од уочених $(\tilde{c}_{m+1}, \tilde{q}_{m+1}(t), \tilde{h}_{m+1}(t))$ не разликују по модулу $p^m$, тј. мора да важи

$$c_{m+1} = \tilde{c}_{m+1} + p^m\gamma,$$

$$q_{m+1} = \tilde{q}_{m+1} + p^m\kappa(t),$$
$$h_{m+1} = \tilde{h}_{m+1} + p^m\eta(t),$$

при чему је $\gamma \in \mathbb{Z}/p\mathbb{Z}$, $\kappa(t) \in \mathbb{Z}/p\mathbb{Z}[t]$ је полином степена мањег од $N$ (јер је већ $\tilde{q}_{m+1}$ моничан степена $N$, па да то не угрозимо) и

$\eta(t) \in \mathbb{Z}/p\mathbb{Z}[t]$, при чему $\eta(0) = 0$, да би слободан члан полинома $h_{m+1}(t)$ остао 1. Такође је

$$l_{m+1}(t) - \tilde{c}_{m+1}\tilde{q}_{m+1}(t)\tilde{h}_{m+1}(t) = p^m d(t),$$

за неки полином $d(t) \in \mathbb{Z}/p\mathbb{Z}[t]$.

Сада је жељени услов (по модулу $p^{m+1}$) $l_{m+1}(t) = c_{m+1}q_{m+1}(t)h_{m+1}(t)$ екивавелантан са

$$l_{m+1}(t) = (\tilde{c}_{m+1} + p^m\gamma)(\tilde{q}_{m+1} + p^m\kappa(t))(\tilde{h}_{m+1} + p^m\eta(t)).$$

Имајући на уму да се ради по модулу $p^{m+1}$, ово је еквивалентно са

$$l_{m+1}(t) = \tilde{c}_{m+1}\tilde{q}_{m+1}(t)\tilde{h}_{m+1}(t)+p^m(\gamma\tilde{q}_{m+1}(t)\tilde{h}_{m+1}(t)+\kappa(t)\tilde{c}_{m+1}\tilde{h}_{m+1}(t)+\eta(t)\tilde{c}_{m+1}\tilde{q}_{m+1}(t)).$$

Даље је (по модулу $p^{m+1}$)

$$p^m(d(t) - \gamma\tilde{q}_{m+1}(t)\tilde{h}_{m+1}(t) + \kappa(t)\tilde{c}_{m+1}\tilde{h}_{m+1}(t) + \eta(t)\tilde{c}_{m+1}\tilde{q}_{m+1}(t)) = 0,$$

односно у $\mathbb{Z}/p\mathbb{Z}$

$$d(t) = \gamma\tilde{q}_{m+1}(t)\tilde{h}_{m+1}(t) + \kappa(t)\tilde{c}_{m+1}\tilde{h}_{m+1}(t) + \eta(t)\tilde{c}_{m+1}\tilde{q}_{m+1}(t).$$

Пошто се редукује по модулу $p$, тада се $\tilde{q}_{m+1}(t)$ редукује у $q_1(t) = l_1(t)$, $\tilde{c}_{m+1}$ се редукује у $c_1 = 1$ и $\tilde{h}_{m+1}(t)$ се редукује у $h_1(t) = 1$. Једначина постаје

$$d(t) = \gamma l_1(t) + \kappa(t) + l_1(t)\eta(t) = (\gamma + \eta(t))l_1(t) + \kappa(t).$$

Приметимо да је $\deg\kappa(t) < N = \deg l_1(t)$, одакле ова једначина представља еуклидско дељење у прстену полинома над пољем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. При томе, ми знамо експлицитно полиноме $d_(t)$ и $l_1(t)$, одакле их можемо еуклидски поделити и добити јединствен количник $\gamma + \eta(t)$ и остатак $\kappa(t)$. Још, због услова $\eta(0) = 0$, добијамо јединственост тражених $\gamma$ и $\eta(t)$, одакле смо и њих експлицитно одредили и самим тим смо конструисали тројку $(c_{m+1}, q_{m+1}(t), h_{m+1}(t))$ која задовољава све тражене услове. Овим је доказ индкуцијом, као и целог тврђења, готов.

Као последицу овог тврђења, имамо следеће корисно тврђење.

**Тврђење 32.** Нека је, као у претходном тврђењу, $0 \neq l(t) = \sum_{n=0}^{\infty} a_n t^n \in \mathbb{Q}[[t]]$ степени ред такав да $\lim_{n\to\infty} a_n = 0$ у $p$-адској метрици и означимо $v_0 = \min\{\mathrm{ord}_p(a_n) \mid n \in \mathbb{N}_0\}$ и $N = \max\{n \in \mathbb{N}_0 \mid \mathrm{ord}_p(a_n) = v_0\}$. Тада је број нула степеног реда $l(t)$ у $\mathbb{Z}_p$ највише $N$.

**Доказ.** По претходном тврђењу, закључујемо да постоје $c \in \mathbb{Q}_p^*$, монични полином $q \in \mathbb{Z}_p[t]$, степена $N$ и степени ред $h(t) \in 1 + pt\mathbb{Z}_p[[t]]$, тако да важи $l(t) = cq(t)h(t)$. Видимо да $h(t)$ нема нула у $\mathbb{Z}_p$, јер $p \nmid 1$. Тако да све нуле $l(t)$ су уједно и нуле полинома $q(t)$, који их има највише $N$, јер је тог степена и над прстеном је који је домен целих.

**Коментар.** Ако знамо како се $p$-адска валуација продужава са $\mathbb{Q}_p$ на $\overline{\mathbb{Q}_p}$, онда можемо рећи да за све корене $\alpha \in \overline{\mathbb{Q}_p}$ важи $v_p(\alpha) \geq 0$. То лако закључујемо из тога што је $\alpha$ корен моничног полинома са коефицијентима ненегативне валуације, па би у супротном случају $v_p(q(\alpha)) = Nv_p(\alpha) < 0$, по ултраметричкој неједнакости, што је контрадикција.

Прелазимо на доказ теореме.

**Завршетак доказа.** Напишимо

$$l(t) = l_0 + l_1 t + ... + l_n t^n + ...$$

и

$$w(t) = w_0 + w_1 t + ... + w_n t^n + ...,$$

тада је $w_n = (n+1)l_{n+1}$. По услову теореме је $\mathrm{ord}_p(w_n) \geq 0$. Из дефиниције видимо да је

$$\mathrm{ord}_p(n+1) \leq \log_p(n+1) \leq C \log n,$$

за неку константу $C > 0$ и све $n \in \mathbb{N}$. Одавде је $\mathrm{ord}(l_n) \geq -C \log n$. Тада, за било које $\tau \in p\mathbb{Z}_p$, тада $\mathrm{ord}_p(\tau) \geq 1$, па $\mathrm{ord}_p(l_n\tau^n) \geq n - C \log n$, што тежи $+\infty$ кад $n \to \infty$, одакле у $p$-адској топологији $\lim_{n\to\infty} l_n\tau^n = 0$ а ово управо значи да ред конвергира. Тиме је први део тврђења доказан.

За други део тврђења, посматрајмо степени ред

$$l'(t) = l(pt) = l_0 + pl_1t + ... + p^n l_n t^n + ...$$

Докажимо да је за овај ред, $N$ из претходног тврђења мање од $m+2$. Прво испитајмо за $m+1$:

$$\mathrm{ord}_p(p^{m+1}l_{m+1}) = m+1+\mathrm{ord}_p(l_{m+1}) = m+1+\mathrm{ord}_p(w_m) - \mathrm{ord}_p(m+1) =$$

$$= m+1-\mathrm{ord}_p(m+1) \leq m+1,$$

јер је $\mathrm{ord}_p(w_m) = 0$, пошто се $w_m$ редукцијом по модулу $p$ слика у 0, по услову теореме. Сада, нека је $n > m$, па

$$\mathrm{ord}_p(p^{n+1}l_{n+1}) = n+1+\mathrm{ord}_p(w_n) - \mathrm{ord}_p(n+1) \geq n+1-\mathrm{ord}_p(n+1).$$

Желимо (и довољно је) да докажемо $n+1-\mathrm{ord}_p(n+1) > m+1$, односно $n-\mathrm{ord}_p(n+1) > m$. Ако је $\mathrm{ord}_p(n+1) = 0$, тврђење је јасно због $n > m$. Иначе, нека је $\mathrm{ord}_p(n+1) = e$, за неко $e \in \mathbb{N}$. Тада је $p^e \leq n+1$, па је довољнода докажемо да је $m+1+e < p^e$. Ово тврђење рутински доказујемо индукцијом, где је базни случај $e = 1$ управо претпоставка тврђења $p > m+2$, а даље индуктивни корак следи тривијално, пошто лева страна расте за 1, а десна расте $p$ пута.

Дакле, сигурно је $\mathrm{ord}_p(p^{m+1}l_{m+1}) < \mathrm{ord}_p(p^n l_n)$, за све $n > m+1$, па овакви бројеви не могу бити индекс (највећег) чалана са најмањом $p$-адском вредношћу. Зато је $N \leq m+1$. Сада применом претходног тврђења закључујемо да $l_1(t)$ има највише $m+1$ нулу у $\mathbb{Z}_p$, а из дефиниције $l_1(t) = l(pt)$, то је еквивалентно са тим да $l$ има највише $m+1$ нулу у $p\mathbb{Z}_p$, што је и требало доказати.

**Напомена.** Доказ се може спровести математичком индукцијом уз помоћ познатих својстава $p$-адских степених редова. Доказ се може наћи у [2] и [25].

# 4 Јакобијан криве

## 4.1 Увод и својства Јакобијана криве

**Препоручена литература:** Овај текст у највећој мери прати [53], док се приступ сличан овоме може наћи и у [21], [37]. За озбиљније проучавање Јакобијана су корисне књиге [14], [34], [33].

Нека је $C$ глатка, пројективна и апсолутно несводљива крива, рода $g$. Подсетимо се да је Пикарова група степена 0 $\mathrm{Pic}^0(C)$ над пољем $K$ (у ознаци $\mathrm{Pic}^0_K(C)$) је, као што и очекујемо, група која се састоји из елемената групе $\mathrm{Pic}^0(C)$ који су фиксирани дејством Галуаове групе $\mathcal{G}_{\overline{K}/K}$. Та група има једно лепо својство, а то је да се може описати као специјална врста алгебарских варијетета који се називају Абелови варијетети, које означавамо са $J(K)$, а због идентификације пишемо

$$J(K) = \mathrm{Pic}^0_K(C),$$

при чему $J(K)$ називамо *Јакобијаном* криве $C$ над пољем $K$. Ако се зна над којим пољем мислимо, онда ћемо Јакобијан означавати само кратко са $J$. Међутим, тај ниво знања алгебарске геометрије је сувише висок за тренутне потребе и могућности, одакле ћемо се овде Јакобијаном криве бавити само као групом дивизора, што ће за сада и бити довољно.

**Пример 51.** Ако је крива рода $g = 0$, тада је њен Јакобијан тривијалан, тј. само једна тачка, тј. $J = \{0\}$. То следи из чињенице да је крива рода 0 изоморфна са $\mathbb{P}^1$, а на $\mathbb{P}^1$ сваки дивизор степена 0 је уједно и главни, по примеру број 16, одакле је $\mathrm{Pic}^0(C)$ тривијална група.

**Пример 52.** Ако је крива рода $g = 1$ и има $K$-рационалну тачку, тј. ако је она елиптичка крива, тада знамо (има у [51]) да је $\mathrm{Pic}^0(C) \cong C$, па у овом случају можемо идентификовати Јакобијан са самом кривом.

Из претходних примера видимо да су најзанимљивији случајеви када је род $g \geq 2$.

Ако је $P_0 \in C(K)$, тада постоји важно пресликавање $i : C \longrightarrow J$ које шаље тачке $P \in C(K)$ у класу дивизора $P - P_0$ у $\mathrm{Pic}^0(C)$, коју означавамо $[P - P_0]$. Ово пресликавање ће бити морфизам алгебарских варијетета, а за $g > 0$ има још једно веома корисно својство - инјективно је!

Заиста, ако $[P - P_0] = [Q - Q_0]$, тада $[P - Q] = 0$, тј. постоји функција $f \in \overline{K}(C)$ која има само једну нулу и само један пол. У [20] је доказано тврђење да је укупан број нула функције $f$, рачунајући вишеструкост једнак степену раширења $[\overline{K}(C) : \overline{K}(f)]$, а како $f$ има само једну нулу вишеструкости 1, одавде закључујемо да је $\overline{K}(C) = \overline{K}(f)$, тј. свака функција из $\overline{K}(C)$ се добија као рационална функција по $f$. Сада уочимо функцију $\phi : C \longrightarrow \mathbb{P}^1$, дефинисану на следећи начин

$$\phi(X) = \begin{cases} [f(X), 1], & X \neq Q \\ [1, 0], & X = Q. \end{cases} \tag{5}$$

Одвојено дефинишемо $\phi$ за $Q$, јер $f$ има пол у $Q$, али то је истог духа као да смо написали $[f(Q), 1]$. Стога, за произвољну рационалну функцију $\dfrac{F(X,Y)}{G(X,Y)} \in \overline{K}(\mathbb{P}^1)$ је $\phi^* \left(\dfrac{F}{G}\right) \in \overline{K}(C)$ за које важи

$$\phi^* \left(\frac{F}{G}\right)(X) = \frac{F(\phi(X))}{G(\phi(X))} = \frac{F[f(X), 1]}{G[f(X), 1]}.$$

$F$ и $G$ су произвољни хомогени полиноми истог степена, одакле на овај начин можемо добити сваку рационалну функцију по $f$ дозвољену у пројективним просторима, што значи да је $\overline{K}(C) = \phi^*(\overline{K}(\mathbb{P}^1))$, одакле је $\phi$ пресликавање степена 1, а по тврђењу 6 је то и изоморфизам, одакле је $C$ изоморфна $\mathbb{P}^1$, што значи да је $C$ рода 0, а ово је контрадикција.

Одавде можемо закључити да ако желимо да одредимо скуп $C(K)$, можемо да одредимо скуп $J(K) \cap i(C)$, одакле ћемо сазнати $C(K)$. Предност је што увођењем Јакобијана добијамо додатну структуру и нове информације. На пример, ако се испостави да је $J(K) = \{0\}$, тада одмах закључујемо да је $C(K) = \{P_0\}$.

За Јакобијане важи иста теорема као за елиптичке криве, коју називамо Мордел-Вејлова теорема. Навешћемо је без доказа.

**Теорема 21.** Нека је $K$ бројно поље и $J(K)$ Јакобијан криве $C$. Тада је група $J(K)$ коначно генерисана.

Ово нам даје информацију да је

$$J(K) \cong \mathbb{Z}^r \oplus J(k)_{\text{tors}},$$

за неко $r \in \mathbb{N}_0$, које се назива *ранг Јакобијана*, а понекад се назива и *Мордел-Вејлов ранг*. Као и код елиптичких кривих, лакше је одредити торзиони део, док се за ранг може успети само у појединачним случајевима. Идемо ка томе да истражимо Јакобијан криве.

**Тврђење 33.** Нека је $C$ глатка, пројективна, апсолутно несводљива крива рода $g$ са фиксираном $K$-рационалном тачком $P_0$ $inC(K)$. Тада а свако $Q \in J(K)$, постоји јединствени ефективни дивизор најмањег степена $D_Q \in \text{Div}_K(C)$, такав да $Q = [D_Q - (\deg D_Q)P_0]$. Тада важи $\deg D_Q \leq g$.

**Доказ.** Нека је $D \in \text{Div}^0(C)$ дивизор који представља $Q$, тј. за који је $Q = [D]$. Посматрајмо просторе $L_n = L(D + nP_0)$, за $n \in \mathbb{Z}$, $n \geq -1$. По дефиницији ових простора је $L_{-1} = \{0\}$, јер је $\deg(d - P_0) = -1$ (тврђење 19 (4)) и $L_{-1} \subset L_0 \subset ... \subset L_n \subset ....$ Применом тврђења 19 (5), закључујемо да је $\dim L_{n+1} - \dim L_n \in \{0, 1\}$. За $n = g$ је $\dim L_n = g - g + 1 + l(K_C - D - nP_0) \geq 1$, по теореми Римана-Роха.

Из претходних чињеница следи да постоји најмање $0 \leq n \leq g$ такво да $\dim L_n = 1$. Тада постоји функција $f \in L_n$ таква да $\text{div}(f) \geq -D - nP_0$, тј. $\text{div}(f) = D_Q - D - nP_0$, за неки ефективан дивизор $D_Q$. Све друге функције у $L_n$ се добијају из $f$ множењем неком константом, што значи да $D_Q$ не зависи од избора $f$. Сада је

$$Q = [D] = [D + \text{div}(f)] = [D_Q - nP_0].$$

Дивизор $D_Q$ је јединствен међу дивизорима степена $n$ са траженим својствима, што се види из чињенице $\dim L_n = 1$. Ако би постојао $D'_Q$ дивизор степена $m < n$ са траженим својствима, онда би из $[D] = [D'_Q - mP_0]$ следило да је $D'_Q - D - mP_0$ главни дивизор, а тада постоји $f \in \overline{K}(C)$ такво да $\text{div}(f) = D'_Q - D - mP_0$, па је $\dim L_m \geq 1$, јер $f \in L_m$.

Остаје још да докажемо да је овај дизивор $K$-рационалан (приметимо да то још увек нисмо доказали). Нека је $\sigma \in \mathcal{G}_{\overline{K}/K}$, произвољно. Тада (коришћењем $Q \in J(K)$ и $P \in C(K)$) добијамо

$$[\sigma(D_Q) - nP_0] = [\sigma(D_Q - nP_0)] = \sigma[D_Q - nP_0] = [D_Q - nP_0].$$

Одавде следи да је и $\sigma(D_Q)$ дивизор са траженим својствима, а пошто је такав дивизор јединствен, онда је $\sigma(D_Q) = D_Q$. Ово важи за све $\sigma \in \mathcal{G}_{\overline{K}/K}$, одакле је $D_Q \in \mathrm{Div}_K(C)$.

Постоји посебна класа дивизора са којом ћемо се овде често сусретати.

**Дефиниција 27.** Нека је $C : y^2 = f(x)$ хиперелиптичка крива непарног степена над $K$. Дивизор $D \in \mathrm{Div}(C)$ је у *општем положају* ако је $D$ ефективан, $\infty \notin \mathrm{supp}(D)$ и не постоји $P \in C$ таква да $D \geq P + \iota(P)$.

Приметимо да дефиниција дивизора у општем положају каже да су му сви коефицијенти позитивни, да не садржи $\infty$ у свом запису, да сваку тачку рамификације $(x_0, 0)$ садржи са коефицијентом 0 или 1, док не садржи у исто време тачке $(x_0, y_0)$ и $(x_0, -y_0)$, за $y_0 \neq 0$. На претходно тврђење се наводезује следеће.

**Тврђење 34.** Нека је $C : y^2 = f(x)$ глатка хиперелиптичка крива, непарног степена, рода $g$ над $K$. Тада за сваку тачку $P \in J(K)$ постоји јединствени дивизор $D \in \mathrm{Div}_K(C)$ у општем положају и степена $d = \deg(D) \leq g$, такав да је $P = [D - d \cdot \infty]$.

**Доказ.** Из претходног тврђења следи да постоји јединствени ефективни дивизор $D$ минималног степена $d \leq g$ такав да $P = [D - d\infty]$. Треба да докажемо да је $D$ у општем положају и да, ако је $D'$ неки дивизор у општем положају, степена $d' \leq g$ такав да $P = [D' - d'\infty]$,тада је $D'$ једнако $D$ да бисмо завршили доказ теореме.

Претпоставимо да $D$ није у општем положају. Тада могу да наступе следеће две могућности.
(1) Нека је $D \geq D_{x_0}$, за неко $x_0$. Знамо да је $D_{x_0}$ линеарно еквивалентан са $D_\infty = 2\infty$ (јер је њихова разлика дивизор функције $x - x_0$), па је

$$P = [D - d\infty] = [D - (d-2)\infty - 2\infty] = [D - (d-2)\infty - 2\infty + (D_\infty - D_{x_0})] =$$

$$= [(D - D_{x_0}) - (d-2)\infty],$$

што је у контрадикцији са минималношћу $d$ (јер је $D - D_{x_0}$ ефективан дивизор).
(2) Нека је $D \geq \infty$. Тада

$$P = [D - d\infty] = [(D - \infty) - (d-1)\infty],$$

што је опет контрадикција.

Доказали смо да је $D$ у општем положају, остаје још да покажемо други део. Претпоставимо да постоји $D'$, дивизор у општем положају, степена $d' \leq g$ такав да $[D' - d'\infty] = [D - d\infty]$. Одатле су дивизори $D' - D$ и $(d' - d)\infty$ линеарно еквивалентни, а самим тим су и линеарно еквивалентни $D' + \iota(D)$, јер су $D + \iota(D)$ и $2d\infty$ еквивалентни дивизори. То значи да постоји $f \in \overline{K}(C)$ такво да $\mathrm{div}(f) = D' + \iota(D) - (d + d')\infty$, што можемо да прочитамо да постоји функција $f \in L((d + d')\infty)$ такво да је $D' + \iota(D)$ дивизор њених нула (тј. $f$ има нуле само у тачкама које се појављују у $D' + \iota(D)$ и то баш те вишеструкости којом се појављују у $D' + \iota(D)$). Знамо да је $d + d' \leq 2g$, па из примера број 30 следи да је $L((d + d')\infty) \subset \langle 1, x, ..., x^g \rangle$. Дакле, $f$ је полином по $x$, а тада је дивизор њених нула линеарна комбинација дивизора облика $D_{x_0}$. Како су и $D'$ и $\iota(D)$ дивизори у општем положају, не може да буде $D' \geq D_{x_0}$ ни $\iota(D) \geq D_{x_0}$ ни за једно $D_{x_0}$ које се појављује у збиру за дивизор нула функије $f$, што значи да се сваки такав $D_{x_0}$ раздваја на члан који је у $D'$ и који је у $\iota(D)$. Зато је $D' = \iota(\iota(D)) = D$, што смо и желели да покажемо.

У случају хиперелиптичке криве непарног степена, постоји експлицитан поступак помоћу којег можемо описати операцију сабирања у њеном Јакобијану. Наводимо тврђење и теорему чији су докази претежно рачунски и овде их не наводимо, а могу се наћи у [53].

**Тврђење 35.** Нека је $C$ глатка хиперелиптичка крива, непарног степена над пољем $K$ и $D \in \mathrm{Div}_K(C)$ дивизор у општем положају на $C$. Тада постоје јединствени полиноми $a, b \in K[x]$ такви да
(1) $a$ је моничан степена $d = \deg D$;

(2) $\deg(b) < d$;
(3) $f \equiv b^2 \pmod{a}$;
(4) ако је $P = (x_0, y_0)$ у афином делу криве $C$, тада важи

$$P \in \mathrm{supp}(D) \iff a(x_0) = 0, b(x_0) = y_0,$$

при чему је $\mathrm{ord}_P(D)$ једнак вишеструкости корена $x_0$ полинома $a$.

Важи и обрнуто, сваки овакав пар $(a, b)$ одређује један дивизор $D$ у општем положају.

Ова репрезентација $D$ преко пара полинома $(a, b)$ се назива *Мамфордова репрезентација дивизора* $D$. Пар $(1, 0)$ представља нулу (неутрални елемент) у Јакобијану. Уз њену помоћ рачунамо на Јакобијану. Следећи алгоритам је први описао математичар Кантор.

**Теорема 22.** Нека је $C : y^2 = f(x)$ глатка хиперелиптичка крива, непарног степена и рода $g$ над пољем $K$. Нека су тачке $P_1, P_2 \in J(K)$ представљене полиномима $(a_1, b_1)$, $(a_2, b_2)$, тј. нека је то њихова Мамфордова репрезентација. Ово значи да $(a_i, b_i)$ преставља дивизор $D_i$ за који је $P_i = [D_i - (\deg D_i)\infty]$, за $i = 1, 2$. Тада рачунамо Мамфордову репрезентацију тачке $P_1 + P_2$ на следећи начин:
(1) Рачунање збира:
(1.1) Одредимо $d =$НЗД$(a_1, a_2, b_1 + b_2)$.
(1.2) Означимо $a = \dfrac{a_1 a_2}{d^2}$.
(1.3) Нека је $b$ јединствени полином степена мањег од $\deg(a)$, такав да

$$b \equiv b_1 \pmod{\frac{a_1}{d}}, \quad b \equiv b_2 \pmod{\frac{a_2}{d}}, \quad , f \equiv b^2 \pmod{a}.$$

(2) Редукција (ако је дивизор степена већег од $g$, смањујемо му степен):
Докле год важи $\deg(a) > g$:
(2.1) Напишимо $f - b^2 = \lambda ac$, за неко $\lambda \in K^*$ и $c \in K[x]$, моничан полином.
(2.2) Заменимо $a$ и $c$. Приметимо да је $\deg(c) < \deg(a)$.
(2.3) Заменимо $b$ са остатком $-b \pmod{a}$, при чему је ово ново $a$,

тј. $c$ из (2.1).

Тада је $(a, b)$ Мамфордова репрезентација дивизора $D$ таквог да $P_1 + P_2 = [D - (\deg D)\infty]$ и $\deg D \leq g$.

**Пример 53.** Посматрајмо хиперелиптичку криву $y^2 = x^5 + 1$ над $\mathbb{Q}$. Једна од тачака Јакобијана је $Q = [(-1, 0) - \infty]$. Одредимо $2Q$ применом Канторовог алгоритма. У овом случају је $D = (-1, 0)$ дивизор у општем положају степена 1. Тражимо полином $a$ степена 1, чија је нула $x = -1$, одакле је $a(x) = x + 1$. Полином $b$ је степена 0, дакле константан полином и $b(0) = 0$, што значи да је $b(x) = 0$. Испуњени су сви услови тражени за Мамфордову репрезентацију. За рачунање заборављамо ознаке $a$ и $b$ и $a_1(x) = a_2(x) = x + 1$ и $b_1(x) = b_2(x) = 0$.

Одређујемо полиноме $d$ =НЗД$(x + 1, x + 1, 0) = x + 1$, и $a = \dfrac{(x+1)\cdot(x+1)}{(x+1)^2} = 1$. Сада тражимо (јединствени) полином $b$ степена мањег од $0 = \deg(a)$ такав да

$$b \equiv 1 \pmod 1, \qquad b^2 \equiv x^5 + 1 \pmod 1,$$

а јасно се види да је то полином $b(x) = 0$ (то је једини полином који има степен мањи од 0). Добијамо $(a, b) = (1, 0)$, а ово је репрезентација нуле, одакле следи да је $2Q = 0$ у $J(\mathbb{Q})$.

Друга тачка коју можемо да уочимо је $P = [(0, 1) - \infty]$. Тада је репрезентација ове тачке $(x, 1)$. Израчунајмо $2P$.

Добијамо полиноме $d$ =НЗД$(x, x, 2) = 1$ и $a = \dfrac{x \cdot x}{1^2} = x^2$. Сада тражимо $b$ степена мањег од $2 = \deg(a)$ такав да

$$b \equiv 1 \pmod x, \qquad b^2 \equiv x^5 + 1 \equiv 1 \pmod{x^2}.$$

Из првог услова да је $b$ облика $b(x) = 1 + \beta x$, а из другог закључујемо да је $\beta = 0$, одакле је $b(x) = 1$. Добијамо репрезентацију $(x^2, 1)$ а то је репрезнетација тачке $2P = [2(0, 1) - 2\infty]$. Рачунамо $3P$.

Полином $d$ =НЗД$(x, x^2, 2) = 1$, док је полином $a = \dfrac{x \cdot x^2}{1^2} = x^3$. За полином $b$ степена мањег од 3 важе услови

$$b \equiv 1 \pmod x, \quad b \equiv 1 \pmod{x^2}, \quad b^2 \equiv x^5 + 1 \equiv 1 \pmod{x^3}.$$

Одавде је опет $b(x) = 1$, тако да је репрезентација $3P$ дата са $(x^3, 1)$. Међутим, полином $x^3$ има већи степен, од дозвољеног, а то је 2, због тога радимо редукцију.

$$x^5 + 1 - 1 = x^5 = 1 \cdot x^3 \cdot x^2,$$

одакле је $c(x) = x^2$, а то је ново $a$, па је $a(x) = x^2$. Ново $b$ добијамо тако што рачунамо остатак при дељењу $-1$ са $x^2$, али ово нема потребе да радимо, $b(x) = -1$. Права репрезентација тачке $3P$ је $(x^2, -1)$, а ово је тачка $3P = [2(0, -1) - 2\infty]$. Даље, рачунамо $4P$, сабирамо $(x, 1)$ и $(x^2, -1)$.

Као и до сада, $d = $НЗД$(x, x^2, 0) = x$, па је $a = \dfrac{x \cdot x^2}{x^2} = x$. Полином $b$ који тражимо је константан полином који задовољава услове

$$b \equiv 1 \pmod 1, \quad b \equiv -1 \pmod x, \quad b^2 \equiv x^5 + 1 \equiv 1 \pmod x.$$

Јасно је да је $b(x) = -1$, а репрезентација $4P$ је дата са $(x, -1)$, односно $4P = [(0, -1) - \infty]$. Саберимо $P$ и $4P$ да одредимо $5P$.

Сада је $d = $НЗД$(x, x, 0) = x$, а $a = \dfrac{x \cdot x}{x^2} = 1$. Одавде мора бити $b = 0$, па се $5P$ представља паром $(1, 0)$, тј. $5P$ је неутрал у $J(\mathbb{Q})$.

У овом примеру смо у Јакобијану нашли тачку реда 2 и тачку реда 5. Ово резултати су и очекивани, ако приметимо $2((-1, 0) - \infty) = \operatorname{div}(x + 1)$ и $5((0, 1) - \infty) = \operatorname{div}(y - 1)$, а на десној страни у претходне две једнакости су главни дивизори. Видимо и још да је $\#J(\mathbb{Q}) \geq 10$, чак и да је $\#J(\mathbb{Q})$ дељиво са 10.

**Пример 54.** Нека је $C : y^2 = f(x)$ глатка хиперелиптичка крива, непарног степена и рода 2 над пољем $K$. Тада, коришћењем Мамфордове репрезентације, можемо експлицитно, на јединствен начин описати класу било ког $Q \in J(K)$ (дакле, $K$-рационалног дивизора). Опис ћемо вршити према полиномима $a(x) \in K[x]$, који су у бијекцији са $K$-рационалним дивизорима у Јакобијану. Сетимо се да је $\deg(a) \leq 2$, па имамо следеће могућности, при чему искључујемо све опције у којима добијени дивизори нису у општем полозају.

(1) Ако је $a(x) = x - x_0$ или $a(x) = 1$, у питању је тачка $Q = [P - \infty]$, где је $x_0$ $x$-координата тачке $P$ у првом случају, док је $P = \infty$ у

другом случају.
(2) Ако је $a(x) = (x - x_0)^2$, тада је $Q = [2P - 2\infty]$, где је, као и у (1), $x_0$ $x$-координата тачке $P$.
(3) Ако је $a(x) = (x - x_0)(x - x_0')$, тада је $Q = [P + P' - 2\infty]$, за тачке $P$ и $P'$ чије су $x$-координате редом $x_0$, $x_0'$.
(4) Ако је $a(x)$ квадратни полином који нема корене у $K$, тада има корене у раширењу $L/K$ степена 2, тада су корени $a(x)$ $\{P, \sigma(P)\}$, при чему је Галуаова група тог раширења $\mathcal{G}_{L/K} = \langle\sigma\rangle$. Онда је $Q = [P + \sigma(P) - 2\infty]$, при чему је ово $K$-рационалан дивизор, јер $\sigma(Q) = [\sigma(P) + P - 2\infty]$.

Из конструкције Јакобијана по којој је Јакобијан Абелов варијетет који задовољава $J(K) = \mathrm{Pic}^0_K(C)$, која је функторијална, се може извести следећа последица, али је овде не доказујемо.

**Теорема 23.** Нека је $C$ глатка, апсолутно несводљива, хиперелиптичка крива над $\mathbb{Q}$, чији је Јакобијан $J$ и нека је $p$ прост број добре редукције криве $C$. Означимо Јакобијан криве $\overline{C}$ са $\overline{J}$. Тада постоји редуктивно пресликавање $J(\mathbb{Q}) \longrightarrow J(\mathbb{F}_p)$ које је хомоморфизам група.

Ако фиксирамо $P_0 \in C(\mathbb{Q})$ и пресликавање $i : C(\mathbb{Q}) \longrightarrow J(\mathbb{Q})$, $i : P \mapsto [P - P_0]$, тада постоји пресликавање $\overline{i} : \overline{C} \longrightarrow \overline{J}$, $i : P \mapsto [P - \overline{P_0}]$ такво да следећи дијаграм комутира.

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\ i\ } & J(\mathbb{Q}) \\ \Big\downarrow{\scriptstyle \rho_{p,C}} & & \Big\downarrow{\scriptstyle \rho_{p,J}} \\ \overline{C}(\mathbb{F}_p) & \xrightarrow{\ \overline{i}\ } & \overline{J}(\mathbb{F}_p) \end{array}$$

Ова теорема је тачна и када се $\mathbb{Q}$ замени са $\mathbb{Q}_p$, тако да постоји редукција модуло $p$ и на $J(\mathbb{Q}_p)$. Језгро тог пресликавања се, очекивано, зове *језгро редукције* и означава се $J(\mathbb{Q}_p)_1$. Ако је $p > 2$, што је свакако испуњено за хиперелиптичке криве, јер за $p = 2$ имају лошу редукцију, може се доказати да је $J(\mathbb{Q}_p)_1 \cong \mathbb{Z}_p^g$ (као групе), одакле одмах видимо да је једини елемент коначног реда у језгру редукције нула. Одавде можемо да изведемо следећи закључак.

**Теорема 24.** Нека је $C$ глатка, апсолутно несводљива, хиперелиптичка крива над $\mathbb{Q}$, чији је Јакобијан $J$ и нека је $p$ прост број добре редукције криве $C$. Тада је рестрикција на $J(\mathbb{Q})_{\text{tors}}$ редуктивног пресликавања $J(\mathbb{Q}) \longrightarrow \overline{J}(\mathbb{F}_p)$ инјективна.

**Доказ.** Нека је $P \in \ker(J(\mathbb{Q})_{\text{tors}} \longrightarrow \overline{J}(\mathbb{F}_p)$. Тада је $P \in \ker(J(\mathbb{Q}_p) \longrightarrow \overline{J}(\mathbb{F}_p)$, одакле је $P \in J(\mathbb{Q}_p)_1$. У овој групи је само нула елемент коначног реда, а пошто је $P$ коначног реда, онда је $P = 0$.

Можемо да приметимо да и ова теорема остаје тачна када заменимо $\mathbb{Q}$ са $\mathbb{Q}_p$, тј. да је инјективно и пресликавање $J(\mathbb{Q}_p) \longrightarrow \overline{J}(\mathbb{F}_p)$. Можемо да претпоставимо шта је примена претходне теореме, то је рачунање торзионе подгрупе Јакобијана. За хиперелиптичке криве рода 2, тај посао олакшава следеће тврђење.

**Тврђење 36.** Нека је $y^2 = f(x)$ глатка хиперелиптичка крива рода $g = 2$ и $p$ прост број, $p \geq 3$. Тада важи

$$\#\overline{J}(\mathbb{F}_p) = \frac{\#\overline{C}(\mathbb{F}_{p^2}) + \#\overline{C}(\mathbb{F}_p)^2}{2} - p.$$

**Доказ.** Докажимо тврђење само у случају непарног степена, јер тада имамо информације из примера број 54. Елементе Јакобијана $\overline{J}(\mathbb{F}_p)$ смо описали у примеру број 54, треба да их пребројимо.

Имамо једну бесконачну тачку и у $\mathbb{F}_p$ и у $\mathbb{F}_{p^2}$. Тачке у $\mathbb{F}_p$ поделимо на $(x_1, 0)$, ... $(x_k, 0)$ и на $(x_1', y_1')$, $(x_1', -y_1')$, ... , $(x_l', y_l')$, $(x_l', -y_l')$, при чему се $y_1'$, ... $y_l'$ различити од нуле. Нека је $\mathbb{F}_{p^2} = \mathbb{F}_p(t)$. Тада је за преосталих $p-k-2l$ $x$-координата $f(x)$ квадратни неостатак модуло $p$ (иначе би дала тачку у $\mathbb{F}_p$), па су то тачке у $\mathbb{F}_{p^2} \backslash \mathbb{F}_p$: $(x_1'', ty_1'')$, $(x_1'', -ty_1'')$, ... , $(x_{p-k-2l}'', ty_{p-k-2l}'')$, $(x_{p-k-2l}'', -ty_{p-k-2l}'')$. Нека су преостале тачке у $\mathbb{F}_{p^2}$ на листи $(\alpha_1, \beta_1)$, $(\overline{\alpha_1}, \overline{\beta_1})$, ... , $(\alpha_v, \beta_v)$, $(\overline{\alpha_v}, \overline{\beta_v})$, при чему овде $\overline{\gamma}$ представља Галуаов конјугат $\gamma$ за раширење $\mathbb{F}_{p^2}/\mathbb{F}_p$. Бројимо сада све елементе $\overline{J}(\mathbb{F}_p)$.
(1) Имамо један неутрал (за бесконачну тачку) и $k + 2l$ дивизора првог облика из примера број 54.
(2) Овде бројимо дивизоре другог и трећег облика у примеру број 54. Сада већ морамо да будемо пажљиви, јер не долазе у обзир све комбинације. На пример, не можемо имати $[2(x_1, 0) - 2\infty]$, јер

$2(x_1, 0)$ није дивизор у општем положају, а и класа наведеног дивизора је тривијална. Зато имамо $\binom{k}{2}$ парова у којима бирамо различите $(x_i, 0)$ и $(x_j, 0)$, $2kl$ могућности за одабир једног $(x_i, 0)$ и једног $(x'_j, y'_j)$ и $2l$ могућности да изаберемо $2(x'_i, y'_i)$ и $\binom{2l}{2} - l$ могућности да изаберемо два различита $(x'_i, y'_i)$ и $(x'_j, y'_j)$, при чему одбацујемо $l$ комбинација са истим $x'_i$, а супротним $y'_i$.
(3) Остаје још да проверимо последњи облик дивизора из примера број 54, тј. комбинације тачака које су у $\mathbb{F}_{p^2}/\mathbb{F}_p$. Морамо узимати коњуговане парове, али не можемо узети парове облика $(x''_i, \pm y''_i)$, јер и они не чине дивизор у општем положају. У овом случају имамо нових $v$ тачака.

Када све ово саберемо,

$$\#\overline{J}(\mathbb{F}_p) = 1 + k + 2l + \binom{k}{2} + 2kl + 2l + \binom{2l}{2} - l + v =$$

$$= 1 + v + 2l + 2kl + 2l^2 + \frac{k^2 + k}{2}.$$

Са друге стране, $\#\overline{C}(\mathbb{F}_{p^2}) = 1 + k + 2(p - k) + 2v = 1 + 2p + 2v - k$ и $\#\overline{C}(\mathbb{F}_p) = 1 + k + 2l$, одакле заменом у

$$\frac{\#\overline{C}(\mathbb{F}_{p^2}) + \overline{C}(\mathbb{F}_p)^2}{2} - p = \frac{1 + 2p + 2v - k + (1 + k + 2l)^2 - 2p}{2} =$$

$$= 1 + v + 2l + 2kl + 2l^2 + \frac{k^2 + k}{2}$$

добијамо тражену једнакост.

**Пример 55.** Посматрајмо поново хиперелиптичку криву $C : y^2 = x^5 + 1$. Одредимо $\#\overline{J}(\mathbb{F}_3)$. Тачке у $\overline{C}(\mathbb{F}_3)$ лако одређујемо, то су $\{(0, \pm 1), (-1, 0), \infty\}$, дакле има их 4. За одређивање тачака у $\overline{C}(\mathbb{F}_9)$ проширимо $\mathbb{F}_3$ елементом $t$ таквим да је $t^2 = -1$, онда тражимо тачке облика $(a + bt, c + dt)$, за $a, b, c, d \in \mathbb{F}_3$. Из једначине криве добијамо

$$c^2 - d^2 - cdt = a^5 - a^3b^2 - ab^4 + (b^5 - a^2b^3 - a^4b)t,$$

одакле имамо две једначине $c^2-d^2=a^5-a^3b^2-ab^4$ и $-cd=b^5-a^2b^3-a^4b$, а у $\mathbb{F}_3$ се ове једначине своде на $c^2-d^2=a+ab^2$ и $-cd=b+a^2b$. Морамо да дискутујемо случајеве.
(1) Ако је $b=0$, тада је $c=0$ или $d=0$. Ако је $d=0$, онда су тачке у $\mathbb{F}_3$, одаке имамо 3 тачке (без $\infty$). Ако је $d\neq 0$, па $c=0$, тада је $-d^2=a$, одакле иммао још 2 тачке, јер $d=\pm 1$, $a=-1$.
(2) Ако је $b\neq 0$, тада $b(a^2+1)\neq 0$, па $cd\neq 0$, одакле је $c^2-d^2=0$, па је $2a=0$, тј. $a=0$. Друга једначина постаје $-cd=b$, што има 4 тачке, јер $c$ и $d$ могу узети вредност $\pm 1$.

Када додамо и бесконачу тачку, добијамо да је $\#\overline{C}(\mathbb{F}_9)=10$. Применом тврђења 36, долазимо до $\#\overline{J}(\mathbb{F}_3)=\dfrac{10+16}{2}-3=10$, одакле је $\#J(\mathbb{Q})_{\text{tors}}\leq 10$. У примеру 53 смо закључили да је $\#J(\mathbb{Q})_{\text{tors}}\geq 10$, па мора бити $\#J(\mathbb{Q})_{\text{tors}}=10$. Још знамо и $J(\mathbb{Q})\cong\mathbb{Z}/10\mathbb{Z}$.

**Пример 56.** Нека је $C: y^2=x^5-x+1$. У простим бројевима 3 и 5 крива $C$ има добру редукцију, јер је њена дискриминанта $2869=19\cdot 151$. Као у претходном примеру, можемо израчунати $\#\overline{J}(\mathbb{F}_3)=29$ и $\#\overline{J}(\mathbb{F}_5)=71$. Пошто су ово узајамно прости бројеви, а $J(\mathbb{Q})_{\text{tors}}$ се инјективно слика у обе групе, њен ред мора делити 1, тј. то је тривијална група $J(\mathbb{Q})_{\text{tors}}=\{0\}$.

За Јакобијане важи слична теорема као и за елиптичке криве. Наводимо је без доказа. Пре исказа, подсетимо се да за Абелову групу $G$, ознака $G[n]$ означава подгрупу свих елемената $x$ таквих да је $nx=0$

**Теорема 25.** Нека је $C$ глатка крива рода $g$ над пољем $K$ и $n\in\mathbb{N}$. Ако је $\operatorname{char}K=0$ или $(n,\operatorname{char}K)=1$, тада је $\#J(\overline{K})[n]=n^{2g}$. Ако је $\operatorname{char}K=p$, за неки прост број $p$, тада је $J(\overline{K})[p]=p^e$, за неко $0\leq e\leq g$.

Претпоставимо да смо нашли торзиону подгрупу $J(K)_{\text{tors}}$ Јакобијана. Желимо да му одредимо ранг $r$. Досетимо се да посматрамо

$$J(K)/2J(K)\cong J(K)_{\text{tors}}/2J(K)_{\text{tors}}\oplus(\mathbb{Z}/2\mathbb{Z})^r\cong J(K)[2]\oplus(\mathbb{Z}/2\mathbb{Z})^r,$$

јер једини елементи $J(K)_{\text{tors}}$ који преживљавају у количничкој групи $J(K)_{\text{tors}}/2J(K)_{\text{tors}}$ су елементи реда 2. Одавде наслућујемо идеју

шта бисмо могли да радимо да бисмо одредили ранг Јакобијана. Ако одредимо $J(K)/2J(K)$ и $J(K)[2]$, онда смо одредили и $r$, узимајући димнезије над $\mathbb{F}_2$ у једнакости изнад. Зато нам је први задатак да одредимо $J(K)[2]$, онда и да опишемо $J(K)/2J(K)$.

**Тврђење 37.** Нека је $C : y^2 = f(x)$ глатка хиперелиптичка крива непарног степена рога $g$, над пољем $K$. Нека је $f = cf_1f_2...f_n$ факторизација полинома $f$ на несводљиве факторе над пољем $K$, при чему су полиноми $f_j$, $1 \leq j \leq n$ монични и $c \in K^*$. Тада тачке $P_j \in J(K)$ са Мамфордовом репрезентацијом $(f_j, 0)$ генеришу $J(K)[2]$, са једином линеарном релацијом међу њима, која гласи $P_1 + ... + P_n = 0$. Специјално, $\dim_{\mathbb{F}_2}(J(K)[2]) = n - 1$.

**Доказ.** Тачка $P \in J(K)$ је реда 2 ако и само ако је $P = -P$. Ово значи да Мамфордове репрезентације тачака $P$ и $-P$ морају да буду исте. Јасно је да, ако је $(a(x), b(x))$ Мамфордова репрезентација тачке $P$, тада је $(a(x), -b(x))$ Мамфордова репрезентација тачке $-P$ (саберимо их по Канторовом алгоритму и добићемо $(1, 0)$ што представља неутрал). Дакле, тачка $P$ је реда 2 ако и само ако за њену Мамфордову репрезентацију $(a, b)$ важи $b = 0$.

Ако је $b = 0$, тада по дефиницији Мамфордове репрезентације $a \mid f$, а пошто је $a \in K[x]$, онда $a$ мора бити прозивод неких $f_j$, али тако да степен полинома $a$ буде мањи или једнак од $g$. Ово доказује да тачке $P_j$ генеришу $J(K)[2]$, јер одабрана тачка $P$ је онда збир тачака $P_j$ које одговарају полиномима $f_j$ који се појављују у факторизацији полинома $a$. Међутим, знамо и више, знамо да је $\#J(K)[2] = 2^{n-1}$, а то следи из чињенице да је производ полинома $f_j$ степена мањег или једнаког $g$ ако и само ако је производ комплементарних полинома степена строго већег од $g$ (заједно у производу дају полином степена $2g + 1$). Према томе од $2^n$ подскупова скупа полинома $\{f_1, f_2, ..., f_n\}$ тачно пола од њих репрезентују тачку у $J(K)[2]$. Дакле, $\dim_{\mathbb{F}_2}(J(K)[2]) = n - 1$, што значи да постоји тачно једна линеарна веза међу тачкама $P_j$.

Ако саберемо $\sum_{j=1}^{n} \mathrm{div}(f_j)$ добијамо дивизор који се састоји од

свих нула полинома $f$ (у $\overline{K}$, али је $K$-рационалан). Сетимо се да је $\mathrm{div}(y)$ дивизор у чији збир улазе нуле полинома $f$ са коефицијентом 1 и $\infty$ са коефицијентом $-2g-1$. Одавде следи да мора бити

$$\sum_{j=1}^{n} P_j = \sum_{j=1}^{n}[\sum_{x:f_j(x)=0}(x,0) - \deg(f_j)\infty] = [\sum_{x:f(x)=0}(x,0) - (2g+1)\infty] =$$

$$= [\mathrm{div}(y)] = 0,$$

што је крај доказа.

## 4.2 2-Селмерове групе

Један од стандардних начина којим одређујемо ранг $r$ Јакобијана $J(\mathbb{Q})$ неке криве $C$ је уз помоћ *2-Селмерових група*. Ради једноставности, претпоставимо да је $C : y^2 = f(x)$ глатка хиперелиптичка крива, непарног степена $2g+1$, тј. рода $g$. Нека је $f$ моничан полином. Уводимо количнички прстен $A = \mathbb{Q}/\langle f\rangle$ и пишемо $\theta$ за слику $x$ у $A$, тада је $A = \mathbb{Q}[\theta]$. Ако је $f$ несводљив, тада је $A$ једно бројно поље, док је у општем случају $A$ директан прозивод бројних поља. Уведимо исте ознаке и за алгебарско затворење $\overline{A} = \overline{\mathbb{Q}}[x]/\langle f\rangle = \overline{\mathbb{Q}}[\theta]$. Тражимо пресликавање које ће да слика дивизоре у $A^*$.

За дивизор $D$ у општем положају, који представљамо у Мамфордовој репрезентацији са $(a,b)$. Претпоставимо за почетак да је $(a,f) = 1$ у прстену полинома и дефинишимо $\delta(D) = (-1)^{\deg(a)}a(\theta) \in A^*$. За дивизоре $D_{x_0}$, при чему $f(x_0) \neq 0$, (који, подсетимо се, нису у општем положају), дефинишемо $\delta(D_{x_0}) = (\theta - x_0)^2$. Сада можемо продужити ову дефиницију до хомоморфизма, за рационалне дивизоре $D = \sum_P n_P P$ (за $P \neq (x_0,0)$) дефинишимо $\delta(D) = \prod_P (x(P)-\theta)^{n_P}$, а овај производ ће бити у $\mathbb{A}^*$, јер је дивизор рационалан. Додајмо још и $\delta(\infty) = 1$. Ако означимо скуп рационалних дивизора у чијем носачу нису тачке облика $(x_i,0)$ са $\mathrm{Div}^{\perp}_{\mathbb{Q}}(C)$, закључујемо да смо добили хомоморфизам

$$\delta : \mathrm{Div}^{\perp}_{\mathbb{Q}}(C) \longrightarrow A^*.$$

Ако је $D - \deg(D)\infty = \mathrm{div}(\phi)$ главни дивизор, тада, пошто $\phi$ нема других полова сем у бесконачности, можемо да претпоставимо да је $\phi = h_1(x) + yh_2(x)$. Онда је у Мамфордовој репрезентацији овог дивизора $a = \lambda(h_1^2 - fh_2^2)$. Подсетимо се да су $a$ и $f$ монични полиноми, а $f$ непарног степена, па неће доћи до скраћивања највећег коефицијента у $h_1^2 - fh_2^2$. То значи да у случају да је $\deg(fh_2^2) > \deg(h_1)$, што је еквивалентно са тим да је $\deg(a)$ непаран, $-\lambda$ квадрат у $A$, а у супротном случају, тј. када је $\deg(a)$ паран, је $\lambda$ квадрат у $A$. Ово можемо сумирати у то да је $(-1)^{\deg(a)}\lambda$ квадрат у $A$. Приметимо да је $\delta(D) = (-1)^{\deg(a)}a(\theta) = (-1)^{\deg(a)}(\lambda h_1(\theta)^2 - \lambda f(\theta)h_2(\theta)^2) = (-1)^{\deg(a)}\lambda h_1(\theta)^2$, јер је $f(\theta) = 0$. Како смо малопре утврдили да је $(-1)^{\deg(a)}$ увек квадрат у $A$, можемо да закључимо да постоји индуковано пресликавање (у истој ознаци)

$$\delta : \mathrm{Div}_{\mathbb{Q}}^{\perp}(C)/(\mathrm{Div}_{\mathbb{Q}}^{\perp}(C) \cap \mathrm{Princ}_{\mathbb{Q}}(C)) \longrightarrow A^*/(A^*)^2,$$

где $\mathrm{Princ}_{\mathbb{Q}}(C)$ означава скуп рационалних главних дивизора.

Може се показати да се за произвољу тачку у $J(\mathbb{Q})$ може наћи њен представник међу дивизорима у $\mathrm{Div}_{\mathbb{Q}}^{\perp}(C)$, као и да се дефиниција пресликавања $\delta$ може проширити и у случају када $a$ и $f$ нису узајамно прости, одакле добијамо пресликавање (које опет обележавамо са $\delta$)

$$\delta : J(\mathbb{Q}) \longrightarrow A^*/(A^*)^2.$$

Овако конструисано пресликавање има јако важно својство. Видимо да су елементи $2J(\mathbb{Q})$ у језгру хомоморфизма $\delta$, јер $\delta(2P) = (\delta(P))^2$. Корисно је то што су то сви елементи језгра $\delta$.

**Теорема 26.** Језгро хомоморфизма $\delta : J(\mathbb{Q}) \longrightarrow A^*/(A^*)^2$ је $2J(\mathbb{Q})$.

**Доказ.** Погледати у [53].

Сада по теореми о изоморфизму за групе закључујемо

$$J(\mathbb{Q})/2J(\mathbb{Q}) \cong \delta(J(\mathbb{Q})).$$

Сетимо се да нам фали опис групе $J(\mathbb{Q})/2J(\mathbb{Q})$ да бисмо одредили ранг $J(\mathbb{Q})$. Уз помоћ пресликавања $\delta$ смо се приближили нашем циљу, јер је сада потребно да одредимо $\delta(J(\mathbb{Q}))$. Пре него што још детаљније опишемо тај скуп, подсетимо се једне дефиниције. Нека је $K$ поље и $A$ коначно-димензиона $K$-алгебра. Тада је $m_a : x \mapsto ax$ $K$-линеарно пресликавање, за свако $a \in A$. Дефинишимо *норму* елемента $a$ са

$$N_{A/K}(a) = \det(m_a).$$

Норма је мултипликативно пресликавање и за свако $a \in A$ знамо да је $N_{A/K}(a) \in K$, одакле следи да постоји и хомоморфизам $A^*/(A^*)^2 \longrightarrow K^*/(K^*)^2$.

**Тврђење 38.** При ознакама из овог поглавља, слика хомоморфизма $\delta$ је подскуп језгра хомоморфизма $N_{A/K} : (A^*)/(A^*)^2 \longrightarrow (K^*)/(K^*)^2$.

**Доказ.** Погледати у [53].

Означимо језгра хомоморфизама $N_{A/K} : (A^*)/(A^*)^2 \longrightarrow (K^*)/(K^*)^2$ за различита поља $K$ на следећи начин - ако је $K = \mathbb{Q}$, онда користимо ознаку $H$, а ако је $K = \mathbb{Q}_p$, онда користимо ознаку $H_p$. Ово последње продужавамо и на $p = \infty$. Инклузија $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ индукује хомоморфизам $\rho_p : H \longrightarrow H_p$. Означимо одговарајуће пресликавање $J(\mathbb{Q}_p) \longrightarrow H_p$ са $\delta_p$ (када у конструкцији у овом поглављу заменимо $\mathbb{Q}$ са $\mathbb{Q}_p$). Тада имамо комутативни дијаграм

$$\begin{array}{ccc} J(\mathbb{Q}) & \xrightarrow{\delta} & H \\ \downarrow & & \downarrow{\scriptstyle \rho_p} \\ J(\mathbb{Q}_p) & \xrightarrow{\delta_p} & H_p \end{array}$$

**Дефиниција 28.** При већ уведеним ознакама, дефинишемо *2-Селмерову групу* као

$$\mathrm{Sel}^{(2)}(J(\mathbb{Q})) = \{\alpha \in H \mid (\forall p)\rho_p(\alpha) \in \mathrm{im}(\delta_p)\}.$$

Следећа теорема нам говори да се 2-Селмерова група може израчунати, а њен доказ је констукриван у смислу да даје упуцтво како да је израчунамо.

**Теорема 27.** Нека је $C : y^2 = f(x)$ глатка хиперелиптичка крива непарног степена, над $\mathbb{Q}$. Тада је $\delta(J(\mathbb{Q})) \subset \mathrm{Sel}^{(2)}(J(\mathbb{Q}))$ и 2-Селмерова група је коначна и може се израчунати.

**Доказ.** Погледати у [53].

## 4.3 Примери рангова Јакобијана неких кривих

**Пример 57.** У [53] је доказано да за хиперелиптичку криву

$$C : y^2 = x(x-1)(x-2)(x-5)(x-6)$$

важи

$$J(\mathbb{Q}) \cong \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^4.$$

**Пример 58.** Слично као у претходном случају се може показати да је за криву $C : y^2 = x(x-3)(x-4)(x-6)(x-7)$

$$J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4.$$

**Пример 59.** У [53] се може наћи још један пример рачунања Јакобијана криве. За криву $C : y^2 = x^5 + 1$ смо до сада доказали да је $J(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/10\mathbb{Z}$. Испоставља се да је ранг Јакобијана ове криве 0, одакле је и

$$J(\mathbb{Q}) \cong \mathbb{Z}/10\mathbb{Z}.$$

Приметимо да смо у примеру број 55 описали скоро све елементе $J(\mathbb{Q})$, а и оне које нисмо, можемо лако да израчунамо знајући да тачка $[(-1,0) - \infty]$ има ред 2, а $[(0,1) - \infty]$ има ред 5. Одавде закључујемо да $C(\mathbb{Q})$ се састоји из највише 10 тачака, а директном

провером тога које тачке $J(\mathbb{Q})$ су слике при инјективном пресликавању $i : C(\mathbb{Q}) \longrightarrow J(\mathbb{Q})$ добијамо

$$C(\mathbb{Q}) = \{(0, \pm 1), (-1, 0), \infty\}.$$

**Пример 60.** У раду [18] је приказано како за неку криву рода 2 техником спуста уз помоћ изогеније криве на неку другу криву рода 2 може да се израчуна ранг Јакобијана $J(\mathbb{Q})$ те криве. Конкретно, наводе се два резултата, за следеће две криве је ранг $J(\mathbb{Q})$ једнак 1.

$$C_1 : y^2 = x(x^2 - 1)(x + \frac{1}{9})(x^2 - 4x - 1)$$

$$C_2 : y^2 = x(x^2 - 1)(x - \frac{1}{9})(x^2 - 18x + 1)$$

**Пример 61.** За криву $C : y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$, у [19] је доказано да је

$$J(\mathbb{Q}) \cong \mathbb{Z} \cdot [\infty_+ - \infty_-].$$

# 5 Колеманова интеграција

## 5.1 Увођење и својства Колемановог интеграла

Математичар Роберт Колеман је у свом раду [16] увео интеграл у $p$-адским просторима. Због потпуне неповезаности $p$-адских простра, увођење интеграла је јако тежак задатак, јер уопштавање извода функције на $p$-адске просторе има један проблем. Можемо да дефинишемо да је функција $f$ диференцијабилна у тачки $a$ ако постоји лимес израза

$$\frac{f(x)-f(a)}{x-a},$$

када $|x-a|_p$ тежи 0. Али тада се испоставља да функција $f:\mathbb{C}_p \longrightarrow \mathbb{C}_p$ која је свуда диференцијабилна мора да има извод идентички једнак нули, иако $f$ не мора бити локално константна. Ово се може наћи у [29]. Стога, можемо очекивати понашање функција и интеграла на које нисмо навикли. Међутим, Колеман ипак конструише интеграл који има особине које очекујемо. Још један материјал који је јако користан за упознавање са Колемановим интегралом је [57].

Сама конструкција захтева добро познавање ригидне аналитичке $p$-адске геометрије, и из тог разлога, овде прескачемо конструкцију и одмах наводимо теорему са главним својствима Колемановог интеграла, која ћемо користити у решавању Диофантових једначина. Пре него што кренемо, морамо да признамо да је потпуно неочекивано да интеграл може помоћи у одређивању свих рационалних тачака неке криве!

**Теорема 28.** Нека је $C$ апсолутно несводљива, глатка, пројективна крива над $\mathbb{Q}_p$, где је $p$ прост број за који $C$ има добру редукцију. Колеманов интеграл

$$\int_P^Q \omega \in \overline{\mathbb{Q}_p},$$

где су $P,Q \in C(\overline{\mathbb{Q}_p})$ произвољне тачке и $\omega \in \Omega_C^{\mathrm{reg}}(\overline{\mathbb{Q}_p})$ било који регуларан диференцијал има следећа својства:

(1) Интеграл је $\overline{\mathbb{Q}_p}$-линеаран по $\omega$.

(2) Ако се $P$ и $Q$ редукују по модулу $p$ у исту тачку $\overline{P} \in \overline{C}(\overline{\mathbb{F}_p})$, тада можемо да израчунамо интеграл на следећи начин. Одредимо равномернизатор $t$ у тачки $P$ који се редукује у равномернизатор у $\overline{P}$ и представимо $\omega$ као степени ред по $t$ који интегралимо формално члан-по-члан, одакле добијамо степени ред $l$ такав да $dl(t) = \omega(t)dt$ и $l(0) = 0$. Вредност интеграла добијемо тако што израчунамо $l(t(Q))$ ($l(t(Q))$ је степени ред, који ће да конвергира). Специјално, $\int_P^P \omega = 0$.

(3) За произвољне $P, P', Q, Q' \in C(\overline{\mathbb{Q}_p})$ важи

$$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^{Q} \omega.$$

Уз помоћ овог тврђења можемо да дефинишемо $\int^D \omega$ за $D = \sum_{j=1}^{n}(Q_j - P_j) \in \mathrm{Div}_C^0(\overline{\mathbb{Q}_p})$ са

$$\int^D \omega = \sum_{j=1}^{n} \int_{P_j}^{Q_j} \omega.$$

(4) Ако је $D$ главни дивизор, онда је $\int^D \omega = 0$.

(5) Интеграл се слаже са дејством Галуаове групе $\mathcal{G}_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}$, тј. за произвољно $\sigma \in \mathcal{G}_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}$ важи

$$\left(\int_P^Q \omega\right)^{\sigma} = \int_{P^\sigma}^{Q^\sigma} \omega^\sigma.$$

(6) Нека је $0 \neq \omega \in \Omega_C^{\mathrm{reg}}(\overline{\mathbb{Q}_p})$ и фиксирајмо $P_0 \in C(\overline{\mathbb{Q}_p})$. Тада је скуп

$$\left\{ P \in C(\overline{\mathbb{Q}_p}) \mid \overline{P} = \overline{P_0} \in \overline{C}(\overline{\mathbb{F}_p}), \int_{P_0}^{P} = 0 \right\},$$

при чему ознака $\overline{P} = \overline{P_0}$ значи да се $P$ и $P_0$ редукцијом по модулу $p$ сликају у исту тачку у $\overline{C}(\overline{\mathbb{F}_p})$, коначан.

**Уместо доказа, коментар.** Својство број (1), тј. линеарност је нешто најосновније што очекујемо од интеграла, као и својство број (2) које имитра основну теорему диференцијалног рачуна, док је и својство (3) нешто најприродне за интеграл, то је адитивност по границама. Узимајући у (3) $P' = Q$ добијамо стандардну адитивност

$$\int_P^Q \omega + \int_Q^{Q'} \omega = \int_P^{Q'} \omega.$$

Јасно је из формуле (3) зашто је добро дефинисан интеграл за дивизор степена 0, јер није важно којим редом ћемо да саберемо и одузимамо тачке у $D$. За својство (4) се може рећи да је бар мало неочекивано, јер услов да је $D$ главни дивизор је потпуно алгебарски, док је интеграл свакако аналитички објекат. Али ово својство је јако корисно и веома брзо ћемо видети његову примену. Својство (5) је нешто што желимо са алгебарске стране. Својство број (6) је кључно у доказу Шаботијеве теореме.

Напоменимо само да услов да $C$ има добру редукцију за тај прост број $p$ није суштински, једина његова улога је да поједностави део (2) претходне теореме.

Ова теорема има важну последицу коју сада наводимо. Наиме, није нам од интереса само да посматрамо овај интеграл са тачкама на кривој, много већу информацију добијамо када проширимо интеграл на Јакобијан. Због тога уводимо „билинеарно" (адитивно по првој компоненти, а $\mathbb{Q}_p$-линеарно по другој) придруживање на

следећи начин.

**Тврђење 39.** Нека је $C$ апсолутно несводљива, глатка, пројективна крива над $\mathbb{Q}_p$, где је $p$ прост број за који $C$ има добру редукцију, $P_0 \in C(\mathbb{Q}_p)$ и $i : C \longrightarrow J$ инјективно пресликавање криве у Јакобијан помоћу $P_0$. Постоји пресликавање

$$J(\mathbb{Q}_p) \times \Omega_C^{\mathrm{reg}}(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p, \qquad (Q, \omega) \mapsto \langle Q, \omega \rangle ,$$

које је адитивно по $Q = [D] \in J(\mathbb{Q}_p)$ и $\mathbb{Q}_p$-линеарно по $\omega$, које је задато са

$$\langle [D], \omega \rangle = \int^D \omega.$$

Специјално, тада је, по дефиницији, за $P \in \mathbb{C}(\mathbb{Q}_p)$

$$\langle i(P), \omega \rangle = \int_{P_0}^{P} \omega.$$

**Доказ.** Из претходне теореме, знамо да је пресликавање

$$\mathrm{Div}_C^0(\overline{\mathbb{Q}_p}) \times \Omega_C^{\mathrm{reg}}(\overline{\mathbb{Q}_p}) \longrightarrow \overline{\mathbb{Q}_p};$$

$$(D, \omega) \mapsto \int^D \omega$$

добро дефинисано, адитивно по левом аргументу и $\overline{\mathbb{Q}_p}$-линеарно по десном аргументу. Пошто је $\displaystyle\int^D \omega = 0$ за сваки главни дивизор (исто из претходне теореме), ово пресликавање индукује и добро дефинисано пресликавање

$$J(\overline{\mathbb{Q}_p}) \times \Omega_C^{\mathrm{reg}}(\overline{\mathbb{Q}_p}) \longrightarrow \overline{\mathbb{Q}_p},$$

јер сада овај интеграл неће зависити од преставника класе дивизора у Јакобијану.

Треба још да се ослободимо алгебарског затворења $\mathbb{Q}_p$. Ту користимо да се интеграл слаже са дејством Галуаове групе. Ако је $[D] \in J(\mathbb{Q}_p)$ и $\omega \in \Omega_C^{\mathrm{reg}}(\mathbb{Q}_p)$, тада је за свако $\sigma \in \mathcal{G}_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}$

$$\left( \int^D \omega \right)^{\sigma} = \int^{D^\sigma} \omega^\sigma = \int^D \omega,$$

па је $\int^D \omega \in \mathbb{Q}_p$, јер је фиксирано дејством Галуаове групе $\mathcal{G}_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p}$. Ово завршава доказ да постоји тражено пресликавање наведених особина.

Сада наводимо још једно, иако лако, корисно тврђење. Лепота овог тврђења је у томе да једно алгебарско својство (тачка $P$ је коначног реда у групи $J(\mathbb{Q}_p)$) можемо да откријемо уз помоћ аналитичког објекта (интеграла).

**Тврђење 40.** Нека је $P \in J(\mathbb{Q}_p)$ тачка коначног реда. Тада је $\langle P, \omega \rangle = 0$, за све регуларне диференцијале $\omega$.

**Доказ.** Ако је $nP = 0$, тада је

$$\langle P, \omega \rangle = \frac{1}{n} \langle nP, \omega \rangle = \frac{1}{n} \langle 0, \omega \rangle = 0.$$

**Коментар.** Може се доказати да у претходном тврђењу важи и обрнуто, ако је $\langle P, \omega \rangle = 0$, за све регуларне диференцијале $\omega$, тада је $P$ тачка коначног реда. Додатно, коришћењем својства (6) теореме 28 можемо да докажемо да ако је $\omega$ регуларан диференцијал за који је $\langle P, \omega \rangle = 0$, за све $P \in J(\mathbb{Q}_p)$, тада је $\omega = 0$.

## 5.2 Примери рачунања Колеманових интеграла

**Пример 62.** Нека је

$$C : y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

Видимо да су $(0, 1)$ и $(-3, 1)$ рационалне тачке на тој кривој, док су $\dfrac{dx}{y}$ и $\dfrac{xdx}{y}$ регуларни диференцијали на њој, јер је рода $g = 2$ (теорема 12), одакле има смисла да рачунамо интеграле

$$\int_{(0,1)}^{(-3,1)} \frac{dx}{y}, \qquad \int_{(0,1)}^{(-3,1)} \frac{xdx}{y}.$$

Рачунамо интеграле у $\mathbb{Q}_3$, а горња тачка се редукује у доњу по модулу 3, одакле можемо користити правило за израчунавање интеграла наведено у теореми 28. Можемо рачунати интеграл по $x$, јер је $x$ равномернизатор у тачки $(0,1)$, па кренимо са рачуном.

$$\int_{(0,1)}^{(-3,1)} \frac{dx}{y} = \int_{(0,1)}^{(-3,1)} (x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1)^{-\frac{1}{2}} dx$$

Ову корену функцију по $x$ можемо развити у степени ред и пошто рачунамо само по $x$, можемо заборавити $y$ координате тачака у границама у интегралу, па настављамо рачун.

$$\int_{(0,1)}^{(-3,1)} (x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1)^{-\frac{1}{2}} dx =$$

$$= \int_0^{-3} (1 - 3x + 11x^2 - 56x^3 + O(x^4)) dx = \left[ x - \frac{3x^2}{2} + \frac{11x^3}{3} - 14x^4 + O(x^5) \right] \Big|_0^{-3} =$$

$$= -3 - \frac{3 \cdot 9}{2} + \frac{11 \cdot (-27)}{3} - 14 \cdot 81 + O(3^5) =$$

$$= -3 - \frac{27}{2} - 99 - 2 \cdot 81 + O(3^5) = -21 - \frac{27}{2} + O(3^5) = -\frac{69}{2} + O(3^5) =$$

$$= -69 \cdot 122 + O(3^5) = 87 + O(3^5),$$

при чему смо множили са 122, јер је $2 \cdot 122 \equiv 1 \pmod{3^5}$. Израчунали смо

$$\int_{(0,1)}^{(-3,1)} \frac{dx}{y} = 87 + O(3^5).$$

Приметимо да можемо да бирамо колику ћемо прецизност да имамо при рачунању интерала, овде смо одабрали да рачунамо до $3^5$. Видећемо касније када будемо одређивали рационалне тачке на овој кривој у 7.4 зашто је то довољно.

Остаје да израчунамо и други интеграл.

$$\int_{(0,1)}^{(-3,1)} \frac{xdx}{y} = \int_{0}^{-3} (x - 3x^2 + 11x^3 - 56x^4 + O(x^5))dx =$$

$$= \left[\frac{x^2}{2} - x^3 + \frac{11x^4}{4} + O(x^5)\right]\Big|_0^{-3} = \frac{9}{2} + 27 + \frac{11 \cdot 81}{4} + O(3^5) =$$

$$= \frac{63}{2} + \frac{2 \cdot 81}{4} + O(3^5) = 72 + O(3^5).$$

Знамо да за Јакобијан криве $C$ важи да је $J(C) \cong \mathbb{Z}[\infty_+ - \infty_-]$, видели смо то у примеру 61. Такође, брзо се рачуна (на пример, програм то може да уради за нас) да је

$$9[\infty_+ - \infty_-] = [(-3,1) - (0,1)].$$

Одавде одређујемо интеграл од бесконачно до бесконачно по адитивности овог интеграла (теорема 28).

$$\int_{\infty_-}^{\infty_+} \frac{dx}{y} = \frac{1}{9} \int_{(0,1)}^{(-3,1)} \frac{dx}{y} = \frac{1}{9}(87 + O(3^5)) = \frac{29}{3} + O(3^3),$$

$$\int_{\infty_-}^{\infty_+} \frac{xdx}{y} = \frac{1}{9} \int_{(0,1)}^{(-3,1)} \frac{xdx}{y} = \frac{1}{9}(72 + O(3^5)) = 8 + O(3^5).$$

# 6 Главне теореме

Коначно смо се сусрели са свим потребним предзнањима и средствима за формулисање и доказивање две главне теореме у овом раду. Прво следи Шаботијева теорема, а онда за њом и Колеманова теорема.

## 6.1 Шаботијева теорема

Ову теорему је Шаботи доказао пре него што је Фалтингс доказао чувену теорему да је број рационалних тачака на апсолутно несводљивој глаткој пројективној кривој рода бар 2 је коначан, тј. док је још увек Морделова хипотеза била хипотеза. Након Фалтингсовог доказа би се чинило да је теорема изгубила смисао, међутим, идеје које се ту крију користи Колеман да докаже ефикаснију теорему. Такође, приметићемо да у доказу ове теореме користимо Колеманов интеграл који је тек касније Колеман увео, тако да је оригинални Шаботијев доказ био ипак нешто другачији од овог који се овде налази.

**Теорема 29.** Нека је $C$ апсолутно несводљива, глатка, пројективна крива рода $g$ над $\mathbb{Q}$, са Јакобијаном $J$. Ако је ранг $r$ Јакобијана $J(\mathbb{Q})$ криве $C$ строго мањи од $g$, тада је $C(\mathbb{Q})$ је коначан, тј. на $C$ се налази само коначно много рационалних тачака.

**Доказ.** При услову теореме мора бити $g > 0$. Претпоставимо да је $C(\mathbb{Q}) \neq \emptyset$ (у супротном је теорема јасно важи). Ако је $g = 1$, тада је $r = 0$, тј. и сам Јакобијан $J(\mathbb{Q})$ се састоји из коначно тачака. Знамо да постоји „1-1" пресликање $i : C(\mathbb{Q}) \longrightarrow J(\mathbb{Q})$, одакле је $C(\mathbb{Q})$ коначан скуп. На даље је $g \geq 2$.

Одаберимо прост број $p$ за који $C$ има добру редукцију. Означимо

$$V = \{\omega \in \Omega_C^{\mathrm{reg}}(\overline{\mathbb{Q}}_p) | (\forall P \in J(\mathbb{Q}))\, \langle P, \omega \rangle = 0\}.$$

Знамо да за сваку тачку $P$ коначног реда у Јакобијану је испуњен овај услов из дефиниције $V$ за све форме, тако да је из адитивности интеграла услов дефиниције скупа $V$ еквивалентан са тим да

је $\langle P_j, \omega \rangle = 0$, за базу $P_1$, $P_2$, ... , $P_r$ слободног дела Јакобијана, а из линеарности интеграла имамо $r$ линеарних услова, одакле је $\dim V \geq g - r > 0$, јер знамо да је простор регуларних диференцијалних форми димензије $g$ по теореми 12. Дакле, постоји неко $0 \neq \omega \in V$.

Одаберимо $P_0 \in C(\mathbb{Q})$, тачку помоћу које ћемо да дефинишемо $i : C \longrightarrow J$. Тада је $i(P) \in J(\mathbb{Q})$, па је $0 = \langle i(P), \omega \rangle = \int_{P_0}^{P} \omega$ (ово смо видели у прошлој глави), за све $P \in C(\mathbb{Q})$. По теореми 28 из претходне главе, знамо да је број оваквих тачака $P$ коначан у свакој класи остатака у $C(\mathbb{Q}_p)$ (у смислу да се редукцијом по модулу $p$ своде на исту тачку у $\overline{C}(\mathbb{F}_p)$). Закључак теореме сада следи из тога да је број могућих класа остатака на кривој $\#\overline{C}(\mathbb{F}_p)$ коначан број (јер имамо коначно могућности за потенцијалне тачке) па како у свакој класи има коначно много рационалних тачака и укупан број рационалних тачака на $C$ је коначан.

## 6.2 Колеманово појачање

Следи теорема коју ћемо примењивати (или неке њене појачане облике) на једначине у следећој глави, пошто претходна теорема нам не даје никакво упутство како бисмо решили неку Диофантову једначину.

**Теорема 30.** Нека је $C$ апсолутно несводљива, глатка, пројективна крива над $\mathbb{Q}$, рода $g$ и са Јакобијаном $J$, ранга $r$. Препоставимо да је $r < g$. Нека је $p > 2g$ прост број за који $C$ има добру редукцију. Тада

$$\#C(\mathbb{Q}) \leq \#\overline{C}(\mathbb{F}_p) + 2g - 2.$$

**Доказ.** Претпоставимо да постоји тачка $P_0 \in C(\mathbb{Q})$, иначе је теорема већ тачна. Као у доказу Шаботијеве теореме, постоји ненула диференцијал $\omega \in \Omega^{\mathrm{reg}}_C(\mathbb{Q}_p)$, такав да $\int_{P_0}^{P} \omega = 0$, за све $P \in C(\mathbb{Q})$.

Посматрајмо тачку $\overline{Q} = \overline{P_0} \in \overline{C}(\mathbb{F}_p)$ и пошто је то глатка тачка, јер крива има добру редукцију модуло $p$, можемо је подићи до тачке $Q \in C(\mathbb{Q}_p)$.

Даље, можемо да одаберемо равномернизатор $t \in \mathbb{Q}_p(C)^*$ у $Q$, такав да се редукцијом модуло $p$ слика у равномернизатор $\bar{t} \in \mathbb{F}_p(\overline{C})^*$ у тачки $\overline{Q}$. Ово ћемо проверити само за хиперелиптичке криве, криве које су од највећег интереса у овом мастер раду. Нека је $C : y^2 = f(x)$. Тада имамо њену редукцију $\overline{C} : y^2 = \overline{f}(x)$ са тачком $(\overline{x_0}, \overline{y_0}) \in C(\mathbb{F}_p)$, која се подиже у тачку $(x_0, y_0) \in C(\mathbb{Q}_p)$.

Ако је $\overline{y_0} \neq 0$, тада је свакако и $y_0 \neq 0$, па можемо узети равномернизатор $x - x_0$ за тачку $Q$, који се слика у равномернизатор $x - \overline{x_0}$ у тачки $\overline{Q}$. Ако је $\overline{y_0} = 0$, тада можемо узети и $y_0 = 0$. Заиста, сличним поступком као у доказу тврђења 23 долазимо до тога. Пошто је $(\overline{x_0}, 0)$ глатка тачка криве $\overline{C}$, и $\dfrac{\partial y^2}{\partial y}(\overline{x_0}, 0) = 0$, мора бити $\dfrac{\partial f}{\partial x}(\overline{x_0}, 0) \neq 0$, одакле је $\overline{x_0}$ проста нула полинома $f(x)$, одакле се по Хенселовој леми подиже до неког $x_0 \in \mathbb{Q}_p$, па је $(x_0, 0) \in C(\mathbb{Q}_p)$ подизање тачке $(\overline{x_0}, 0)$. Сада за равномернизаторе у обе тачке можемо узети функцију $y$. Овим је тврђење доказано.

Можемо да скалирамо диференцијал $\omega$ тако да његова редукција $\overline{\omega}$ буде дефинисан и ненула, јер је $\overline{\omega}$ диференцијал за криву над коначним пољем, која има коначан број тачака. Тада је $\overline{\omega} \in \Omega^{\mathrm{reg}}_{\overline{C}}(\mathbb{F}_p)$, тј. то је регуларан диференцијал, а онда по тврђењу 21 знамо да је $\deg(\mathrm{div}(\overline{\omega})) = 2g - 2$.

Даље, како знамо да је простор диференцијала једнодимензиони над простором функција над кривом, постоји функција $f \in \mathbb{Q}_p(C)$ таква да $\omega = f dt$. Међутим, пошто знамо да је $\omega$ регуларан дивизор, тада $f$ не може имати полове, тј. $f \in \mathbb{Q}_p[C]$, а тада из доказа теореме 6 следи да се $f$ може представити као степени ред по $t$. Дакле $\omega = \omega(t)dt$, где је $\omega(t) \in \mathbb{Q}_p[[t]]$, тај степени ред. Сетимо се да смо скалирали $\omega$ тако да његова редукција $\overline{\omega}$ буде дефинисан и регуларан диференцијал, отуда сви коефицијенти у степеном реду за $\omega(t)$ морају заправо бити у $\mathbb{Z}_p$. Долазимо до закључка $\omega = \omega(t)dt$, за $\omega(t) \in \mathbb{Z}_p[[t]]$.

Тада је $\overline{\omega} = \overline{\omega}(\bar{t})d\bar{t}$. По дефиницији равномернизатора за тачку $\overline{Q}$ је

$$\overline{\omega}(\bar{t}) = \bar{t}^{\mathrm{ord}_{\overline{Q}}(\overline{\omega})}(u_0 + u_1\bar{t} + ...),$$

при чему $u_0 \in \mathbb{F}_p^*$, јер би у супротном и тај члан нестао у редукцији модуло $p$, па изабрани равномернизатор не би био равномернизатор.

По особини Колемановог интеграла из теореме 28 је $\int_{P_0}^{P} \omega = l(t(P))$, где је $l \in \mathbb{Q}_p[[t]]$ степени ред чији је формални извод $\omega(t)$ и $l(0) = 0$, за све $P \in C(\mathbb{Q}_p)$, такве да $\overline{P} = \overline{Q}$.
Сада можемо да применимо теорему 20 на степени ред $l(t)$, јер су испуњени сви услови - то је степени ред у $\mathbb{Q}_p$, чији је формални извод $\omega(t)$ степени ред са коефицијентима у $\mathbb{Z}_p$, чија слика при редукцији модуло $p$ је облика

$$\overline{\omega}(\bar{t}) = u_0\bar{t}^{\mathrm{ord}_{\overline{Q}}(\overline{\omega})} + u_1\bar{t}^{\mathrm{ord}_{\overline{Q}}(\overline{\omega})+1} + ...,$$

при чему $u_0 \in \mathbb{F}_p^*$ и $p > 2g = 2g - 2 + 2 \geq \mathrm{ord}_{\overline{Q}}(\overline{\omega}) + 2$. Ово последње важи због тога што је $\omega$ регуларан диференцијал, па нема полова и у степен $\mathrm{div}(\omega)$ само улазе редови њихових нула, а степен овог дивизора је, као што знамо, баш $2g - 2$. Закључак је да ред $l(t)$ има највише $\mathrm{ord}_{\overline{Q}}(\overline{\omega}) + 1$ нулу у $p\mathbb{Z}_p$. Међутим, то је довољно да закључимо да је број тих нула уједно и број тачака $P \in C(\mathbb{Q}_p)$ за које је $\int_{P_0}^{P} \omega = 0$. Треба оправдати да $t(P) \in p\mathbb{Z}_p$. То следи из чињенице да се $P$ редукује у исту тачку као и $Q$ модуло $p$, а $t$ је равномернизатор у $Q$ који се редукује у равномернизатор у $\overline{Q}$ модуло $p$, тј. $\bar{t}(\overline{Q}) = 0$ у $\mathbb{F}_p$, одакле $t(Q) \in p\mathbb{Z}_p$, па самим тим и $t(P) \in p\mathbb{Z}_p$, јер је $t$ рационална функција, а $P$ и $Q$ се поклапају модуло $p$.

Како знамо да за све тачке $P \in C(\mathbb{Q})$ важи $\int_{P_0}^{P} \omega = 0$, то је

$$\#C(\mathbb{Q}) \leq \# \left\{ P \in C(\mathbb{Q}_p) \mid \int_{P_0}^{P} \omega = 0 \right\},$$

а по претходно доказаном је

$$\# \left\{ P \in C(\mathbb{Q}_p) \mid \int_{P_0}^{P} \omega = 0 \right\} \leq \sum_{\overline{Q} \in \overline{C}(\mathbb{F}_p)} (\mathrm{ord}_{\overline{Q}}(\overline{\omega}) + 1).$$

За крај је довољно да уочимо да је

$$\sum_{\overline{Q} \in \overline{C}(\mathbb{F}_p)} (\mathrm{ord}_{\overline{Q}}(\overline{\omega}) + 1) = \sum_{\overline{Q} \in \overline{C}(\mathbb{F}_p)} (\mathrm{ord}_{\overline{Q}}\, \overline{\omega}) + \sum_{\overline{Q} \in \overline{C}(\mathbb{F}_p)} 1 = \deg(\mathrm{div}(\overline{\omega})) + \#\overline{C}(\mathbb{F}_p).$$

Пошто је $\deg(\mathrm{div}(\overline{\omega})) = 2g - 2$, повезивањем последњих неколико линија добијамо тражени закључак

$$\#C(\mathbb{Q}) \leq \#\overline{C}(\mathbb{F}_p) + 2g - 2.$$

Даље наводимо неколико сродних верзија овој теореми. Крећемо са резултатима из оригиналног Колемановог рада и завршавамо са уопштењима ове теореме које је доказао Михаел Штол у својим радовима.

## 6.3 Колеманов рад „Ефективни Шаботи"

Овде се бавимо прегледом Колеманових оригиналних резултата из рада [15] у којем је он први доказао теорему. Као што видимо, теорему не можемо применити ако користимо просте бројеве 2 и 3, зато има одвојена теорема која може да послужи у том случају. Пре тога, формулисаћемо општију теорему коју је доказао Колеман, а видећемо да ток доказа прати процес доказивања теореме, само што је овде тај процес исписан доста једноставнијим речником.

Нека је $p$ фиксиран прост број. Уочимо $K$ комплетно потпоље $\mathbb{C}_p$ (подсетимо се, $\mathbb{C}_p$ је комплетирање алгебарског затворења $\mathbb{Q}_p$) и $A$ Абелов варијетет над $K$ димензије $g$ (за наше потребе ће $K$ бити баш $\mathbb{Q}_p$, а $A$ ће играти улогу Јакобијана криве, који је, као што знамо Абелов варијетет). У свом раду у којем уводи интеграцију [16], за сваки регуларан диференцијал $\omega$, Колеман доказује да постоји локално аналитички хомоморфизам $\lambda_\omega$, такав да $d\lambda_\omega = \omega$.

За подгрупу $G$ од $A(K)$, дефинишемо скуп $V_G$ као скуп свих регуларних диференцијала $\omega$ за које је $\lambda_\omega(x) = 0$, за све $x \in G$ (овај скуп се у доказу теореме приказује као скуп $V$ регуларних диференцијала $\omega$ таквих да $\langle P, \omega\rangle = 0$, за све $P \in J(\mathbb{Q}))$. Тада је $V_G$ потпростор и при томе се испоставља да ако је $L$ коначно генерисана подгрупа од $A(K)$, ранга $r$, тада је димензија $V_L$ бар $g - r$, што је позитивно када је $r \leq g - 1$. У доказу теореме, ово је аналог онога да постоји ненула регуларан диференцијал $\omega$ у $V$. Тада имамо тврђење које се изводи из својстава Колеманове интеграције.

**Тврђење 41.** Нека је $K$ комплетно потпоље од $\mathbb{C}_p$, са дискретном валуацијом. Нека је $j : (C, c_0) \longrightarrow (A, 0)$ морфизам над $K$ криве $C$ са уоченом тачком $c_0$ на њој у Абелов варијетет, тако да и оба имају добру редукцију. Нека је $G$ подгрупа од $A(K)$. Тада се $j(C(K)) \cap G$ се садржи у скупу свих $x \in C(K)$, таквих да

$$\int_{c_0}^{x} \omega = 0,$$

за све $\omega \in j^* V_G$, где $*$ означава пул-бек форми.

Нека је $K$ бројно поље, $C$ крива дефинисана над $K$ и узмимо да је $L = J(C)$ - Јакобијан криве $C$ над пољем $K$. Нека је $v : K \longrightarrow \mathbb{C}_p$ место изнад простог броја $p$ у ком $C$ има добру редукцију и $K_v$ комплетирање $K$ у односу на $v$. Тада применом претходног тврђења можемо да закључимо

$$v(C(K)) \subset \{x \in C(K_v) \mid (\forall \omega \in j^* V_{v(L)}) \lambda_\omega(x) = 0\},$$

где је $j : C \longrightarrow J(C)$ познати морфизам и $\lambda_\omega(x) = \int_{v(c_0)}^{x} \omega$.

Идеја Шаботијевог доказа је била у томе што је десна страна инклузије коначан скуп, што је случај ако је $V_{v(L)}$ позитивне димензије, а то се сигурно дешава када је ранг $v(L)$ највише $g-1$. Међутим, Шаботијев доказ се ту завршио, без конкретне процене, а Колеман уз помоћ анализе $p$-адских степених редова поставља конкретно ограничење. Уводимо нове ознаке - за позитиван реалан број $s$, означимо

$$B[s] = \{x \in \mathbb{C}_p \mid |x|_p \leq s\},$$

даље, $\operatorname{ord}_0 f$ је степен најмањег степена $t$ (дакле, који не иде уз коефицијент 0) у степеном реду $f(t)$, док, као и до сада, надвлачење представља рестрикцију модулу $p$ и још за $s < 1$ уведимо ознаку

$$n(k,s) = \max\left\{ n \in \mathbb{N} \mid \frac{s^n}{|n|_p} \geq \frac{s^k}{|k|_p} \right\}.$$

Теорема која броји нуле $p$-адског степеног броја настаје из следећег тврђења.

**Тврђење 42.** Нека је $f(t) \in \mathbb{C}_p[[t]]$, такав да $f'(t) \in \mathbb{R}_p[[t]]$, где је $f'(t)$ формални извод степеног реда $f(t)$, а $\mathbb{R}_p$ прстен целих поља $\mathbb{C}_p$. Ако је $\operatorname{ord}_0 \overline{f'} = k - 1 < \infty$, тада $f(t)$ има највише $n(k,s)$ нула у $B[s]$.

Видимо да треба да знамо да израчунамо бројеве облика $n(k,s)$, а одговор на то нам даје следеће тврђење. Нећемо га доказивати, али ћемо израчунати неке конкретне вредности касније.

**Тврђење 43.** Нека је $s = \operatorname{ord}_p k$. Тада

$$n(k, |p|_p) = \begin{cases} k, & (\forall r > s)\left\{\frac{-k}{p^r}\right\} > \frac{r-s}{p^r} \\ \max\left\{ p^r\left(-\left[\frac{-k}{p^r}\right]\right) \mid \left\{\frac{-k}{p^r}\right\} \leq \frac{r-s}{p^r} \right\}, & \text{иначе.} \end{cases} \tag{6}$$

Долазимо до последњег тврђења које нам је потребно за доказ теореме. Нека је сада $K$ коначно раширење $\mathbb{Q}_p$, индекса рамификацаије $e$, са прстеном целих $R$ и количницким пољем $\mathbb{F}_q$.

**Тврђење 44.** Нека је $C$ глатка крива над $R$ и нека је $\omega$ регуларан диференцијал криве $C$ над $R$, такав да $\overline{\omega} \neq 0$. Нека је $\lambda$ таква да је $d\lambda = \omega$, као и раније. Тада је број нула степеног реда $\lambda$ у $C(K)$ највише

$$\sum_{\overline{Q} \in \overline{C}(\mathbb{F}_q)} n(\mathrm{ord}_{\overline{Q}}\,\overline{\omega} + 1, |p|_p^{\frac{1}{e}}).$$

Као последицу ових наведених тврђења, можемо доказати последње тврђење које нам фали за доказ читаве теореме.

**Тврђење 45.** Нека је $e = 1$ и $v_{\overline{Q}}(\overline{\omega}) < p - 2$, за све $\overline{Q} \in \overline{C}(\mathbb{F}_q)$ (ово је испуњено ако је $g > 2p$). Тада је број нула $\lambda$ на $C(K)$ највише

$$q - 1 + 2g(\sqrt{q} + 1).$$

Овај број се добија тако што користимо Хасе-Вејлову теорему ($|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}$, иначе се у доказу, у процени на десној страни баш добија $\#C(\mathbb{F}_q) + 2g - 2$, као што и гласи у теореми. Тачност теореме је последица свих претходних тврђења и Колеман је то формулисао на следећи начин.

**Теорема 31.** Нека је $C$ глатка крива рода $g$, над бројним пољем $K$, при чему је ранг Јакобијана те криве $r < g$. Претпоставимо да је $\mathfrak{p}$ нерамификовани прост идеал у $K$ у којем $C$ има добру редукцију, при чему је карактеристика количничког поља за $\mathfrak{p}$ строго већа од $2g$. Тада

$$\#C(K) \leq N\mathfrak{p} + 2g(\sqrt{N\mathfrak{p}} + 1) - 1,$$

при чему је $N\mathfrak{p}$ ознака за норму идеала $\mathfrak{p}$.

Сада се враћамо случајевима $p = 2$ и $p = 3$, који се никако не могу појавити у примени теореме, јер посматрамо криве рода $g \geq 2$. Ту имамо следећу теорему, којој ћемо доказати први део уз веровање неких чињеница.

**Теорема 32.** Препоставимо да је $C$ крива рода 2 над $\mathbb{Q}$, чији Јакобијан има ранг највише 1.
(1) Ако $C$ има добру редукцију за просте бројеве 2 и 3, тада $\#C(\mathbb{Q}) \leq 12$.
(2) Ако $C$ има добру редукцију за $p = 3$ и има четири рационалне тачке рамификације, тада $\#C(\mathbb{Q}) \leq 6$.

**Доказ.** Претпоставимо да $C$ има добру редукцију по модулу 2. Нека је $\omega$ регуларан диференцијал чија редукција $\overline{\omega}$ по модулу 2. Тада, по претходном, морамо да докажемо

$$\sum_{\overline{Q} \in \overline{C}(\mathbb{F}_2)} n(\operatorname{ord}_{\overline{Q}} \overline{\omega} + 1, |2|_2) \leq 12.$$

Сетимо се да је $\deg(\operatorname{div}(\overline{\omega})) = 2 = 2 \cdot 2 - 2$, јер је крива $C$ рода $g = 2$, одакле је $\sum_{\overline{Q} \in \overline{C}(\mathbb{F}_2)} \operatorname{ord}_{\overline{Q}} \overline{\omega} \leq 2$, а самим тим и $\operatorname{ord}_{\overline{Q}} \overline{\omega} \leq 2$, за све $\overline{Q} \in \overline{C}(\mathbb{F}_2)$. Дакле, могу да се појаве три вредности $n(1, |2|_2)$, $n(2, |2|_2)$ и $n(3, |2|_2)$. Одредимо их по дефиницији.

$$n(1, |2|_2) = \max \left\{ \{n \mid \frac{\frac{1}{2^n}}{|n|_2} \geq \frac{\frac{1}{2}}{|1|_2} = \frac{1}{2} \right\},$$

тј. тражимо највеће $n$ за које је $2 \geq 2^n |n|_2$. Запишимо $n = 2^k m$, где је $m$ непаран број, тада је услов еквивалентан са $1 \geq 2^k m - k \geq 2^k - k$. Међутим, како је $k + 1 < 2^k$, за $k \geq 2$, то мора бити $k \in \{0, 1\}$. Ако је $k = 0$, добијамо $1 \geq m$, тј. $n = 1$, а ако је $k = 1$, онда из $1 \geq 2m - 1$ је $m = 1$, тј. $n = 2$, па је ово и највећи број са овим својством. Дакле $n(1, |2|_2) = 2$. Пошто је

$$\frac{\frac{1}{2}}{|1|_2} = \frac{\left(\frac{1}{2}\right)^2}{|2|_2} = \frac{1}{2},$$

онда је аутоматски $n(2,|2|_2)=2$. За одређивање $n(3,|2|_2)$ треба да нађемо највећи $n$ такав да $8 \geq 2^n|n|_2$. Истим записом као до сада, $n=2^k m$, долазимо до тога да $3 \geq 2^k - k$, односно $k \leq 2$. Провером три случаја, добијамо да је највећи број који се уклапа $n=4$, одакле је $n(3,|2|_2)=4$. Сада видимо да треба да докажемо

$$2\#\{\overline{Q} \in \overline{C}(\mathbb{F}_2) \mid \mathrm{ord}_{\overline{Q}}(\overline{\omega}) \leq 1\} + 4\#\{\overline{Q} \in \overline{C}(\mathbb{F}_2) \mid \mathrm{ord}_{\overline{Q}}(\overline{\omega}) = 2\} \leq 12.$$

Знамо да број тачака на кривој $\overline{C}$ у пољу $\mathbb{F}_2$ не може бити већи од 6, међутим, испоставља се да ако постоји тачка $\overline{Q} \in \overline{C}(\overline{F}_2)$, таква да је $\mathrm{ord}_{\overline{Q}}(\overline{\omega}) = 2$, онда их на кривој $\overline{C}$ може бити највише 5. Пошто може да буде највише једна тачка са тим својсвом, у оба случаја добијамо да тај збир не може да пређе $6 \cdot 2 = 4 \cdot 2 + 1 \cdot 4 = 12$, што је и требало показати.

Други део се доказује на сличан начин, имајући у виду да $C$ има рационалне тачке рамификације.

## 6.4 Уопштења Колеманове теореме

У овом делу наводимо без доказа два побољшања Колеманове теореме, које је у својим радовима доказао Михаел Штол.

**Теорема 33.** Нека је $C$ апсолутно несводљива, глатка, пројективна крива над $\mathbb{Q}$, рода $g$ и са Јакобијаном $J$, ранга $r$. Препоставимо да је $r < g$. Нека је $p > 2r+2$ прост број за који $C$ има добру редукцију. Тада

$$\#C(\mathbb{Q}) \leq \#\overline{C}(\mathbb{F}_p) + 2r.$$

**Доказ.** Погледати у [56].

**Теорема 34.** Нека је $C$ хиперелиптичка крива над $\mathbb{Q}$, рода $g$ са Јакобијаном $J$. Нека је ранг $r$ Јакобијана $J(\mathbb{Q}$ задовољава $r \leq g-3$. Тада

$$\#C(\mathbb{Q}) \leq 8(r+4)(g-1) + \max\{1, 4r\} \cdot g.$$

**Доказ.** Погледати у [61].

# 7 Решавање неких Диофантових једначина

Пре него што кренемо у решавање неких Диофантових једначина, наведимо уопштено шта нам је потребно да решимо неку једначину уз помоћ Шаботи-Колемановог метода. Нека је $C$ крива којој тражимо рационалне тачке (тј. коју добијемо из једначине коју решавамо), $r$ њен ранг и $g$ њен род.

За почетак, треба да одредимо групну структуру Јакобијана $J(\mathbb{Q})$, где мора да се испуни $r \leq g-1$, а и врло је пожељно да знамо генераторе $J(\mathbb{Q})$. Даље, желимо неки прост број $p$ у којем $C$ има добру редукцију, такав да у свакој класи остатака модуло $p$ на кривој $C$, што су класе тачака из $\overline{C}(\mathbb{F}_p)$, постоји рационална тачка која се редукује у ту класу и при томе да се број рационалних тачака које смо нашли поклапа са оценом коју добијемо посматрајући Колеманов интеграл.

## 7.1 Једначина $y^2 = x(x-1)(x-2)(x-5)(x-6)$

Ово је најпознатији пример примене Шаботи-Колемановог метода, јер како неки математичари који се баве овом облашћу тврде, ово је прва Диофантова једначина која је у потпуности решена коришћењем Шаботи-Колемановог метода. Задатак је решити у скупу рационалних бројева једначину

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

Посматрамо хиперелиптичку криву $C$ задату овом једначином и већ знамо доста информација о њој.
(1) Крива $C$ је рода $g = 2$.
(2) $C$ има добру редукцију за $p = 7$, јер 7 не дели разлику различитих нула овог полинома по $x$, одакле не дели његову дискриминанту, што управо значи да је $p = 7$ прост број добре редукције за $C$.
(3) У примеру 57 смо видели да за Јакобијан ове криве важи $J(\mathbb{Q}) \cong \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^4$, одакле је ранг њеног Јакобијана $r = 1$.

Приметимо да су испуњени услови за примену Шаботи-Колеманове теореме, јер $p = 7 > 4 = 2g$ и $r = 1 < 2 = g$, одакле можемо да

закључимо

$$\#C(\mathbb{Q}) \leq \#\overline{C}(\mathbb{F}_7) + 4 - 2.$$

Остаје још да одредимо број тачака на криви редукованој по модулу 7, пошто је непарног степена, имамо једну бесконачну тачку, а остале су у скупу $\{(0,0),(1,0),(2,0),(5,0),(6,0),(3,\pm 1)\}$, јер једино за $x = 4$ не добијамо решење, пошто $6 \equiv -1 \pmod 7$ није квадрат по модулу 7. Дакле, $\#\overline{C}(\mathbb{F}_7) = 8$, одакле је

$$\#C(\mathbb{Q}) \leq 10.$$

Са друге стране, на овој кривој $C$ заиста постоји 10 рационалних тачака и то су тачке из скупа

$$\{\infty,(0,0),(1,0),(2,0),(5,0),(6,0),(3,\pm 6),(10,\pm 120)\}.$$

Одавде закључујемо да је баш $\#C(\mathbb{Q}) = 10$ и

$$C(\mathbb{Q}) = \{\infty,(0,0),(1,0),(2,0),(5,0),(6,0),(3,\pm 6),(10,\pm 120)\}.$$

Ова једначина није тако ретка у литератури, може се пронаћи, на пример, у [31], [53], [41].

## 7.2 Једначина $y^2 = x(x-3)(x-4)(x-6)(x-7)$

Други пример је сличан првом по поставци, а добра је илустрација шта треба урадити када не пролази директно Шаботи-Колеманова теорема. Задатак је решити у скупу рационалних бројева једначину

$$y^2 = x(x-3)(x-4)(x-6)(x-7).$$

Опет посматрамо криву $C$ дефинисану овом једначином. Тада:
(1) $C$ је рода $g = 2$.
(2) $C$ има добру редукцију за $p = 5$, јер, као и у претходном примеру, одмах видимо да разлика било која два различита корена овог полинома по $x$ није дељива са 5.
(3) За Јакобијан ове криве важи $J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4$, што можемо видети у примеру број 58 и одакле је ранг тог Јакобијана $r = 0$.

Испуњени су сви услови за примену Шаботи-Колеманове теореме, јер $p = 5 > 4 = 2g$ и $r = 0 < 2 = g$. Још треба да одредимо $\#\overline{C}(\mathbb{F}_5)$. Видимо да се у полиному по $x$ појављује сваки остатак по модулу 5, одакле је јасно

$$\overline{C}(\mathbb{F}_5) = \{\infty, (0,0), (1,0), (2,0), (3,0), (4,0)\},$$

и $\#\overline{C}(\mathbb{F}_5) = 6$, што нам даје горњу процену за број рационалних решења

$$\#C(\mathbb{Q}) \leq 6 + 4 - 2 = 8.$$

Међутим, када кренемо да тражимо решења, лако налазимо 6 решења $\{\infty, (0,0), (3,0), (4,0), (6,0), (7,0)\}$ и не успевамо да нађемо још два решења! Поставља се питање да ли је граница у Шаботи-Колемановој теореми довољна да решимо ову једначину. Испоставља се да није, што видимо применом једне од побољшаних верзија, тј. теореме 33, чији су услови такође испуњени, јер $r = 0 < 2 = g$ и $p = 5 > 2 = 2r + 2$, одакле је

$$\#C(\mathbb{Q}) \leq 6 + 0 = 6.$$

Пошто смо и нашли већ 6 рационалних тачака на кривој, одатле знамо $\#C(\mathbb{Q}) = 6$ и

$$C(\mathbb{Q}) = \{\infty, (0,0), (3,0), (4,0), (6,0), (7,0)\}.$$

Ова једначина се може наћи у [41].

## 7.3 Једначина облика $y^2 = x(x^2-1)(x-\frac{1}{\lambda})(x^2+ax+b)$

Претпоставимо да желимо да решимо Диофантову једначину

$$y^2 = x(x^2-1)(x-\frac{1}{\lambda})(x^2+ax+b),$$

при чему $a, b, \lambda \in \mathbb{Z}$, $3^{2r} \mid\mid \lambda$, за неко $r \in \mathbb{N}$ и $3 \nmid b(1-a+b)(1+a+b)$. Ови услови гарантују да крива

$$C : y^2 = x(x^2-1)(x-\frac{1}{\lambda})(x^2+ax+b)$$

има добру редукцију модуло 3. Тада је $C$ крива рода 2. Такође, видимо да крива има четири тачке рамификације, то су тачке из скупа $\{(0,0),(1,0),(-1,0),(\lambda,0)\}$, одакле можемо да применимо теорему 32 која нам даје одмах да је број рационалних тачака на овој кривој највише 6. Нашли смо већ четири рационалне тачке, а преостале две су у бесконачности, јер је полином по $x$ парног степена, водећег коефицијента један (што је квадрат). Одредили смо све рационалне тачке

$$C(\mathbb{Q}) = \{\infty_+, \infty_-, (0,0), (\pm 1, 0), (\lambda, 0)\}.$$

Два примера оваквих једначина су

$$y^2 = x(x^2-1)\left(x+\frac{1}{9}\right)(x^2-4x-1),$$

при чему смо у примеру број 60 видели да је Јакобијан ове криве над $\mathbb{Q}$ ранга 1,

$$y^2 = x(x^2-1)\left(x-\frac{1}{9}\right)(x^2-4x-1),$$

за коју је такође $J(\mathbb{Q})$ ранга 1, што смо навели у истом примеру. Дакле, сва рационална решења прве једначине су $\{0, \pm 1, -\frac{1}{9}\}$, док су сва рационална решења друге једначине $\{0, \pm 1, \frac{1}{9}\}$.

## 7.4 Једначина $y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$

Овај пример је веома користан јер конкретно имитира процедуру Шаботи-Колемановог метода. Нећемо га решити самом применом теореме, јер сама теорема није довољна за коначан закључак и стога ћемо ручно поновити апстракти поступак из доказа теореме, одакле би овај пример могао да понесе титулу најилустративнијег примера. Задатак је решити у скупу $\mathbb{Q}$ једначину

$$y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

Нека је $C : y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$. Тада брзо изводимо следеће закључке.

(1) Крива је рода $g = 2$.
(2) Дискриминанта овог полинома по $x$ је $15159296 = 2^{12} \cdot 3701$, одакле ова крива има добру редукцију модуло сваки прост број $p \notin \{2, 3701\}$.
(3) У примеру 61 смо видели да је Јакобијан криве $C$

$$J(C) \cong \mathbb{Z}[\infty_+ - \infty_-].$$

Одавде имамо информацију да је $J(C)$ ранга $r = 1$, али и додатно, знамо његов генератор. То ће бити веома важно у решавању ове једначине.

Ручно налазимо следећа решења $(0, 1)$, $(0, -1)$, $(-3, 1)$, $(-3, -1)$ и наравно два бесконачна ресехња. Укупно смо их нашли 6. Желимо да применимо теорему на ову једначину. Услов $r = 1 \geq 1 = 2 - 1 = g - 1$ је испуњен. Најмањи прост број који можемо узети је $p = 5$, јер нам треба услов да је $p > 2g = 4$. За $p = 5$ имамо

$$\overline{C}(\mathbb{F}_5) = \{(0, \pm 1), (1, 0), (2, \pm 1), \infty_\pm\},$$

тј. $\#\overline{C}(\mathbb{F}_5) = 7$. Применом теореме, можемо да закључимо

$$\#C(\mathbb{Q}) \leq 7 + 4 - 2 = 9,$$

а то нам није довољно. Треба нам неко јаче процењивање броја тачака. Зато, ипак посмтрајмо $p = 3$. Јесте $3 < 4$, али нећемо се директно позвати на теорему. Радимо над пољем $\mathbb{Q}_3$. Тада је

$$\overline{C}(\mathbb{F}_3) = \{(0, \pm 1), \infty_\pm\}.$$

Крива је рода $g = 2$ (као и њене редукције), одакле је скуп регуларних диференцијала векторски простор димензије 2 (у складу са теоремом 12) и база тог простора је скуп $\left\{\dfrac{dx}{y}, \dfrac{xdx}{y}\right\}$. Желимо да нађемо ненула диференцијал $\omega$ такав да је $\langle P, \omega\rangle = 0$, за све $P \in J(C)$. Овде користимо то да знамо генератора за $J(C)$, треба одредити константу $k$, такву да за $\omega = k\dfrac{dx}{y} + \dfrac{xdx}{y}$ важи $\langle \omega, [\infty_+ - \infty_-]\rangle = 0$. Израчунали смо у петој глави

$$\left\langle \frac{dx}{y}, [\infty_+ - \infty_-] \right\rangle = \frac{29}{3} + O(3^3)$$

и

$$\left\langle \frac{xdx}{y}, [\infty_+ - \infty_-] \right\rangle = 8 + O(3^3).$$

Стога, узмимо

$$k = \frac{-8 + O(3^3)}{\frac{29}{3} + O(3)} = \frac{-24 + O(3^4)}{29 + O(3^4)} = (-24) \cdot 14 + O(3^4) = 69 + O(3^4),$$

јер су ове последње операције рађене по модулу $81 = 3^4$ и $29^{-1} \equiv 14 \pmod{81}$. Даље знамо да било која рационална тачка мора да се редукује у неку од тачака у $\overline{C}(\mathbb{F}_3)$, а за сваку од тачака на редукованој кривој постоји рационална тачка која се редукује у њу. Нека је $P$ рационална тачка која се редукује у исту тачку као и нека од познатих тачака $P_0$. Тада мора бити $\int_{P_0}^{P} \omega = 0$! Ово користимо да ограничимо број рационалних тачака у свакој класи по модулу 3.

Кренимо од класе $(0,1)$. Нека је $P = (t,s) \equiv (0,1) \pmod 3$. Сада рачунамо

$$\int_{(0,1)}^{(t,s)} \omega = \int_{(0,1)}^{(t,s)} \frac{(k+x)dx}{y} = \int_0^t (k+x)(1 - 3x + 11x^2 - 56x^3 + ...) =$$

$$= \int_0^t k + (1-3k)x + (11k-3)x^2 + ... = kt + \frac{1-3k}{2}t^2 + \frac{11-3k}{3}t^3 + O(t^4).$$

У рачуну смо овде стали, видећемо ускоро зашто. Приметимо да $t \equiv 0 \pmod 3$, одакле је $t = 3z$, за неко $z \in \mathbb{Z}_3$. Имамо

$$\int_{(0,1)}^{(t,s)} \omega = 3(69+O(3^4))z + \frac{9}{2}(1-207+O(3^5))z^2 + 9(-3+11\cdot 69+O(3^4))z^3 + O(3^4) =$$

$$= (3^2 \cdot 23 + O(3^5))z + (-3^2 \cdot 103 + O(3^7))z^2 + (3^3 \cdot 252 + O(3^6))z^3 + O(3^4) =$$
$$= (3^2 \cdot 23 + O(3^5))z + (-3^2 \cdot 103 + O(3^7))z^2 + (3^5 + O(3^6))z^3 + O(3^4).$$

Можемо да применимо тврђење 32 на овај степени ред $\sum_{n=1}^{\infty} a_n z^n$ (јер ће заиста коефицијенти $a_n$ да теже 0 у $p$-адској топологији, јер је $t = 3z$, а степени $t$, ондосно $3z$ само расту), где видимо да је $\min\{\mathrm{ord}_3(a_n) \mid n \in \mathbb{N}\} = 2$, јер су прва два коефицијента реда дељива тачно са $3^2$, док су сви остали дељиви бар са $3^4$. Одавде је највећи индекс таквог коефицијента $N = 2$, одакле овај степени ред има највише две нуле у $\mathbb{Z}_p$. Сада видимо зашто је у примеру 62 било довољно да се зауставимо код $O(3^5)$ у рачунању интеграла. Закључујемо да у овој класи модуло 3 постоји највише 2 рационалне тачке на кривој $C$, а ми смо их и нашли - у питању су $(0, 1)$ и $(-3, 1)$! Ово је конкретизација доказа главне теореме!

Урадимо сада исти поступак за другу класу $(0, -1)$. Међутим, нема потребе да се мучимо, јер видимо да нема разлике у односу на претходни случај. Од почетка се губи друга компонента, јер тако израчунавамо Колеманов интеграл. Добијамо потпуно исти степени ред као малопре, са истим закључком да постоје највише две тачке које се редукују на њу и то су $(0, -1)$ и $(-3, 1)$.

Пошто је редукција добра, једине тачке које се редукцијом сликају у бесконачне тачке су управо бесконачне тачке. Овим смо успели да боље ограничимо број рационалних тачака на кривој $C$. Уз постепено рачунање ових интеграла добили смо ограничење

$$\#C(\mathbb{Q}) \leq 2 + 2 + 1 + 1 = 6,$$

а 6 тачака смо и нашли, одакле је

$$C(\mathbb{Q}) = \{(0, 1), (0, -1), (-3, 1), (-3, -1), \infty_+, \infty_-\}.$$

**Коментар.** Можемо да приметимо да смо у овом доказу имитирали доказ Колеманове теореме за $p = 3$, односно да смо оправдали примену теореме за $p = 3$, која је била неоправдана из услова $p > 4$, а процена коју смо добили се стварно поклапа са одабиром $p = 3$, јер је тада $\overline{C}(\mathbb{F}_3) + 2g - 2 = 4 + 4 - 2 = 6$.
Ова једначина се може наћи у [45] и у [31].

## 7.5 Мордел-Вејлово решето - $y^2 = 2x^6 - 3x^2 - 2x + 1$

Доказаћемо да су сва рационална решења наведене једначине у скупу

$$A = \{(0,1), (0,-1), (-2,11), (-2,-11)\}.$$

Нека је $C : y^2 = 2x^6 - 3x^2 - 2x + 1$, тада је $C$ глатка крива, којој знамо 4 рационалне тачке. Изводимо закључке.
(1) $C$ је рода $g = 2$.
(2) Дискриминанта полинома по $x$ је $41879552 = 2^{11} \cdot 11^2 \cdot 13^2$, што значи да $C$ има добру редукцију за све просте бројеве $p \notin \{2, 11, 13\}$.
(3) Може се показати да је Јакобијан криве

$$J(\mathbb{Q}) \cong \mathbb{Z}[(-2,-11) - (0,1)].$$

Знамо да је ранг $J(\mathbb{Q})$ једнак $r = 1$, одакле је испуњен услов $r \leq g-1$. Међутим, директна употреба теореме нам не даје решење, границе које можемо да добијемо ће бити веће од 4 (имајмо на уму да сигурно у збиру имамо 2, да ли од $2g-2$ или од $2r$, а већ постојећа 4 рационална решења ће дати и различита решења модуло $p$, за све просте $p > 2$). Чак није довољна ни примена теореме за $p = 3$, јер тада добијемо процену да има највише 6 тачака! То је због чињенице да је

$$\overline{C}(\mathbb{F}_3) = \{(0,1), (0,-1), (1,1), (1,-1)\}.$$

Проверимо и ручно да нам сам модул 3 не може дати довољну информацију.

Тражимо регуларан диференцијал $\omega$ за који је $\int_{(0,1)}^{(-2,-11)} \omega = 0$. Довољно је то да проверимо, због линеарности интеграла и чињенице да је $[(-2,-11) - (0,1)]$ генератор Јакобијана криве $C$. Можемо да израчунамо да је тражени диференцијал

$$\omega = (66 + O(3^5))\frac{dx}{y} + \frac{xdx}{y}.$$

Онзначимо $k = 66 + O(3^5)$.

За сваку класу по модулу 3, постоји већ једна рационална тачка која се редукује у њу. Ако желимо овако да докажемо да су

то све тачке, морамо да докажемо да у свакој класи заиста постоји највише једна рационална тачка. То проверавамо рачунајући интеграл у свакој класи. Ипак немамо 4 случаја, већ само 2, пошто се случајеви $(0,1)$ и $(0,-1)$, односно $(1,1)$ и $(1,-1)$ исто испитују.

Нека је $P=(0,1)$. Нека је $Q=(t,s)$ рационална тачка која се редукује на $P$ модуло 3. Тада мора бити

$$0=\int_P^Q \omega=\int_{(0,1)}^{(t,s)}\frac{k+x}{y}dx=\int_0^t (k+x)(1+x+3x^2+O(x^3))dx=$$

$$=\int_0^t (k+(k+1)x+(3k+1)x^2+O(x^3))=\left[kx+\frac{(k+1)x^2}{2}+\frac{(3k+1)x^3}{3}+O(x^4)\right]\Bigg|_0^t=$$

$$kt+\frac{(k+1)t}{2}+\frac{(3k+1)t^3}{3}+O(t^4).$$

Знамо да се $t$ редукује у 0, што значи да је $t=3z$, $z\in\mathbb{Z}_p$, одакле овај степени ред је облика (када заменимо $k=66+O(3^5)$)

$$(3^2\cdot 22+O(3^6))z+(67\cdot 2^{-1}\cdot 3^2+O(3^7))z^2+(199\cdot 3^2+O(3^7))z^3+O(3^4),$$

па применом тврђења за број нула степеног реда, добијамо да постоји највише 3 рационалне тачке које се редукују на $(0,1)$. То ипак није довољно добро, пошто треба да добијемо само једну тачку која се редукује.

Испитајмо шта би се десило ако погледамо следећи степен тројке - 9, нека је $Q=(t,s)$ рационална тачка која се редукује на $P$ модуло 9. Цео поступак се понавља, сем последњег корака, када уместо $t=3z$, можемо да ставимо $t=9z$, одакле добијамо следећи степени ред

$$(3^3\cdot 22+O(3^7))z+(67\cdot 2^{-1}\cdot 3^4+O(3^9))z^2+(199\cdot 3^5+O(3^{10}))z^3+O(3^4).$$

У овом степеном реду је први коефицијент дељив тачно са $3^3$, док су сви други дељиви бар са $3^4$, одакле је број $N$ из тврђења 32 једанак 1, што значи да постоји само једна тачка која се модуло 9

редукује у $(0,1)$. Потпуно исти закључак имамо и за $P=(0,-1)$.

Нека је сада $P=(-2,-11)$ и $Q=(t,s)$ рационална тачка која се редукује на $P$ модуло 3. И даље рачунамо исти интеграл, само са промењеним границама

$$\int_{(-2,-11)}^{(t,s)} \frac{k+x}{y}dx.$$

Али морамо бити пажљиви! Функција $x$ није равномернизатор за тачку $(-2,-11)$, већ је то функција $u=x+2$! Стога, морамо све изразити преко $u$. Јасно је да је $du=dx$. Промениће се и границе, а пошто друга координата нема утицаја, имаћемо интеграл од 0 до $t+2$. Даље морамо променити

$$y^2=2x^6-3x^2-2x+1=121-374u+477u^2-320u^3+120u^4-24u^5+2u^6.$$

Такође се и развој за $\dfrac{1}{y}$ мења

$$(121-374u+477u^2-320u^3+120u^4-24u^5+2u^6)^{-\frac{1}{2}}=\frac{1}{11}+\frac{17u}{121}+\frac{195u^2}{1331}+O(u^3).$$

Тражени интеграл постаје

$$\int_{(-2,-11)}^{(t,s)} \frac{k+x}{y}dx=\int_0^{t+2}(k+1+u)(\frac{1}{11}+\frac{17u}{121}+O(u^2))du=$$

$$=\int_0^{t+2}\left(\frac{k+1}{11}+\frac{17k+28}{121}u+O(u^2)\right)du=$$

$$=\frac{k+1}{11}(t+2)+\frac{17k+28}{242}(t+2)^2+O(\frac{(t+2)^3}{3}).$$

Заменом $t+2=3z$, $z\in\mathbb{Z}_3$ (јер се $t$ редукује у $1=-2$ модуло 3), добијамо степени ред

$$\frac{3(k+1)}{11}z+\frac{9(17k+28)}{242}z^2+O(3^2).$$

Сада можемо да применимо тврђење 32 да закључимо да је $N = 1$. То иде једноставно, јер због тога што $3 \mid k$, следи да $3 \nmid k+1$, па $3 \mid\mid \dfrac{3(k+1)}{11}$, док су сви остали коефицијенти дељиви са бар $3^2$. Одавде овај степени ред може да има највише једну нулу. Овим смо закључили да у овом случају заиста нема других рационалних решења. Исто је и за $(-2, 11)$. Претходне закључке сводимо у следећу чињеницу.

Ако означимо $B_m(P) = \{Q \in C(\mathbb{Q}_3) \mid Q \equiv P \pmod{m}\}$, тада видимо да све рационалне тачке у

$$B_9(0,1) \cup B_9(0,-1) \cup B_3(-2,11) \cup B_3(-2,-11)$$

припадају $A = \{(0,1),(0,-1),(-2,11),(-2,-11)\}$. Иако бисмо могли да помислимо да је ово крај доказа, није! Разлог због којег није довољно да проверимо по модулу 9 су друге класе које могу да настану, које нисмо узели у разматрање. Стога, да бисмо завршили доказ, морамо ипак да докажемо да нема више рационалних решења у

$$B_3(0,1) \cup B_3(0,-1) \cup B_3(-2,11) \cup B_3(-2,-11).$$

Овде на сцену наступа *Мордел-Вејлово решето*. Уместо једног простог $p$ (у овом случају $p = 3$), посматраћемо још многе просте бројеве $p$ да бисмо извукли више информација. Наравно, и даље су дозвољени само прости бројеви у којима $C$ има добру редукцију. Информације ћемо извлачити из следећег комутативног дијаграма. Одаберимо $P_0 = (0,1)$ и подсетимо се да имамо следеће инјективно пресликавање

$$i : C \longrightarrow J, \qquad i(Q) = [Q - P_0],$$

као и да је

$$J(\mathbb{Q}) \cong \mathbb{Z} \cdot D, \qquad D = [(-2,-11) - (0,1)].$$

Тада је

$$i(0,1) = 0, \quad i(0,-1) = -2D, \quad i(-2,11) = -3D, \quad , i(-2,-11) = D.$$

Тада имамо комутативни дијаграм

$$\begin{array}{ccccc} C(\mathbb{Q}) & \xrightarrow{i} & J(\mathbb{Q}) & \xleftarrow[\eta]{} & \mathbb{Z} \\ \downarrow{\scriptstyle red} & & \downarrow{\scriptstyle red} & & \downarrow{\scriptstyle red} \\ C(\mathbb{F}_p) & \xrightarrow{i} & J(\mathbb{F}_p) & \xleftarrow[\eta]{} & \mathbb{Z}/N_p\mathbb{Z} \end{array}$$

На овом дијаграму је $N_p$ ред слике $\overline{D}$ у $J(\mathbb{F}_p)$, док је $\eta(m) = mD$. Корист коју извлачимо из разних простих бројева $p$ је следећа. Ако је $Q \in C(\mathbb{Q})$, тада $i(Q) = nD$, за неки природан број $n$. Занима нас какво то $n$ може бити. Користићемо просте $p$ да извучемо информације о $n \pmod{N_p}$. Означимо

$$W_p = \{m \in \mathbb{Z}/N_p\mathbb{Z} \mid m \cdot D \in i(C(\mathbb{F}_p)\}.$$

Желимо да одредимо $C(\mathbb{Q})$, дакле то не знамо. Јакобијан $J(\mathbb{Q})$ потпуно знамо. Када одаберемо прост број $p$, тада можемо да одредимо $C(\mathbb{F}_p)$ (или компјутерски програм). Исто је и за $J(\mathbb{F}_p)$, као и за сабирање у $J(\mathbb{F}_p)$, одакле можемо да одредимо и $W_p$. За конкретно $Q$, комутативни дијаграм изгледа овако

$$\begin{array}{ccccc} Q & \xrightarrow{i} & nD & \xleftarrow[\eta]{} & n \\ \downarrow{\scriptstyle red} & & \downarrow{\scriptstyle red} & & \downarrow{\scriptstyle red} \\ \overline{Q} & \xrightarrow{i} & n\overline{D} & \xleftarrow[\eta]{} & n \pmod{N_p} \end{array}$$

Одавде је $n\overline{D} \in i(C(\mathbb{F}_p)$, тј. $n \pmod{N_p} \in W_p$. Идеја је да узимањем разних $p$, добијамо $N_p$ који нису узајамно прости, јер тада упоређивањем свих могућих остатака, можемо избацити многе класе остатака, а самим тим и смањити избор кандидата за $n$, што нам је и циљ, јер желимо да ограничимо број решења. Наравно, овај рачун ће уместо нас извршавати компјутерски програм. Узимајући у обзир просте бројеве $p \in \{3, 5, 7\}$ добијамо табелу

| $p$ | $N_p$ | $W_p$ |
|---|---|---|
| 3 | 13 | $\{0, 1, 10, 11\}$ |
| 5 | 21 | $\{0, 1, 18, 19\}$ |
| 7 | 65 | $\{0, 1, 13, 19, 27, 36, 44, 50, 62, 63\}$ |

Након излиставања табеле, треба да избацујемо бројеве који дају контрадикцију, на пример, уочимо за $p = 7$ број $19 \in W_7$, тада је $n \equiv 19 \pmod{65}$. Онда је $n \equiv 6 \pmod{13}$, али ово је немогуће, јер из $p = 3$ видимо да остатак $n$ модуло 13 мора бити у скупу $\{0, 1, 10, 11\}$. На сличан начин можемо одбацити још само 44 (mod 65). Број 21 за $p = 5$ нам не даје никакву контрадикцију ни за $p = 3$ ни за $p = 7$. Зато нам треба још простих бројева. У томе је и тајна успеха овог метода, након довољне претраге, одбацићемо велики број могућности и свести задатак на мали број случајева које можемо некако лакше да решимо. Додајући $p = 17$ и $p = 19$, правимо нову табелу, при чему прецртавамо вредности за које знамо да добијамо контрадикцију.

| $p$ | $N_p$ | $W_p$ |
|---|---|---|
| 3 | 13 | $\{0, 1, 10, 11\}$ |
| 5 | 21 | $\{0, 1, 18, 19\}$ |
| 7 | 65 | $\{0, 1, 13, \cancel{19}, 27, 36, \cancel{44}, 50, 62, 63\}$ |
| 17 | 39 | $\{0, 1, 36, 37\}$ |
| 19 | 234 | $\{0, 1, 42, 67, 72, 82, 100, 132, 150, 160, 165, 190, 231, 232\}$ |

Овде смо већ имали више среће, јер $39 \mid 234$, а то ћемо моћи да искористимо да прецртамо велики број вредности. Бројеви из скупа $\{42, 67, 72, 82, 100, 132, 150, 160, 165, 190\}$ не дају остатке из скупа $\{0, 1, 36, 37\}$ модуло 39, па сви ти бројеви воде у контрадикцију. Добијамо нову информацију.

Ако је $Q \in C(\mathbb{Q})$, тада $i(Q) = nD$, за $n \equiv -3, -2, 0, 1 \pmod{234}$. Нека је $n \equiv v \pmod{234}$. Присетимо се

$$i(0, 1) = 0, \quad i(0, -1) = -2D, \quad i(-2, 11) = -3D, \quad , i(-2, -11) = D$$

и означимо са $R$ тачку за коју је $i(R) = vD$. Тада је $n = 234n_0 + v$, за неко $n_0 \in \mathbb{Z}$, па можемо написати

$$[Q - P_0] = i(Q) = nD = (234n_0 + v)D = n_0(234D) + vD = n_0(234D) + [R - P_0].$$

Ако је $Q \in C(\mathbb{Q})$, тада постоји $R \in A$, такво да

$$[Q - R] \in \mathbb{Z} \cdot (234D).$$

На овом месту ћемо искористити помоћ из $p$-адских филтрација, тачније, повероваћемо у једно тврђење које каже да $234D \equiv 0 \pmod{3^3}$, а одатле да мора бити $Q \equiv R \pmod{3^3}$. Ово онда завршава доказ, јер одавде следи да

$$Q \in B_{27}(0,1) \cup B_{27}(0,-1) \cup B_{27}(-2,11) \cup B_{27}(-2,-11) \subset$$

$$\subset B_9(0,1) \cup B_9(0,-1) \cup B_3(-2,11) \cup B_3(-2,-11),$$

што управо значи да $Q \in A$. Након свега овога, коначно смо доказали да је

$$C(\mathbb{Q}) = \{(0,1),(0,-1),(-2,11),(-2,-11)\}.$$

Ова једначина се може наћи у [45].

## 7.6 Преглед једначина које се могу решити Шаботи-Колемановим методом и његовим модификацијама

Постоји много начина да се искористи Шаботи-Колеманов метод у решавању Диофантових једначина. Иако због те разноврсности није било времена да се у овом раду прикаже још више једначина, то није разлог да се оне не наведу, са упутством за литературу, одакле се сви заинтересовани могу боље информисати о даљим идејама и могућностима у овој области.

Кренимо од једначине коју је још давно поставио Диофант у својој чувеној „Аритметици". То је задатак број 17 у шестој књизи. Одредити рационалана решења једначине

$$y^2 = x^8 + x^4 + x^2.$$

Избацујући тачку $(0,0)$ са криве дефинисане овом једначином (која је и сингуларна!), добијамо нову једначину (тј. криву)

$$C : y^2 = x^6 + x^2 + 1,$$

коју је у својој доктроској тези решио математичар Ветерел. Шаботи-Колеманов метод се не може директно применити, а он је уз модификације и придруживање овој једначини две елиптичке криве,

$$y^2 = x^3 + x + 1, \qquad y^2 = x^3 + x^2 + 1$$

доказао да постоји тачно 8 рационалних решења ове једначине и то су

$$C(\mathbb{Q}) = \{(0, \pm 1), (\pm\frac{1}{2}, \pm\frac{9}{8}), \infty_{\pm}\}.$$

Поступак решавања ове једначине се налази у [62].

Прелазимо на једначине мало другачијег облика

$$x^p + y^q = z^r,$$

на даље ће се тражити *примитивна решења* по $(x, y, z)$, тј. решења таква да су $x$, $y$ и $z$ узајамно прости. Ово је прилика да се уверимо да се Шаботи-Колеманов метод може применити и на једначине другачијег облика од $y^2 = f(x)$. Ипак, мора се признати да се једначине првог облика углавном своде на једначине другог облика, где се онда примењује Шаботи-Колеманов метод, врло често у сарадњи са још неким методом.

Крећемо од заједничких резултата Самира Сиксека и Михаела Штола. Први од резултата је налажење примитивних решења једначине

$$x^2 + y^3 = z^{15}.$$

Једначина се решава тако што се креће од једначине

$$x^2 = y^3 + z^3.$$

Примитивна решења ове једначине је могуће параметризовати, тј. постоје узајамно прости цели бројеви $s$ и $t$ такви да је испуњена једна од следећих могућности (при чему $y$ и $z$ могу да замене места, ако је потребно)

$$x = \pm(s^2 - 2st + t^2)(s^4 + 2s^3t + 6s^2t^2 - 4st^3 + 4t^4),$$

$$y = s(s + 2t)(s^2 - 2st + 4t^2),$$
$$z = -4t(s - t)(s^2 + st + t^2),$$

при чему $2 \nmid s$ и $3 \nmid s - t$,

$$x = 3(s - t)(s + t)(s^4 + 2st^3 + 6s^2t^2 + 2st^3 + t^4),$$

$$y = s^4 - 4s^3t - 6s^2t^2 - 4st^3 + t^4,$$
$$z = 2(s^4 + 2s^3t + 2st^3 + t^4),$$

при чему $2 \nmid s - t$ и $3 \nmid s - t$,

$$x = 6st(3s^4 + t^4),$$

$$y = -3s^4 + 6s^2t^2 + t^4,$$
$$z = 3s^4 + 6s^2t^2 - t^4,$$

при чему $2 \nmid s - t$ и $3 \nmid t$.

Доказ овог тврђења се може наћи у [32]. Сада се решавање једначине своди на решавање 6 једначина

$$u^5 = f(s, t),$$

при чему је $f(s, t)$ један од ових 6 полинома помоћу којих се изражавају $y$ и $z$, а на те појединачне случајеве се може применити Шаботи-Колеманов метод, тако да се као крајњи резултат добија да су сва примитвна решења почетне једначине тривијална решења $(\pm 1, -1, 0)$, $(\pm 1, 0, 1)$, $(0, 1, 1)$, $(0, -1, -1)$ и једно нетривијално решење $(\pm 3, 2, 1)$. Ова једначина је решена у [50].

Исти аутори имају још неколико заједничких запажених резултата. На пример, решавајући једначину

$$x^3 + y^4 + z^5 = 0,$$

која има само тривијална решења, они у свом раду [49] показују колико је математике потребно за решавање ове једначине, а Шаботи-Колеманов метод користе у једном од случајева који испитују. Слично као и у претходној једначини, прво посматрају једначину облика

$$a^2 + b^3 + c^5 = 0,$$

одакле добијају чак 49 различитих случајева, а даље испитују када ће то решење што се добије за $a$ бити потпун квадрат.

Листу завршавамо једним занимљивим резултатом, који каже да једина аритметичка прогресија узајамно простих бројева облика

$$(a^2, b^2, c^2, d^5)$$

јесте само она коју чине све јединице, а доказ ове чињенице се може наћи у [48].

У изузетно богатом раду [39], изложено је решавање једначине

$$x^2 + y^3 = z^7$$

која има занимљиво велики број примитивних целобројних решења, чак 16, а то су

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1) \quad (\pm 3, -2, 1) \quad (\pm 71, -17, 2)$$

$$(\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113), \quad (\pm 21063928, -76271, 17).$$

У раду [46], који се бави проценама како би се Шаботијева теорема пренела у бројна поља је доказано да једначина

$$x^2 + y^3 = z^{10}$$

има следећа притивна целобројна решења

$$(\pm 3, -2, \pm 1), \quad (\pm 1, 0, \pm 1), \quad (\pm 1, -1, 0), \quad (0, 1, \pm 1).$$

Једначина облика

$$x^5 + y^5 = z^p,$$

где је $p$ прост број је решена за $7 \leq p \leq 19$ безусловно, а за $23 \leq p \leq 53$ претпостављући тачност *уопштене Риманове хипотезе*. У наведеним случајевима једначина има само тривијална примитивна целобројна решења, тј. решења код којих је $xyz = 0$, а доказ овог тврђења се налази у [54].

Овде је занимљиво напоменути да једначина са слично-обрнутим степенима

$$x^{2p} + y^{2p} = z^5$$

се решава на потпуно другачији начин, модуларним методама, тако да је ово још један пример да се уверимо у лепоту и разноврсност математике коју нам пружају Диофантове једначине!

Још наводимо резултате математичара Бруина, који користи разне модификације Шаботијевог метода у решавању једначина.

У раду [11] доказује да су сва примитивна целобројна решења једначине

$$x^3 + y^9 = z^2$$

су у скупу

$$(x, y, z) \in \{(1, 1, 0), (0, 1, \pm 1), (1, 0 \pm 1), (2, 1, \pm 3), (-7, 2, \pm 13)\}.$$

Процес решавања је до сада већ познат, у [32] постоји параметризација примитивних целобројним решења једначине

$$a^3 + b^3 = c^2,$$

при чему се $a$ и $b$ изражавају са 6 могућих (оба по 3) хомогених полинома по две променљиве $s, t \in \mathbb{Z}[\frac{1}{2}, \frac{1}{3}]$, таквих да не 2 или 3 не деле истовремено $s$ и $t$. Добијају се 6 једначина облика $y^3 = f(s, t)$, од којих је за две потребна модификација Шаботијевог метода, док се преостала четири случаја могу решити без употребе Шаботијевог метода. Пажљивим испитивањем добијају се горе наведена решења.

Сличним методама, у раду [10], налази сва примитивна целобројна решења једначина

$$x^2 \pm y^4 = z^5$$

и за једначину $x^2 + y^4 = z^5$ су то само тривијална решења ($xyz = 0$), док је листа решења занимљивија за другу једначину и то је

$$(x, y, z) \in \{(\pm 1, 0, 1), (0, \pm 1, -1), (\pm 7, \pm 3, -2), (\pm 122, \pm 11, 3)\}.$$

Последњи његов резултат који наводимо се налази у раду [9] у којем решава једначину

$$x^8 + y^3 = z^2,$$

где се поред тривијалних и очигледних решења нашло и једно велико решење

$$(x, y, z) \in \{(\pm 1, 0, \pm 1), (0, 1, \pm 1), (\pm 1, 2, \pm 3), (\pm 43, 96222, \pm 30042907)\}.$$

**Коментар.** Напоменимо за крај да ово нису све једначине које су решене Шаботи-Колемановим методом и његовим модификацијама и да их има још велики број. Циљ је увидети на које још једначине се овај и остали методи могу заједно применити и комбиновати да бисмо решили што већу класу Диофантових једначина.

# 8 Литература


[1] Горан Ђанковић, *Теорија бројева*, Математички факултет, Београд, 2013.

[2] Горан Ђанковић, *Скрипта која се нелинеарно допуњава*, Математички факултет, 2016.

[3] Душан Ђукић, Зоран Каделбург, Владимир Митић, *Увод у теорију бројева*, Друштво математичара Србије, Београд, 2013.

[4] Michael F. Atiyah, Ian G. Macdonald, *Introduction to commutative algebra*, *Addison-Wesley Publishing Company*, 1969.

[5] Alan Baker, *A concise introduction to the theory of numbers*, *Cambridge University Press*, 1984.

[6] Alan Baker, *Transcendental Number Theory*, *Cambridge University Press*, 1990.

[7] Manjul Bhargava, *Most hyperelliptic curves over* $\mathbb{Q}$ *have no rational points*, *arXiv:1308.0395*, 2013.

[8] Enrico Bombieri, Walter Gubler, *Heights in Diophantine Geometry*, *Cambridge University Press*, 2006.

[9] Nils Bruin, *Chabauty methods using covers on curves of genus 2*, *http://www.math.leidenuniv.nl/reports/1999-15.shtml*, 1999.

[10] Nils Bruin, *Chabauty methods using elliptic curves*, *J. reine angew. Math. 562*, 27-49, 2003.

[11] Nils Bruin, *The primitive solutions to* $x^3+y^9 = z^2$, *Journal of Number Theory 111*, 179-189, 2005.

[12] Nils Bruin, Michael Stoll *Deciding Existence of Rational Points on Curves: An Experiment*, *Experiment. Math. 17*, 181-189, 2008.

[13] Nils Bruin, Michael Stoll *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, *LMS J. Comput. Math. 13*, 272-306, 2010.

[14] John William Scott "Ian" Cassels, Victor Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, *Cambridge University Press*, 1996.

[15] Robert F. Coleman, *Effective Chabauty*, *Duke Mathematical Journal, Vol. 52, No. 3*, 765-770, 1985.

[16] Robert F. Coleman, *Torsion Points on Curves and p-Adic Abelian Integrals*, *Annals of Mathematics Vol. 121 No. 1*, 111-168, 1985.

[17] Keith Conrad, *Selmer's example*, *http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy/selmerexample.pdf*

[18] Victor Flynn, *On a Theorem of Coleman*, *Manuscripta mathematica 88*, 447-456, 1995.

[19] Victor Flynn, Bjorn Poonen, Edward Schaefer, *Cycles of quadratic polynomials and rational points on a genus-2 curve* *Duke Mathematical Journal 90*, 435-463, 1997.

[20] William Fulton, *Algebraic curves*, *Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA*, 2008.

[21] Steven D. Galbraith, *Mathematics of Public Key Cryptography*, *Cambridge University Press*, 2012.

[22] Thomas Garrity, Richard Belshoff, Lynette Boos, Ryan Brown, Carl Lienert, David Murphy, Junalyn Navarra-Madsen, Pedro Poitevin, Shawn Robinson, Brian Snyder, Caryn Werner, *Algebraic Geometry: A Problem Solving Approach*, *AMS Student Mathematical Library: Park City Mathematics Subseries* 2008.

[23] Andreas Gathmann, *Algebraic Geometry*, *TU Kaiserslautern*, 2014.

[24] Andreas Gathmann, *Commutative Algebra*, *TU Kaiserslautern*, 2014.

[25] Fernando Gouvêa, *p-adic Numbers*, *Springer*, 1993.

[26] David Grant, *A curve for which Coleman's effective Chabauty bound is sharp*, *Proceedings of the American Mathematical Society Vol. 122, No. 1*, 317-319, 1994.

[27] Robin Hartshorne, *Algebraic Geometry*, *Springer*, 1977.

[28] Marc Hindry, Joseph Silverman, *Diophantine Geometry, An Introduction*, *Springer*, 2000.

[29] Neal Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, *Springer*, 1984.

[30] Qing Liu, *Algebraic Geometry and Arithmetic Curves*, *Oxford University Press*, 2002.

[31] William McCallum, Bjorn Poonen, *The method of Chabauty and Coleman*, *"Explicit methods in Number Theory: Rational Points and Diophantine Equations", eds K. Belabas et al., Panoramas et synthéses 36*, 2012.

[32] Louis J. Mordell, *Diophantine Equations*, *Academic Press INC*, 1969.

[33] David Mumford, *Curves and Their Jacobians*, *The University off Michigan Press*, 1975.

[34] David Mumford, *Tata Lectures on Theta II*, *Birkhäuser Boston*, 1984.

[35] Filip Najman, *Elipticke krivulje nad poljima algebarskih brojeva*, *PMF Zagreb*, 2013.

[36] Jürgen Neukirch, *Algebraic Number Theory*, *Springer*, 1999.

[37] Giulio Di Piazza, *Arithmetic on Jacobians of algebraic curves*, *ALGANT*, Мастер теза, 2013.

[38] Bjorn Poonen, *Computing rational points on curves*, *Number theory for the millennium, III*, 149-172, 2002.

[39] Bjorn Poonen, Edward Schaefer, Michael Stoll, *Twists of $X(7)$ and primitive solutions to $x^2+y^3=z^7$*, Duke Mathematical Journal *137*, 103-158, 2007.

[40] Bjorn Poonen, Michael Stoll, *A local-global principle for densities*, Topics in number theory. In honor of B. Gordon and S. Chowla, 241-244, 1999.

[41] Samuel Porritt, *p-adic Analysis and Rational Points on Curves*, University of Oxford, Мастер теза, 2015.

[42] Miles Reid, *Undergraduate Algebraic Geometry*, University of Warwick, 2013.

[43] Ernst Sejersted Selmer, *The Diophantine equation $ax^3+by^3+cz^3=0$*, Acta Mathematica 85, 203-362, 1951.

[44] Jean-Pierre Serre, *A Course in Arithmetic*, Springer, 1973.

[45] Samir Siksek, *Chabauty and Mordell-Weil Sieve*, http://homepages.warwick.ac.uk/ maseap/papers/ohrid.pdf 2014.

[46] Samir Siksek, *Explicit Chabauty over Number Fields*, Algebra & Number Theory *7*, 765-793, 2013.

[47] Samir Siksek, *The modular approach to Diophantine equations*, http://homepages.warwick.ac.uk/ maseap/sarajevo/notes.pdf, 2016.

[48] Samir Siksek, Michael Stoll, *On a problem of Hajdu and Tengely*, Algorithmic Number Theory, Proceedings of the 9th International Symposium, Nancy, France, 316-330, 2010.

[49] Samir Siksek, Michael Stoll, *Partial descent on hyperelliptic curves and the generalized Fermat equation $x^3+y^4+z^5=0$*, Bulletin of the LMS *44*, 151-166, 2012.

[50] Samir Siksek, Michael Stoll, *The generalized Fermat equation $x^2+y^3=z^{15}$*, Archiv der Mathematik *102*, 411-421, 2014.

[51] Joseph H. Silerman, *The Arithmetic of Elliptic Curves*, Springer, 2008.

[52] Joseph H. Silerman, John Tate, *Rational Points on Elliptic Curves*, *Springer*, 1994.

[53] Michael Stoll, *Arithmetic of Hyperelliptic Curves*, *University of Bayreuth*, 2014.

[54] Michael Stoll, *Chabauty without the Mordell-Weil Group*, arXiv:*1506.04286*, 2015.

[55] Michael Stoll, *How to solve a Diophantine equation*, из књиге *An Invitation to Mathematics*, *Springer*, 2011.

[56] Michael Stoll, *Indenpendence of rational points on twists of a given curve*, *Compositio Math.* 142, 1201-1214, 2006.

[57] Michael Stoll, *p-adic Analysis in Arithmetic Geometry*, *University of Bayreuth*, 2016.

[58] Michael Stoll, *Rational points on curves*, *J. Théor. Nombres Bordeaux 23*, 257-277, 2011.

[59] Michael Stoll, *Rational points on curves*, *http://www.mathe2.uni-bayreuth.de/stoll/papers/Hay-on-Wye-2015.pdf*, 2015.

[60] Michael Stoll, *Rational points on hyperelliptic curves: recent developments*, *Computeralgebra-Rundbrief 54*, 2014.

[61] Michael Stoll, *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank*, *J. Eur. Math. Soc.*, 2015.

[62] Joseph Loebach Wetherell, *Bounding the number of rational points on certain curves of high rank*, *Berkeley*, Докторска теза 1998.