УНИВЕРЗИТЕТ У БЕОГРАДУ

МАТЕМАТИЧКИ ФАКУЛТЕТ

Горица Божић

Хасеов принцип за системе квадратних Диофантових једначина

мастер рад

Београд, 2024

Ментор:

др Горан Ђанковић, ванредни професор
Универзитет у Београду, Математички факултет

Чланови комисије:

др Александар Липовски, редовни професор
Универзитет у Београду, Математички факултет

др Драган Ђокић, доцент
Универзитет у Београду, Математички факултет

Датум одбране: .....

Садржај

Глава 1

1 Увод

Израз Диофантова једначина долази од древног грчког математичара Диофанта из Александрије, који је живео током трећег века нове ере и који је био аутор серије књига названих *Arithmetica.* Многе од тих књига су изгубљене током времена, а преостале су преведене на латински језик током 17. века и постале су извор инспирације за математичаре тог времена. Током последњих 300 година, Диофантове једначине су биле веома важан и врло активан дио чисте математике. Да бисмо укратко објаснили одакле долази фасцинираност Диофантовим једначинама можемо споменути следеће тачке:

- неколико делова модерне математике (као што су: алгебра, теорија бројева, алгебарска геометрија) развијени су у великој мери како би се решиле Диофантове једначине, а тај утицај траје и дан данас;
- Диофантове једначине пружају посебно једноставан начин постављања тешких и занимљивих математичких проблема.

Подсетимо се, *Диофантова једначина* је једначина облика:

$$f(x_1, \dots, x_n) = 0, \tag{1.0.1}$$

где је f полином од n променљивих $x_1, \dots, x_n$, и $n \geq 2$. Ако је f полином са целобројним коефицијентима тада се (1.0.1) назива *алгебарска Диофантова једначина*.

n-торка $({x_1}^0, \dots, {x_n}^0) \in \mathbb{Z}^n$ која задовољава услов (1.0.1) се назива *решењем* једначине (1.0.1). Једначина која има једно или више решења се назива *решивом*.

Када су у питању Диофантове једначине постављају се три основна питања:

1. Да ли је једначина решива?
2. Уколико је једначина решива, да ли има коначно или бесконачно много решења?
3. Ако је решива, која су њена решења.

Решивост Диофантове једначине:

$$aX^2 + bY^2 + cZ^2 = 0 \tag{1.0.2}$$

истраживали су сви велики математичари, од Ојлера до Гауса. Овде претпостављамо да су a, b и c ненула цели бројеви. Ојлер је пронашао потребне услове да би једначина имала нетривијална решења у скупу целих бројева, а то су:

(i) a, b и c нису истог знака и

(ii) $-ab$ је квадратни остатак по модулу $|c|$, $-bc$ је квадратни остатак по модулу $|a|$ и ,$-ca$ је квадратни остатак по модулу $|b|$

Лагранж је проучавао специјалан случај, када је $a = 1$, и доказао да Диофантова једначина (1.0.2) има решење акко су Ојлерови услови задовољени док је млади математичар Гаус у његовој књизи: *Disquisitiones Arithmeticae* доказао да једначина има решење на основу његове теорије о тернарним квадратним формама.

Велики немачки математичар Хилберт је на међународном математичком конгресу у Паризу 1900. године формулисао 23 проблема чије је решавање значајно допринело развоју математичких наука у прошлом веку. Један од тих проблема је такозвани 10. Хилбертов проблем – проблем решивости Диофантових једначина: "За дату Диофантову једначину са било којим бројем непознатих величина и са целобројним кофицијентима измислити поступак којим се може одлучити да ли та једначина има или нема целобројних решења". Јурij В. Матијашевич је 1970. године показао да не постоји алгоритам који би за сваку Диофантову једначину одлучивао да ли она има решења: на тај начин је негативно решен 10. Хилбертов проблем из 1900. године.

Хелмут Хасе је представио своје решење једначине (1.0.2) 1920. године базирано на претходном раду Минковског и било је формулисано на веома елегантан начин користећи и p-адске бројеве које је дефинисао Хенсел неколико деценија раније.

Хасеов локално-глобални принцип, познатији и као Хасеов принцип, је основни идејни принцип у теорији Диофантових једначина. Класично је формулисан и доказан за квадратне форме над $\mathbb{Z}$, са произвољним бројем променљивих: квадратна једначина има нетривијално глобално решење (над $\mathbb{Z}$) акко има нетривијално локално решење над $\mathbb{R}$ и има решење по модулу p^k за сваки прост број p и $k > 1$. Овај принцип даје концептуално разумевање скупа решења Диофантове једначине.

Међутим, већ за кубне једначине, овај принцип више не важи у општем случају. Чувен је Селмеров контрапример $3X^3 + 4Y^3 + 5Z^3 = 0$. Ова кубна једначина има свуда нетривијално локално решење, али нема нетривијално решење над $\mathbb{Q}$. Циљ и задатак овог мастер рада је да се проучи важење Хасеовог принципа за систем квадратних једначина облика

$$aU^2 + bV^2 + cW^2 = dZ^2, \qquad UW = V^2$$

и да се добију контрапримери коришћењем што елементарнијих техника: елементарне теорије бројева и алгебре. Ови контрапримери у модерној терминологији одговарају нетривијалним елементима Тејт-Шафаревичевих група одређених елиптичких кривих.

Искористила бих прилику да се захвалим свом ментору на подршци, сугестијама и помоћи приликом израде овог рада. Такође, желим да се захвалим члановима комисије који су својим сугестијама допринели његовом финалном уобличавању.

Горица Божић

Глава 2

2 Дефиниције, основни појмови и тврђења

Овде се упознајемо са основним појмовима које ћемо користити у даљем раду.

Посматрајмо следећу *Диофантову једначину*:

$$F(X_1, \ldots . X_m) = 0 \tag{2.0.1}$$

где је $F(X_1, \ldots . X_m) \in \mathbb{Z}[X_1, \ldots, X_m]$ хомогени полином степена d. m-торка $(a_1, \ldots . a_m)$ која задовољава услов (2.0.1) назива се *решењем* једначине.

Дефиниција 2.0.1 *m-торка* $(a_1, \ldots . a_m) \in \mathbb{Z}^m$ *се назива тривијалним решењем једначине ако* $\forall i$, $a_i = 0$. *Самим тим, m-торка* $(a_1, \ldots . a_m)$ *се назива нетривијалним решењем једначине ако је бар један од* $a_i \neq 0$.

Дефиниција 2.0.2 *m-торка* $(a_1, \ldots . a_m) \in \mathbb{Z}^m$ *се назива примитивним решењем једначине ако за сваки прост број p постоји* a_i *које није дељиво са p.*

2.1 Конгруенције и квадратни остаци

Дефиниција 2.1.1 *За целе бројеве* a *и* b *који при дељењу са* $m \neq 0$ *дају исте остатке (тј. ако цео број* $m \neq 0$ *дели* $a - b$*) каже се да су конгруентни по модулу* m*. Симболички се то пише* $a \equiv b \pmod m$. *Ако* $m \neq 0$ *не дели* $a - b$ *каже се да* a *није конгруентно* b *по модулу* m *и пише се* $a \not\equiv b \pmod m$.

Ову нотацију је увео Гаус у књизи "Disquisitiones arithmeticae“, која је била објављена 1801.године, када је Гаусу било свега 24 године.

Дефиниција 2.1.2 *Потпун систем остатака по модулу* m $(m \geq 2)$ *је сваки скуп* A *такав да за свако* $y \in \mathbb{Z}$ *постоји тачно један* $x \in A$ *такав да је* $y \equiv x \pmod m$.
Сведен систем остатака по модулу m *је сваки скуп* A *чији су сви елементи узајамно прости са* m*, и такав да, за свако* $y \in \mathbb{Z}$ *које је узајамно просто са* m*, постоји тачно једно* $x \in A$ *такаво да је* $y \equiv x \pmod m$.

Теорема 2.1.3 (Дирихелова теорема) *Нека су* a *и* m *узајамно прости позитивни цели бројеви. Тада постоји бесконачно много простих бројева који су конгруентни* a *по модулу* m*. Другим речима, свака класа остатака по модулу* m *која се састоји од бројева узајамно простих са* m *садржи бесконачно много простих бројева.*

Пропозиција 2.1.4 *Нека су* a, b, c, d *цели бројеви.*

1) *Ако је* $a \equiv b \pmod m$ *и* $c \equiv d \pmod m$*, тада је и* $a + c \equiv b + d \pmod m$, $a - c \equiv b - d \pmod m$, $ac \equiv bd \pmod m$.

2) *Ако је* $a \equiv b \pmod m$ *и* $d \mid m$ *тада* $a \equiv b \pmod d$.
3) *Ако је* $a \equiv b \pmod m$, *тада је* $ac \equiv bc \pmod{mc}$ *за свако* $c \neq 0$.

Доказ: (1) Нека је $a - b = mk$ и $c - d = ml$.
Тада је $(a + c) - (b + d) = m(k + l)$ и $(a - c) - (b - d) = m(k - l)$, па је $a + c \equiv b + d \pmod m$ и $a - c \equiv b - d \pmod m$.
Због $ac - bd = a(c - d) + d(a - b) = m(al + dk)$ следи да је $ac \equiv bd \pmod m$.
(2) Нека је $m = de$. Тада из $a - b = mk$, следи да је $a - b = d \cdot (ek)$, па је $a \equiv b \pmod d$.
(3) Из $a - b = mk$ следи да је $ac - bc = (mc) \cdot k$, па је $ac \equiv bc \pmod{mc}$. □

Пропозиција 2.1.5 *Нека је* f *полином са целобројним коефицијентима. Ако је* $a \equiv b \pmod m$, *онда је и* $f(a) \equiv f(b) \pmod m$.

Доказ: Нека је $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$, где $\forall i = 0, \dots, n,\ c_i \in \mathbb{Z}$. *Из* $a \equiv b \pmod m$, узастопном применом пропозиције 2.1.4 (1), добијамо да је
$a^2 \equiv b^2 \pmod m$, $a^3 \equiv b^3 \pmod m$, … $a^n \equiv b^n \pmod m$. Тада је и $c_i a^i \equiv c_i b^i \pmod m$, па је и $c_n a^n + c_{n-1}a^{n-1} + \cdots + c_0 \equiv c_n b^n + c_{n-1}b^{n-1} + \cdots + c_0 \pmod m$. □

Пропозиција 2.1.6 $ax \equiv ay \pmod m$ *акко* $x \equiv y \pmod{\frac{m}{(a,m)}}$. *Специјално, ако је* $ax \equiv ay \pmod m$ *и* $(a, m) = 1$, *онда је* $x \equiv y \pmod m$. □

Пропозиција 2.1.7 *Нека је* $\{x_1, \dots, x_m\}$ *потпуни систем остатака по модулу* m.
a) Тада је за свако $a \in \mathbb{Z}$ *и* $\{a + x_1, \dots, a + x_m\}$ *потпуни систем остатака по модулу* m.
b) Ако је и $NZD\ (a, m) = 1$. *Тада је и* $\{ax_1, \dots, ax_m\}$ *потпуни систем остатака по модулу* m.□

Пропозиција 2.1.8 *Нека је* $\{x_1, \dots, x_m\}$ *сведен систем остатака по модулу* m *и* $NZD\ (a, m) = 1$.
Тада је и $\{ax_1, \dots, ax_m\}$ *сведен систем остатака по модулу* m. □

Дефиниција 2.1.9 *Ојлерова функција је функција* $\varphi: \mathbb{N} \to \mathbb{N}$ *дефинисана са*
$\varphi(n) = |m \in \{1,2, \dots n\}: (m, n) = 1|$ *(број природних бројева* $\leq n$ *који су узајамно прости са* n*).*

Пример 2.1.10 $\varphi(5) = 4, \varphi(6) = 2,\ \varphi(1) = 1$.

Ојлерова функција је мултипликативна, тј. важи $\varphi(mn) = \varphi(m)\varphi(n)$ ако је $(m, n) = 1$.
Ако је p прост број тада је $\varphi(p) = p - 1$. Додатно, ако је је $n = p_1^{\alpha_1}p_2^{\alpha_2} \dots\ p_k^{\alpha_k}$, за прост број p онда је $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots (1 - \frac{1}{p_k})$.

Пример 2.1.11 $\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = 120\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 32$

Теорема 2.1.12 (Ојлерова теорема) *Ако за природне бројеве* a *и* m *важи да је* $(a, m) = 1$, *тада је* $a^{\varphi(m)} \equiv 1 \pmod m$.

Доказ: Ако је $S = \{r_1, r_2\ \dots, r_{\varphi(m)}\}$ сведен систем остатака по модулу m, и ако важи да је $(a, m) = 1$ тада из Пропозиције 2.1.8 следи да је и $R = \{a \cdot r_1, a \cdot r_2\ \dots, a \cdot r_{\varphi(m)}\}$ такође сведен систем

остатака по модулу m па закључујемо да је $\prod_{j=1}^{\varphi(m)}(ar_j) \equiv \prod_{i=1}^{\varphi(m)} r_i \ (mod\ m)$, односно $a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{i=1}^{\varphi(m)} r_i \ (mod\ m)$. Како је $(r_i, m) = 1$, применом Пропозиције 2.1.6 добијамо $a^{\varphi(m)} \equiv 1 \ (mod\ m)$. □

Теорема 2.1.13 (мала Фермаова теорема) *Ако за природан број a и прост број p важи $p \nmid a$, тада је $a^{p-1} \equiv 1 \ (mod\ p)$.* □

Мала Фермаова теорема налази практичну примену у рачунарству: за потребе кодирања потребно је одредити велике просте бројеве (класични начин за установљавање сложености неког броја n је Ератостеново сито, односно потребно је испитати да ли је дељив са неким простим бројем мањим или једнаким од $\sqrt{n}$, али тај поступак тражи веома много времена) и тада ако нам неки "псеудопрост" број да резултат мале Фермаове теореме за неколико (што више то боље - већа је вероватноћа да је тај број заиста прост) различитих вредности a онда га можемо сматрати као прост за генерисање неког кода.[2]
Међутим, ово није потпуно тачно јер постоје на пример *Кармајклови бројеви* који нису сви прости а пролазе овакав тест.
Пјер де Ферма није дао доказ ове теореме, први који је то учинио био је немачки математичар Готфрид Лајбниц, у рукопису без датума, али је сам Лајбниц написао поред да је знао доказ пре 1683. године.

Теорема 2.1.14 (Лагранжова теорема) *Нека је p прост број и $p \nmid a_n$ и нека је $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ дати полином са целобројним коефицијентима. Тада конгруенција $f(x) \equiv 0 \ (mod\ p)$ има највише n решења по модулу p.* □

Последица 2.1.15 *Нека је p прост број и нека је $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ дати полином са целобројним коефицијентима. Ако конгруенција $f(x) \equiv 0 \ (mod\ p)$ има више од n решења по модулу p, онда је сваки коефицијент полинома $f(x)$ дељив са p.* □

Вилсонова теорема је једна од познатих теорема у теорији бројева. Ову теорему је открио арапски математичар Иб ал Хајтам (*Ibn al-Haitam*) још у 10. веку, док ју је Едвард Варинг објавио у 18. веку без доказа, приписујући откриће свом ученику Џону Вилсону. Лагранж је 1771. године први доказао ову теорему.

Теорема 2.1.16 (Вилсонова теорема) *Ако је p прост број, тада је*

$$(p - 1)! \equiv -1 \ (mod\ p)$$

Доказ: За $p = 2$ и $p = 3$ конгруенција очигледно важи. Претпоставимо да је $p \geq 5$. Групишимо чланове скупа $\{2, 3, \dots, p-2\}$ у парове (i, j) са својством $i \cdot j \equiv 1 \ (mod\ p)$. Очигледно је $i \neq j$ јер би иначе број $(i-1)(i+1)$ био дељив са p а то је немогуће због $0 < i - 1 < i + 1 < p$. На тај начин добијамо $\frac{p-3}{2}$ парова и ако помножимо одговарајућих $\frac{p-3}{2}$ конгруенција, добијамо $2 \cdot 3 \cdot \dots \cdot (p-2) \equiv 1 \ (mod\ p)$, па је $(p - 1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \ (mod\ p)$. □

Систем од две или више конгруенција не мора да има решења, премда свака појединачна конгруенција има решења. Рецимо не постоји x које истовремено задовољава $x \equiv 1 \ (mod\ 2)$ и

$x \equiv 0\ (mod\ 4)$, мада свака од појединачних конгруенција има решења. Разлог томе је што модули конгруенција 2 и 4 нису узајамно прости. Следећа теорема, позната у литератури као *Кинеска теорема о остацима* даје услове под којима више линеарних конгруенција има заједничко решење ако су модули конгруенција узајамно прости у паровима. Мада је прво опште решење за проблеме овог типа дао Ојлер, следећа теорема се назива кинеском јер је кинески математичар Сун-Цу (*Sun Tzu*, познатији и као *Sun Zi*) у трећем веку решио задатак који се своди на налажење целих бројева x који при дељењу са 3, 5 и 7 дају редом остатке 2, 3 и 2.[2]

Теорема 2.1.17 (Кинеска теорема о остацима) *Нека су $m_1, m_2, \dots, m_r$ природни бројеви који задовољавају $(m_i, m_j) = 1$ за $i \neq j$, и нека су $b_1, b_2, \dots, b_r$ произвољни цели бројеви. Тада систем конгруенција*

$$\begin{cases} x \equiv b_1\ (mod\ m_1) \\ x \equiv b_2\ (mod\ m_2) \\ \dots \\ x \equiv b_r\ (mod\ m_r) \end{cases}$$

има тачно једно решење x_0 по модулу $m = m_1 \cdot m_2 \cdot \ \dots \cdot m_r$.

Доказ: Нека је $m = m_1 m_2 \cdot \ \dots \ m_r$, те нека је $n_i = \frac{m}{m_i}$ за $i = 1,2, \dots r$. Тада је $NZD(n_i, m_i) = 1$, па постоји цео број x_i такав да је $n_i x_i \equiv b_i\ (mod\ m_i)$. Посматрајмо сада број $x_0 = n_1 x_1 + \dots + \ n_r x_r$. Видимо да важи $x_0 \equiv 0 + \dots + 0 + n_i x_i + 0 + \dots + 0 \equiv b_i\ (mod\ m_i)$ па је x_0 решење система. Ако су x и y решења система, тада је $x \equiv y\ (mod\ m_i)$ за $i = 1,2, \dots r$ јер су m_i у паровима узајамно прости, па је самим тим и $x \equiv y\ (mod\ m)$. □

Важи и следеће уопштење Теореме 2.1.17.

Теорема 2.1.18 *Нека су $m_1, m_2, \dots, m_r$ природни бројеви који су узајамно прости у паровима ($(m_i, m_j) = 1$ за $i \neq j$) и нека су $a_1, a_2, \dots, a_r$ и $b_1, b_2, \dots, b_r$ цели бројеви, такви да $(a_i, m_i) = 1$, $i = 1, .. r$. Тада систем конгруенција*

$$\begin{cases} a_1 x \equiv b_1\ (mod\ m_1) \\ a_2 x \equiv b_2\ (mod\ m_2) \\ \dots \\ a_r x \equiv b_r\ (mod\ m_r) \end{cases}$$

има тачно једно решење x_0 по модулу $m = m_1 \cdot m_2 \cdot \ \dots \cdot m_r$. □

Сада ћемо навести неколико основних дефиниција и тврђења за квадратне остатке.

Дефиниција 2.1.19 *Нека је $(a, m) = 1$. Ако конгруенција $x^2 \equiv a\ (mod\ m)$ има решења, онда кажемо да је a квадратни остатак по модулу m.*

Дефиниција 2.1.20 (Лежандров симбол) *Нека је p непаран прост број. Лежандров симбол $\left(\frac{a}{p}\right)$ је по дефиницији:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ако је } a \text{ квадратни остатак по модулу } p, \\ 0 & \text{ако је } a \text{ дељиво са } p, \\ -1 & \text{ако } a \text{ није квадратни остатак по модулу } p. \end{cases}$$

Пример 2.1.21. Пошто је 2 квадратни остатак по модулу 7 ($3^2 \equiv 2$), а 3 то није, имамо $\left(\frac{2}{7}\right) = 1$ и $\left(\frac{3}{7}\right) = -1$.

На основу Фермаове теореме важи $a^{p-1} \equiv 1 \ (mod\ p)$, одакле следи и $a^{\frac{p-1}{2}} \equiv \pm 1 \ (mod\ p)$. Прецизније, важи следеће тврђење.

Теорема 2.1.22 (Ојлеров критеријум) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (mod\ p)$.

Доказ: Ако је $\left(\frac{a}{p}\right) = 0$, онда p дели a, па је тврђење очигледно тачно.

Ако је $\left(\frac{a}{p}\right) = 1$, онда постоји $x_0 \in \mathbb{Z}$, такво да је ${x_0}^2 \equiv a \ (mod\ p)$, па из Мале Фермаове теореме следи да је $a^{\frac{p-1}{2}} \equiv {x_0}^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) (mod\ p)$.

Нека је сада $\left(\frac{a}{p}\right) = -1$. За сваки $i \in \{1, \dots p-1\}$ одаберимо $j \in \{1, \dots p-1\}$ такво да је $i \cdot j \equiv a \ (mod\ p)$ (ово важи на основу Порпозиције 2.1.7 (b)). Како конгруенција $x^2 \equiv a \ (mod\ p)$ нема решења, следи да је $i \neq j$. Дакле, скуп $\{1, \dots p-1\}$ се може поделити на $\frac{p-1}{2}$ парова (i, j) за које важи $i \cdot j \equiv a \ (mod\ p)$. Множењем ових $\frac{p-1}{2}$ конгруенција, те користећи Вилсонову теорему добијамо $a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \ (mod\ p)$. □

Основна својства Лежандровог симбола резимирана су у следећој теореми.

Теорема 2.1.23 *Нека је p непаран прост број, и нека су a и b цели бројеви*

(i) *Ако је $a \equiv b \ (mod\ p)$, тада је $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ *(Лежандров симбол је мултипликативан)*

Доказ: (i) Ако је $a \equiv b \ (mod\ p)$, тада је $a^{(p-1)/2} \equiv b^{(p-1)/2} \ (mod\ p)$, одакле је $(a/p) \equiv (b/p) \ (mod\ p)$. Другим речима, $p \mid (a/p) - (b/p)$. Међутим, приметимо да важи $|(a/p) - (b/p)| \leq 2$, па из $p > 2$ следи да је $(a/p) = (b/p)$.
(ii) Лева и десна страна једнакости коју доказујемо су конгруентне по модулу p, будући да су, по дефиницији Лежандровог симбола, обе конгруентне са $(ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2}$. Сада закључак о једнакости следи исто као и у претходној тачки. □

Теорема 2.1.24 (Гаусов квадратни закон реципроцитета) *Нека су p и q различити непарни прости бројеви. Тада важи:* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. *Другим речима, ако су p и q оба облика $4k+3$ онда једна од конруенција $x^2 \equiv p \ (mod\ q)$, $x^2 \equiv q \ (mod\ p)$ има решења, а друга нема. Ако барем*

један од бројева p и q има облик $4k+1$, онда или обе конгруенције имају решења или обе немају решења. □

2.2 Апсолутне вредности на пољима p-адских бројева

Дефиниција 2.2.1 *Апсолутна вредност на пољу K је пресликавање:* $|\cdot|: K \to \mathbb{R}_{\geq 0}$, *са следећим својствима:*

(i) $|x| = 0$ *акко* $x = 0$;
(ii) $|xy| = |x| \cdot |y|$ *за све* $x, y \in K$;
(iii) $|x + y| \leq |x| + |y|$ *за све* $x, y \in K$.

Ако апосолутна вредност додатно задовољава и ултра-метричку неједнакост:

$$|x + y| \leq \max\{|x|, |y|\}$$

тада се та апсолутна вредност назива неархимедска апсолутна вредност, док све оне које ову неједнакост не задовољавају називамо *архимедска* апсолутна вредност.

Основна теорема артиметике јесте тврђење да се сваки природан број већи од 1 може приказати као производ (позитивних) простих бројева, и при томе је та факторизација јединствена до на поредак фактора, тј. за $x \in \mathbb{N}$, $x > 1$ важи следеће: $x = u\prod_p p^{n_p} = u2^{n_2}3^{n_3}5^{n_5}$ ... где $u \in \{-1,1\}$ и $n_p \in \mathbb{Z}$ за сваки прост број p, и $n_p = 0$ за скоро свако p.

Дефиниција 2.2.2 *Нека је p прост број. p-адска валуација је функција:*

$$v_p: \mathbb{Q}^x \to \mathbb{Z}$$

$$x \mapsto v_p(x) \coloneqq n_p$$

која нам даје степен броја p у факторизацији ненула рационалног броја x. Ако је $x = 0$, тада дефинишемо да је $v_p(0) := +\infty$.

p-адску валуацију можемо дефинисати и на следећи начин: ако је x ненула рационални број, тада x можемо записати као: $p^n\frac{r}{s}$, где су r и s цели бројеви који нису дељиви са p, и $n \in \mathbb{Z}$. Тада је $v_p(x) \coloneqq n$.

Пример 2.2.3 $v_2(5/24) = -3$, јер је $\frac{5}{24} = 2^{-3}\frac{5}{3} = 2^{-3}3^{-1}5^1$.

Лема 2.2.4 *За свако $x, y \in \mathbb{Q}$, p-адска валуација задовољава следеће:*

(i) $v_p(x) = +\infty$ *акко* $x = 0$;
(ii) $v_p(xy) = v_p(x) + v_p(y)$;
(iii) $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$.

Доказ: Услов (ii) нам заправо говори да је v_p хомоморфизам: $\mathbb{Q}^x \to \mathbb{Z}$.
Како бисмо доказали да важи услов (iii) претпоставимо да је $x + y \neq 0$ и $x, y \neq 0$ (случај када је $x = 0$ или $y = 0$ или $x + y = 0$ је тривијалан).
Нека је $x = p^n \frac{r}{s}$ и $y = p^m \frac{u}{v}$ где r, s, u, v нису дељиви са p, па је $v_p(x) = n$ и $v_p(y) = m$. Без умањења општости претпоставимо да је $n \leq m$. Тада је $x + y = p^n \left(\frac{r}{s} + \frac{p^{m-n}u}{v}\right) = p^n \frac{N}{sv}$ где sv није дељиво са p, али N може бити дељиво са p па је $v_p(x + y) \geq n = \min\{n, m\} = \min\{v_p(x), v_p(y)\}$.□

Дефиниција 2.2.5 *Нека је p прост број. p-адска апсолутна вредност рационалног броја x је дефинисана са $|x|_p := p^{-v_p(x)}$. За $x = 0$ дефинишемо да је $|0|_p := 0$.*

Пропозиција 2.2.6 *p-адска апсолутна вредност је неархимедска апсолутна вредност на пољу $\mathbb{Q}$.*

Доказ: Нека су $x, y \in \mathbb{Q}$. Претпоставимо да је $x = 0$. Тада је $|0|_p = 0$.
Претпоставимо сада да је $x \neq 0$.
Тада је $|x|_p = p^{-v_p(x)}$. Како је $p \neq 0$, $|x|_p \neq 0$, па следи да p-адска апослутна вредност задовољава услов (i) (Дефиниција 2.2.1).
Проверавамо сада услов (ii). (Дефиниција 2.2.1)
Уколико је $x = 0$ или $y = 0$, тада је $|xy|_p = |x|_p |y|_p$.
Посматрајмо сада случај када је $x \neq 0$ и $y \neq 0$. Тада је
$|xy|_p = p^{-v_p(xy)}$, и $|x|_p |y|_p = p^{-v_p(x)} p^{-v_p(y)} = p^{-v_p(x)-v_p(y)}$. На основу Леме 2.2.4 (ii)
$-v_p(xy) = -v_p(x) - v_p(y)$, па је $|xy|_p = |x|_p |y|_p$, и p-адска апослутна вредност задовољава услов (ii). (Дефиниција 2.2.1)
Проверавамо сада услов (iii) и ултра-метричку неједнакост.
Уколико је $x + y = 0$, $|x + y|_p = 0$. Тада је $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.
Посматрајмо сада случај када је $x + y \neq 0$.
Без умањења општости претпоставимо да је $|x|_p \geq |y|_p$. Тада је $|x|_p \neq 0$, па је $x \neq 0$, па следи да је $v_p(x) \leq v_p(y)$. Из дефиниције p-адске апсолутне вредности следи да је $|x + y|_p = p^{-v_p(x+y)}$ и $|x|_p = p^{-v_p(x)}$. На основу Леме 2.2.4 (iii) следи да је $v_p(x + y) \geq \min\{v_p(x), v_p(y)\} = v_p(x)$, па следи да је $p^{-v_p(x+y)} \leq p^{-v_p(x)}$. Еквивалентно, $|x + y|_p \leq |x|_p = \max\{|x|_p, |y|_p\}$, па следи да p-адска апослутна вредност задовољава ултра-метричку неједнакост, па самим тим задовољава и услов (iii). (Дефиниција 2.2.1). □

Дефиниција 2.2.7 *За две апсолутне вредности $|\cdot|$ и $|\cdot|'$ на пољу K кажемо да су еквивалентне ако постоји $\alpha \in \mathbb{R}_{>0}$ такво да важи: $|x|' = |x|^\alpha$, за свако $x \in K$.*

Дефиниција 2.2.8 (**Островски**) *Све нетривијалне апсолутне вредности на $\mathbb{Q}$ су еквивалетне једној од $|\cdot|_\infty$ или $|\cdot|_p$ где је p неки прост број.*

Доказ ове теореме се може пронаћи у [7].

2.3 Комплетирање поља, и прстен целих p-адских бројева

Нека је K поље са апсолутном вредношћу $|\cdot|$.

Дефиниција 2.3.1 *Низ* $(a_i) \in K$ *је конвергентан ако постоји коначан број* $l \in K$ *и ако за* $\forall \varepsilon > 0$ *постоји* $N(\varepsilon) \in \mathbb{N}$ *тако да је* $|a_i - l| < \varepsilon$ *за* $\forall i \geq N(\varepsilon)$. *Број* l *је гранична вредност (граница, лимес) низа* (a_i).

Дефиниција 2.3.2 *Низ* $(a_i) \in K$ *је Кошијев ако* $\forall \varepsilon > 0$ *постоји* $N(\varepsilon) \in \mathbb{N}$ *тако да је* $|a_i - a_j| < \varepsilon$ *за* $\forall i, j \geq N(\varepsilon)$.

Дефиниција 2.3.3 *Поље K је комплетно у односу на* $|\cdot|$ *ако сваки Кошијев низ конвергира.*

Дефиниција 2.3.4 *Поље које је настало комплетирањем поља* $\mathbb{Q}$ *у односу на* p*-адску апослутну вредност* $|\cdot|_p$ *називамо поље* p*-адских бројева, и означавамо га са* $\mathbb{Q}_p$.*Специјално, поље* $\infty -$*адских бројева је добро познато поље реалних бројева* $\mathbb{R}$.

На основу теореме Островског знамо да су реални бројеви и p-адски бројеви једина комплетирања рационалних бројева. Егзистенција и јединственост поља $\mathbb{Q}_p$ следи из наредне теореме.

Теорема 2.3.5 *Нека је K поље са апсолутном вредношћу* $|\cdot|$. *Тада постоји јединствено, до на изоморфизам, комплетно поље* K' *са апсолутном вредношћу* $|\cdot|'$ *такво да се поље K изометрично утапа у у поље* K', *и слика поља K при том утапању је густа у* K'. *При том је апсолутна вредност* $|\cdot|'$ *неархимедска акко је то и* $|\cdot|$. □

Доказ ове теореме се може пронаћи у [5].

Дефиниција 2.3.6 *Елементе затвореног диска* $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ *у пољу* $(\mathbb{Q}_p, |\cdot|_p)$ *називамо целим* p*-адским бројевима.*

Дефиниција 2.3.7 *Прстен* $(\mathbb{Z}_p, +, \cdot)$ *називамо прстеном целих* p*-адских бројева.*

Приметимо да је за свако $x \in \mathbb{Z}, v_p(x) \geq 0$, па је $|x|_p \leq 1$, па је $\mathbb{Z} \subset \mathbb{Z}_p$.

Лема 2.3.8 *Нека су* $a, b \in \mathbb{Q}_p$. *Ако је* $|a|_p > |b|_p$ *онда је и* $|a + b|_p = |a|_p$.

Доказ: Из особине p-адске асполутне вредности ($|a + b|_p \leq \max\{|a|_p, |b|_p\}$ и претпоставке леме следи да је $|a + b|_p \leq |a|_p$. Имамо $|a|_p = |(a + b) - b|_p \leq \max\{|a + b|_p, |b|_p\}$. Како је $|a|_p > |b|_p$ следи да је $|a|_p \leq |a + b|_p$, па тврђење следи. □

Лема 2.3.9 *Нека су* $a_1, \dots a_n \in \mathbb{Q}_p$. *Тада важи следеће:* $|a_1 + \cdots + a_n|_p \leq max\{|a_1|_p, \dots |a_n|_p\}$.

Доказ: доказ изводимо индукцијом по n.
Нека је $n = 2$ и нека $a_1, a_2 \in \mathbb{Q}_p$. По претходној леми имамо да је $|a_1 + a_2|_p = |a_1|_p$ ако је $|a_1|_p > |a_2|_p$, односно $|a_1 + a_2|_p = |a_2|_p$ ако је $|a_2|_p > |a_1|_p$. Дакле, вреди да је $|a_1 + a_2|_p \leq \max\{|a_1|_p, |a_2|_p\}$.

Претпоставимо сада да је тврђење тачно за неко $k \in \mathbb{N}$, тј. да је$|a_1 + \cdots + a_k|_p \leq \max\{|a_1|_p, \ldots |a_k|_p\}$.
Доказујемо да је тврђење тачно за $k+1 \in \mathbb{N}$, тј. да важи да је $|a_1 + \cdots + a_k + a_{k+1}|_p \leq \max\{|a_1|_p, \ldots |a_k|_p, |a_{k+1}|_p\}$.

$$|a_1 + \cdots + a_k + a_{k+1}|_p \leq |a_1 + \cdots + a_k|_p + |a_{k+1}|_p$$

(из особине p-адске асполутне вредности)

$$\leq \max\{|a_1|_p, |a_2|_p, \ldots |a_k|_p\} + |a_{k+1}|_p$$

(из претпоставке индукције)

$$\leq \max\{|a_1|_p, |a_2|_p, \ldots |a_k|_p, |a_{k+1}|_p\}$$

(по претходној леми имамо да је $|a_1 + \cdots + a_k + a_{k+1}|_p \leq \max\{|a_1|_p, |a_2|_p, \ldots |a_k|_p\}$ ако је $|a_{k+1}|_p \leq \max\{|a_1|_p, |a_2|_p, \ldots |a_k|_p\}$, а ако је $|a_{k+1}|_p \geq \max\{|a_1|_p, |a_2|_p, \ldots |a_k|_p\}$ онда је $|a_1 + \cdots + a_k + a_{k+1}|_p = |a_{k+1}|_p$. Дакле вреди да је $|a_1 + \cdots + a_k + a_{k+1}|_p \leq \max\{|a_1|_p, |a_2|_p, \ldots |a_k|_p, |a_{k+1}|_p\}$.
Овим је доказ завршен □

Пропозиција 2.3.10 *Елемент $\alpha \in \mathbb{Z}_p$ је јединица акко α није дељиво са p. Другим речима, група p-адских јединица $\mathbb{Z}_p{}^x \cong \mathbb{Z}_p/p\mathbb{Z}_p$.*

Доказ: Ако $\{a_n\} \to \alpha \in \mathbb{Z}_p$ дељив са p, тада је $a_1 = 0$, па α очигледно не може бити инвертибилан. Ако α није дељив са p тада $a_1 \neq 0$, па следи да је $a_n \equiv a_{n-1} \equiv \cdots \equiv a_0 \ (mod\ p)$, тако да $a_n \not\equiv 0 \ (mod\ p)$. Сада за било које n можемо наћи b_n такво да $a_n b_n \equiv 1 (mod\ p^n)$.
Како $a_n \equiv a_{n-1} \ (mod\ p^n)$ и $a_n b_n \equiv a_{n-1} b_{n-1} \ (mod\ p^n)$ тада је такође $b_n \equiv b_{n-1} \ (mod\ p^n)$ па вреди да $\{b_n\} \to \beta \in \mathbb{Z}_p$. Стога, $\alpha\beta = 1$, тј. β је инверз од α па је α јединица. С обзиром да је множење комутативно видимо да је и α инверз од β па је и β p-адска јединица. □

Пропозиција 2.3.11 *Сваки ненула елемент $\alpha \in \mathbb{Z}_p$ може се на јединствен начин записати као $p^n u$, где је $u \in \mathbb{Z}_p{}^x$ и $n \in \mathbb{Z}_{\geq 0}$.*

Доказ: Ако је α јединица тада за $n = 0$ пропозиција вреди. Нека је $\{a_n\} \to \alpha \neq 0$ где α није јединица па према Пропозицији 2.3.10 α је дељиво са p и постоји бар једно n такво да је $a_n = 0$ ($a_1 = 0$). Због $\alpha \neq 0$ можемо пронаћи највећи број n за који је $a_n = 0$. За тај n вреди да $\alpha \equiv 0 \ (mod\ p^n)$ па постоји $u \in \mathbb{Z}_p$ такав да је $\alpha = p^n u$. Докажимо још да је u јединица. У случају да u није јединица, тада је по Пропозицији 2.3.10, u је дељиво са p, па је $\alpha = p^{n+1}$ из чега следи да је $a_{n+1} = 0$ што је у контрадикцији са претпоставком да је n највећи индекс за који је $a_n = 0$.
Докажимо сада и јединственост. Претпоставимо $p^n u_1 = p^m u_2$. Ако је $m = n$, тада због инјективности множења следи да је $u_1 = u_2$. У супротном, без умањења општости можемо претпоставити да је $m < n$. Тада је $u_2 = p^{n-m} u_1$, па према Пропозицији 2.3.10, u_2 није јединица што је у контрадикцији са претпоставком пропозиције.

Дефиниција 2.3.12 *Поље p -адских бројева $\mathbb{Q}_p$ је поље разломака од $\mathbb{Z}_p$.*

За $a \in \mathbb{Q}_p$ по дефиницији вреди $a = \frac{p^n u_1}{p^m u_2} = p^{n-m} u_1 u_2^{-1}$, па можемо сваки елемент из $\mathbb{Q}_p$ записати као $p^k u$, где је $u \in \mathbb{Z}_p{}^x, k \in \mathbb{Z}$. Сада можемо проширити дефиницију од v_p на $\mathbb{Q}_p$ тако да за $a = p^k u$, где је $u \in \mathbb{Z}_p{}^x, k \in \mathbb{Z}$ вреди $v_p(up^k) = k$, те је као и пре $v_p(0) = +\infty$. Приметимо да је $\mathbb{Z}_p \subset \mathbb{Q}_p$, тј. $\mathbb{Z}_p = \{a \in \mathbb{Q}_p | v_p(a) \geq 0\}$.

Пропозиција 2.3.13 *Поље $\mathbb{Q}_p$ је комплетно у односу на $|\cdot|_p$, тј. сваки Кошијев низ у $\mathbb{Q}_p$ је конвергентан.* □

Глава 3

3 Хенселова лема и Хасеова теорема

3.1 Хенселова лема

Посматрајмо следећу Диофантову једначину:

$$F_1(X_1, \ldots . X_m) = 0 \tag{3.1.1}$$

где је $F_1(X_1, \ldots . X_m) \in \mathbb{Z}[X_1, \ldots, X_m]$ хомогени полином степена d. На основу хомогености ако једначина (3.1.1) има бар једно нетривијално решење (у $\mathbb{Z}^m$, или у $\mathbb{Q}^m$), онда она има и примитивно решење. Проширићемо ову терминологију на два начина: на системе хомогених полиномних једначина и на решења по модулу N. Дакле примитивно решење по модулу N је примитивна m-торка која решава конгруенцију $F_1(X_1, \ldots . X_m) \equiv 0 \ (mod\ N)$.

Најлакши начин да покажемо да једначина (3.1.1) нема нетривијално решење јесте да покажемо да једначина нема нетривијално решење у $\mathbb{R}$. Затим, други најлакши начин да покажемо да једначина (3.1.1) нема нетривијално решење јесте да покажемо да она нема примитивно решење по модулу N за неко N.

Пре него што дефинишемо Хасеову теорему, наводимо и дајемо доказ Хенселове леме коју ћемо користити у даљем раду.

Теорема 3.1.1 (Хенселова лема: верзија 1) *Ако је* $f(X) \in \mathbb{Z}_p[X]$ и $a \in \mathbb{Z}_p$ *такво да је* $f(a) \equiv 0 \ (mod\ p)$ *и* $f'(a) \not\equiv 0 \ (mod\ p)$, *тада постоји јединствено* $\alpha \in \mathbb{Z}_p$ *такво да је* $f(\alpha) = 0$ *у* $\mathbb{Z}_p$ *и* $\alpha \equiv a \ (mod\ p)$.

Доказ: Индукцијом ћемо показати да за свако $n \geq 1$ постоји $a_n \in \mathbb{Z}_p$ такво да:

- $f(a_n) \equiv 0 \ (mod\ p^n)$
- $a_n \equiv a \ (mod\ p)$

Случај $n = 1$ је тривијалан (узмимо $a_1 = a$).
Даље, претпоставимо да је тврђење тачно за n. Тражимо $a_{n+1} \in \mathbb{Z}_p$ такво да:

- $f(a_{n+1}) \equiv 0 \ (mod\ p^{n+1})$
- $a_{n+1} \equiv a \ (mod\ p)$

Из $f(a_{n+1}) \equiv 0 \ (mod\ p^{n+1}) \Rightarrow\ f(a_{n+1}) \equiv 0 \ (mod\ p^n),$ следи да се сваки корен $f(X)$ по модулу p^{n+1} може свести на корен $f(X)$ по модулу p^n. На основу индуктивне хипотезе постоји корен a_n по модулу p^n такав да је $a_n \equiv a \ (mod\ p)$, па тражимо p-адски цели a_{n+1} такав да је $a_{n+1} \equiv a_n \ (mod\ p^n)$ и $f(a_{n+1}) \equiv 0 \ (mod\ p^{n+1})$. Уколико a_{n+1} запишемо на следећи начин:

$$a_{n+1} = a_n + p^n t_n$$

за неко $t_n \in \mathbb{Z}_p$, да ли можемо направити да је $f(a_n + p^n t_n) \equiv 0 \ (mod\ p^{n+1})$?
За израчунавање $f(a_n + p^n t_n)$ по модулу p^{n+1} користићемо следећи полиномски идентитет:

$$f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2 \tag{3.1.2}$$

где полином $g(X,Y) \in \mathbb{Z}_p[X,Y]$. Дакле,ово је практично проширење Тејлорове формуле на $\mathbb{Z}_p$.Записујући $f(X) = \sum_{i=0}^{d} c_i X^i$ добијамо следеће:

$$f(X+Y) = \sum_{i=0}^{d} c_i (X+Y)^i = c_0 + \sum_{i=1}^{d} (c_i (X^i + iX^{i-1}\, Y) + g_i(X,Y)Y^2),$$

где $g_i(X,Y) \in \mathbb{Z}[X,Y]$

Према томе

$$f(X+Y) = \sum_{i=0}^{d} c_i X^i + \sum_{i=1}^{d} i c_i X^{i-1} Y + \sum_{i=1}^{d} g_i(X,Y)Y^2 = f(X) + f'(X)Y + g(X,Y)Y^2$$

где $g(X,Y) = \sum_{i=1}^{d} c_i g_i(X,Y) \in \mathbb{Z}_p[X,Y]$. Ово нам даје жељени идентитет. Сада убацујемо вредности из прстена p-адских целих. За све x и $y \in \mathbb{Z}_p$, како је $z := g(x,y)$ у $\mathbb{Z}_p$, важи следеће: $x, y \in \mathbb{Z}_p \Rightarrow\ f(x+y) = f(x) + f'(x)y + zy^2$ где је $z \in \mathbb{Z}_p$.

Нека је $x = a_n$ и $y = p^n t_n$

$$f(a_n + p^n t_n) = f(a_n) + f'(a_n)p^n t_n + z p^{2n} t_n^2 \equiv f(a_n) + f'(a_n)p^n t_n \ (mod\ p^{n+1})$$

јер је $2n \geq n+1$. Како је $a_n \equiv a \ (mod\ p)$, добијамо $f'(a_n)p^n t_n \equiv f'(a)p^n t_n (mod\ p^{n+1})$, па је због тога $f(a_n + p^n t_n) \equiv 0 \ (mod\ p^{n+1}) \Leftrightarrow f(a_n) + f'(a)p^n t_n \equiv 0 \ (mod\ p^{n+1}) \Leftrightarrow f'(a)t_n \equiv -f(a_n)/p^n \ (mod\ p)$ где је $-f(a_n)/p^n \in \mathbb{Z}_p$ јер смо претпоставили да је $f(a_n) \equiv 0 \ (mod\ p^n)$.
Дакле, постоји решење за t_n у $f'(a)t_n \equiv -f(a_n)/p^n \ (mod\ p)$ конгруенције по модулу p јер смо претпоставили да је $f'(a) \not\equiv 0 \ (mod\ p)$.
Наоружани избором t_n и узимајући да је $a_{n+1} = a_n + p^n t_n$, имамо да је $f(a_{n+1}) \equiv 0 \ (mod\ p^{n+1})$ и $a_{n+1} \equiv a_n \ (mod\ p^n)$, дакле $a_{n+1} \equiv a \ (mod\ p)$. Овим је индукција завршена.

Започевши са $a_1 = a$ наш индуктивни аргумент је конструисао низ $a_1, a_2, a_3, ..$ у $\mathbb{Z}_p$ такав да је $f(a_n) \equiv 0 \ (mod\ p^n)$ и $a_{n+1} \equiv a_n \ (mod\ p^n)$ за свако n. Услов $a_{n+1} \equiv a_n \ (mod\ p^n)$ имплицира да је $\{a_n\}$ Кошијев низ у $\mathbb{Z}_p$. Пошто је $\mathbb{Q}_p$ комплетно поље, овај низ има граничну вредност у $\mathbb{Q}_p$, и сви његови чланови имају апсолутну вредност највише 1, па је то случај и са његовим лимесом, и зато ће остати у $\mathbb{Z}_p$.

Нека је α његова граница у $\mathbb{Z}_p$. Желимо да покажемо да је $f(\alpha) = 0$ и $\alpha \equiv a \ (mod\ p)$.
Из $a_{n+1} \equiv a_n \ (mod\ p^n)$ за свако n, добијамо да је $a_m \equiv a_n \ (mod\ p^n)$ за све $m > n$, дакле

$\alpha \equiv a_n \ (mod\ p^n)$ када пустимо да $m \rightarrow$

а да заиста то можемо урадити је оправдано Хенселовом лемом која ће нам обезбедити услове под којима се корен полинома по модулу p може подићи до корена у $\mathbb{Z}_p$. Па се тако два корена полинома $X^2 - 7$ за $p = 3$, могу подићи на квадратни корен од 7 у $\mathbb{Z}_3$.

Сада ћемо навести јачу варијацију Хенселове леме, која се може користити у ситуацијама када је a по модулу p вишеструки корен $f(X)$ по модулу p: $f(a) \equiv 0 \ (mod\ p)$ и $f'(a) \equiv 0 \ (mod\ p)$. Ову теорему наводимо без доказа. Два различита доказа ове теореме се могу пронаћи у [8].

Теорема 3.1.4 (Хенселова лема: верзија 2) *Нека је* $f(X) \in \mathbb{Z}_p[X]$ и $a \in \mathbb{Z}_p$ *такво да је* $|f(a)|_p < |f'(a)|^2{}_p$. *Тада постоји јединствено* $\alpha \in \mathbb{Z}_p$ *такво да је* $f(\alpha) = 0$ *у* $\mathbb{Z}_p$ *и* $|\alpha - a|_p < |f'(a)|_p$. *Штавише важи следеће:*

(i) $|\alpha - a|_p = |f(a)/f'(a)|_p < |f'(a)|_p$
(ii) $|f'(\alpha)|_p = |f'(a)|_p$. □

Због $f'(a) \in \mathbb{Z}_p$, $|f'(a)|_p \leq 1$. Ако је $|f'(a)|_p = 1$, тада се претпоставка Теореме 3.1.4 своди на претпоставку Теореме 3.1.1: уколико је $|f(a)|_p < 1$ и $|f'(a)|_p = 1$ то значи да је $f(a) \equiv 0 \ (mod\ p)$ и $f'(a) \not\equiv 0 \ (mod\ p)$. Теорема 3.1.4 заправо иде даље од закључка Теореме 3.1.1 када су претпоставке Теореме 3.1.1 задовољене, јер у Теореми 3.1.4 сазнајемо колико тачно је удаљен корен α од приближног корена a. Али главни циљ Теореме 3.1.4 јесте да дозволимо могућност да $|f'(a)|_p < 1$ што уопште није покривено Теоремом 3.1.1.

Теорема 3.1.5 *Број* $b \in \mathbb{Z}_2{}^{\times}$ *је квадрат у* $\mathbb{Z}_2{}^{\times}$ *акко је* $b \equiv 1 \ (mod\ 8)$.

Доказ: ($\Longleftarrow$) Нека је $f(X) = X^2 - b$ и нека је $b \equiv 1 \ (mod\ 8)$. Тада за $\alpha_1 = 1$ важи да је $f(\alpha_1) \equiv 0 \ (mod\ 8)$, па $|f(\alpha_1)|_2 \leq 2^{-3}$. Такође, $f'(\alpha_1) = 2\alpha_1 = 2$ па је $|f'(\alpha_1)|_2{}^2 = |4|_2 = 2^{-2}$. Дакле, услови за употребу Теореме 3.1.4 су испуњени па постоји $\alpha \in \mathbb{Z}_p$ такво да је $f(\alpha) = 0$.
($\Longrightarrow$) Ако је $b^2 = a$ онда је и a јединица у $\mathbb{Z}_2$. То значи да је $a = 1 + 2x$ (јер $a \equiv 1 \ (mod\ 2)$) па $b = 1 + 4x + 4x^2 \equiv 1 + 4x(x + 1) \equiv 1 \ (mod\ 8)$. □

Пример 3.1.6 Нека је $f(X) = X^4 - 7X^3 + 2X^2 + 2X + 1$. Тада $f(X) \equiv (X + 1)^2(X^2 + 1) \ (mod\ 3)$. Примећујемо да је 2 по модулу 3 двоструки корен. Како је $|f(2)|_3 = 1/27$ и $|f'(2)|_3 = |-42|_3 = 1/3$, услов $|f(2)|_3 < |f'(2)|^2{}_3$ је задовољен, дакле постоји јединствени корен полинома $f(X)$, α у $\mathbb{Z}_3$, такав да је $|\alpha - 2|_3 < 1/3$, на пример: $\alpha \equiv 2 \ (mod\ 9)$.
Заправо постоје два корена $f(X)$ у $\mathbb{Z}_3$:
$2 + 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^6 + \cdots$ и $2 + 3^2 + 3^4 + 2 \cdot 3^5 + 2 \cdot 3^6 + \cdots$
Други корен се своди на 2 по модулу 9, и то је α. Први корен се своди на 5 по модулу 9, и његово постојање се потврђује провером $|f(5)|_3 = 1/27 < |f'(5)|^2{}_3 = 1/9$.

3.2 Хасеова теорема

Једна од последица Хенселове леме јесте да за дати полином са целобројним коефицијентима, обично није тешко утврдити да ли он има корене у $\mathbb{Z}_p$, пошто је довољно пронаћи корене по модулу p. Исто важи и за $\mathbb{R}$, где можемо закључити да ли постоје корени, на основу знака полинома (на пример, ако полином има различите знакове у $x = a_1$ и $x = a_2$ између ова два броја мора постојати реалан корен). Такође, лако је уочити да ако полином има корене у $\mathbb{Q}$ онда има и корене у сваком $\mathbb{Q}_p,\ p \leq \infty$. Дакле, можемо закључити да полином нема рационалних корена ако постоји неко $p \leq \infty$ за које полином нема p-адских корена. На пример: $x^2 + 1 = 0$ нема корене у $\mathbb{R}$, самим тим нема корене у $\mathbb{Q}$ или $x^2 - 2 = 0$, нема корене у $\mathbb{Q}_2$, самим тим нема корене у $\mathbb{Q}$. Чињеница да су корени у $\mathbb{Q}$ аутоматски и корени у $\mathbb{Q}_p,\ p \leq \infty$, значи да је "глобални" корен такође и "локални" корен у сваком p. Много интересантније би било обрнуто, тј. да "локалне" корене можемо "сјединити" тако да дају "глобалне" корене. Ево једног таквог примера:

Теорема 3.2.1 $x \in \mathbb{Q}$ *је квадрат акко је квадрат у сваком* $\mathbb{Q}_p,\ p \leq \infty$.

Доказ: За било које $x \in \mathbb{Q}$, имамо да је $x = \pm \prod_{p<\infty} p^{v_p(x)}$. Ако је x квадрат у ∞, позитиван је. Ако је x квадрат за прост p, тада је валуација $v_p(x)$ парна, па следи да је такво x квадрат у $\mathbb{Q}$. □

Ова веома важна идеја нас враћа назад до Хенсела, али такође је и позната као "Хасеов принцип", зато што је Хасе, Хенселов ученик, први дао теорему у том правцу. Принцип бисмо могли записати на следећи начин: уколико објединимо локалне информације за све $p \leq \infty$ требали бисмо добити и глобалне информације. Веома интересантан пример ове врсте методе је теорија Диофантових једначина, у којој нам је дата једначина за коју желимо да пронађемо решења у $\mathbb{Q}$ или бар да видимо да ли је она уопште решива у $\mathbb{Q}$.

Циљ наредних теорема јесте да видимо да у неким случајевима можемо закључити обрнуто, тј. ако постоји локални корен за свако $\mathbb{Q}_p$, да ли и када то значи да постоји и глобалан корен, тј. корен у $\mathbb{Q}$.

Теорема 3.2.2 (Хасеова теорема, верзија 1) *Нека је* $F \in \mathbb{Z}[X_1, \ldots . X_m]$ *квадратна форма. Тада* $F(X_1, \ldots . X_m) = 0$ *има нетривијално решење у* $\mathbb{Z}^m$ *(или еквивалетно у* $\mathbb{Q}^m$*) акко:*

(i) *има нетривијално решење у* $\mathbb{R}^m$ *и*
(ii) *има примитивно решење по модулу* N *за све позитивне целе* N. □

Тврдња да су (i) и (ii) потребан и довољан услов за постојање нетривијалних решења се зове *Хасеов принцип* за квадратне форме.

Кинеска теорема о остацима нам дозвољава да преформулишемо теорему на следећи начин:

Теорема 3.2.3 (Хасеова теорема, верзија 2) *Нека је* $F \in \mathbb{Z}[X_1, \ldots . X_m]$ *квадратна форма. Тада* $F(X_1, \ldots . X_m) = 0$ *има нетривијално решење у* $\mathbb{Z}^m$ *акко:*

(i) *има нетривијално решење у* $\mathbb{R}^m$ *и*
(ii) *има примитвно решење по модулу* p^k *за сваки прост број* p *и* $k > 1$ □

Теорема 3.2.4 (Хасеова теорема, верзија 3) *Нека је* $F \in \mathbb{Z}[X_1, \ldots . X_m]$ *квадратна форма. Тада* $F(X_1, \ldots . X_m) = 0$ *има нетривијално решење у* $\mathbb{Q}$ *акко:*

(i) *има нетривијално решење у* $\mathbb{Q}_p$ *за свако* $p \leq \infty$. □

Дакле, једначина (3.1.1) задовољава Хасеов принцип ако има нетривијално решење у $\mathbb{Z}^m$ акко:

(i) има решење у $\mathbb{R}^m$ и
(ii) има примитвно решење по модулу N за све $\mathrm{N} > 0$ тј.

(ii') има примитивно решење по модулу p^k за сваки прост број p и $k > 1$.

Нека су $a, b, c \in \mathbb{Q}$ и посматрајмо једначину: $aX^2 + bY^2 + cZ^2 = 0$. Желимо да користимо Хасеову теорему да бисмо видели када једначина има нетривијална рационална решења. Видимо да можемо претпоставити да ни један од a, b, c није нула (јер у супротном има решење када су две променљиве 0 а трећа ненула). Можемо претпоставити и да $a, b, c \in \mathbb{Z}$. Даље, можемо претпоставити да $(a, b, c) = 1$, у супротном скратимо заједничке факторе. Покажимо да можемо узети бесквадратне a, b, c, и да можемо отићи корак даље и претпоставити да су у паровима узајамно прости. Ако је $a = a'n^2$, онда се наша једначина трансформише у $a'(nX)^2 + bY^2 + cZ^2 = 0$, па ако она има решење, онда и полазна једначина има решење и обрнуто. Ако је $(a, b) = k$, следи да је k бесквадратан и $(k, c) = 1$. Нека је $a = a'k$ и $b = b'k$. Онда се једначина трансформише у $a'kX^2 + b'kY^2 + cZ^2$, па видимо да $k \mid cZ^2$, одакле $k \mid Z^2$, па $k \mid Z$ (јер k није дељив са квадратом осим 1). Нека је $Z = kZ'$, па се једначина трансформише у $a'X^2 + b'Y^2 + ckZ'^2$, па следи да можемо претпоставити да су a, b, c у паровима узајамно прости. Дакле, желимо решења $aX^2 + bY^2 + cZ^2 = 0$, где су $a, b, c \in \mathbb{Z}$ у паровима узајамно прости, и нису дељиви квадратом осим 1. По Хасеовој теореми, довољно је да видимо шта се дешава у $\mathbb{Q}_p$ за $p \leq \infty$.

(i) Нека је $p = \infty$, па је $\mathbb{Q}_p = \mathbb{R}$. Тада знак игра веома битну улогу: докле год можемо пронаћи нешто позитивно, можемо узети квадратни корен како би нашли реално решење. Дакле, једначина ће имати нетривијално решење акко нису сви a, b, c истог знака.
(ii) Нека је сада p непаран прост број који не дели ни један од a, b, c. Проучимо решења по модулу p.

Теорема 3.2.5 *Нека је* p *непаран прост број, и нека су* $a, b, c \in \mathbb{Z}$ *у паровима узајамно прости цели бројеви који нису дељиви са* p. *Тада постоје* $x_0, y_0, z_0 \in \mathbb{Z}_p$ *који нису сви дељиви са* p *такви да* $ax_0^2 + by_0^2 + cz_0^2 \equiv 0\ (mod\ p)$.

Доказ: Како x, y, z пролазе кроз целе између 0 и $p - 1$, постоји p^3 различитих тројки (x, y, z). Сада ћемо покушати да пребројимо тројке које су решења $aX^2 + bY^2 + cZ^2 \equiv 0\ (mod\ p)$. Користићемо следећи трик: приметимо да је

$$(ax^2 + by^2 + cz^2)^{p-1} \equiv \begin{cases} 1\ (mod\ p) & \text{ако } (x, y, z) \text{ није решење} \\ 0\ (mod\ p) & \text{ако је } (x, y, z) \text{ решење} \end{cases}$$

на основу Мале Фермаове теореме, јер је $n^{p-1} \equiv 1\ (mod\ p)$ кад год је $n \not\equiv 0\ (mod\ p)$. Ако је N укупан број тројки које нису решење, онда

$$N \equiv \sum_{(x,y,z)} (ax^2 + by^2 + cz^2)^{p-1} \ (mod\ p)$$

где сваки од x, y, z пролазе кроз целе између 0 и $p-1$. Расписивањем израза са десне стране добија се сума по i, j, k (тако да је $i + j + k = p - 1$) чији су сабирци облика

$$\sum_{(x,y,z)} \alpha x^{2i} y^{2j} z^{2k}$$

где $\alpha \in \mathbb{Z}$. Тврдимо да је свака од ових сума конгруентна са 0 по модулу p. Приметимо да је неки од i, j, k мањи од $p-1$ (ако су сви бар $p-1$, онда је $2i + 2j + 2k \geq 3(p-1)$ што није тачно). Нека је рецимо $i < p - 1$. Онда нашу суму можемо записати на следећи начин

$$\sum_{(y,z)} (\alpha y^{2j} z^{2k} \sum_{x} x^{2i})$$

Сада ћемо се позвати на следећу лему:

Лема 3.2.6 *Нека је n цео број, такав да је $0 \leq n < p - 1$. Тада је $\sum_{x=0}^{p-1} x^n \equiv 0 \ (mod\ p)$* □

Напомена: у Леми 3.2.6, ако је $n = 0$, тада је наша сума $= 0^0$; у овом случају узимамо да је то синоним за 1.

Позивајући се на ову лему, видимо да је и наша сума конгруентна са 0 по модулу p, што значи да је и $N \equiv 0 \ (mod\ p)$. Другим речима, број тројки које нису решење је дељив са p, па је и број тројки које јесу решење дељив са p (јер има p^3 тројки). Знамо да је тројка $(0,0,0)$ решење. Комбинујући две последње чињенице добијамо да постоји још бар једно решење. □

Оно што можемо да закључимо након ове теореме јесте да када $p \nmid 2abc$, тада конгруенција $aX^2 + bY^2 + cZ^2 \equiv 0 \ (mod\ p)$ има решење које је нетривијално по модулу p. Дакле, можемо да изведемо следећу последицу:

Последица 3.2.7 *Нека је p непаран прост број, који не дели abc, тада једначина $aX^2 + bY^2 + cZ^2 = 0$ има нетривијално решење у $\mathbb{Q}_p$.* □

Остаје нам још да испитамо шта се дешава када је $p = 2$, и када p дели неки од коефицијената.

(iii) Нека је сада $p = 2$ и нека су a, b, c сви непарни. У овом случају ће нам бити потребан неки посебан услов који ће нам загарантовати да постоје решења у $\mathbb{Q}_2$. Ако претпоставимо да је (x, y, z) нетривијално решење где $x, y, z \in \mathbb{Q}_2$, тада можемо претпоставити да је $max\{|x|_2, |y|_2, |z|_2\} = 1$, тј. да су x, y, z заправо 2-адски цели који нису сви у $2\mathbb{Z}_2$. (потребно је помножити дато решење са позитивним или негативним степеном од 2 како би се добио обај резултат). Сужавајући на $mod\ 2\mathbb{Z}_2$, и како су сви коефицијенти непарни, можемо закључити да ће тачно два од x, y, z бити 2-адске јединице, а један је дељив са 2. Претпоставимо да су y, z јединице. Квадрат 2-адске јединице увијек припада $1 + 4\mathbb{Z}_2$, док квадрат елемента из $2\mathbb{Z}_2$ увијек припада $4\mathbb{Z}_2$. Дакле, у $4\mathbb{Z}_2$ имамо $b + c \equiv 0 \ (mod\ 4)$. Другим речима, ако је $p = 2$, $2 \nmid abc$, и постоји решење у $\mathbb{Q}_2$, тада је збир нека

два од a, b, c дељив са 4.
Нека је $b + c \equiv 0\ (mod\ 4)$. Ако $b + c \equiv 0\ (mod\ 8)$, онда је за $x_0 = 0, y_0 = 1, z_0 = 1, {x_0}^2 + b{y_0}^2 + c{z_0}^2 \equiv 0\ (mod\ 8)$, а ако $b + c \equiv 4\ (mod\ 8)$, онда је за $x_0 = 2, y_0 = 1, z_0 = 1,\ {x_0}^2 + b{y_0}^2 + c{z_0}^2 \equiv 0\ (mod\ 8)$. Свакако имамо услове за јачу верзију Хенселову леме чијом применом добијамо да једначина $aX^2 + bY^2 + cZ^2$ има решење у $\mathbb{Q}_2$.

(iv) Нека је $p = 2$ и један од a, b, c паран. Тада једначина $aX^2 + bY^2 + cY^2$ има нетривијално решење у $\mathbb{Q}_2$ акко је збир нека два од a, b, c дељив са 8, или је збир сва три дељив са 8. (ово следи аналогно из (iii)).

(v) Нека је $p \neq 2$ и a дељив са p. Користићемо следећу терему:

Теорема 3.2.8 *Нека је p непаран прост број који дели a. Тада једначина $aX^2 + bY^2 + cZ^2 = 0$ има нетривијална решења у $\mathbb{Q}_p$ акко $-b/c$ квадратни остатак по модулу p.*

Доказ: Претпоставимо да једначина има решење (x, y, z). Можемо да претпоставимо да $\max\{|y|_p, |z|_p\} = 1$ (у супротном поделимо или помножимо са одговарајућим p^k). Како $p \mid a$, следи да је $by^2 + cz^2 \equiv 0\ (mod\ p)$, па следи да $|y|_p = |z|_p = 1$. Онда претходну конгруенцију можемо записати као $b + (z/y)^2 c \equiv 0\ (mod\ p)$ па је $-b/c$ квадратни остатак.
Ако је $-b/c$ квадратни остатак по модулу p, тада је $-b/c \equiv r^2\ (mod\ p)$, и узмимо $y_0 = 1$, $z_0 = r$, $x_0 = 1$. Тада је $a{x_0}^2 + by_0^2 + cz_0^2 \equiv 0\ (mod\ p)$. Како је још $y_0 \neq 0$ имамо услове за Хенселову лему, чијом применом добијамо да дата једначина има решење у $\mathbb{Q}_p$. □

Дакле, прошли смо све случајеве простих бројева p. Спајањем последњих неколико теорема и закључака, добијамо следеће тврђење.

Теорема 3.2.9 *Нека су a, b, c у паровима узајамно прости бесквадратни цели бројеви. Једначина $aX^2 + bY^2 + cZ^2 = 0$ има нетривијална решења у $\mathbb{Q}$ акко су задовољени следећи услови:*

- *(i)* *a, b, c нису сви истог знака;*
- *(ii)* *за сваки непран прост број p који дели a, постоји $r \in \mathbb{Z}$ такав да $b + r^2 c \equiv 0\ (mod\ p)$, и слично за непране просте које деле b, c;*
- *(iii)* *ако су a, b, c сви непарни, збир нека два од њих је дељив са 4;*
- *(iv)* *ако је a паран, онда је неки од $b + c, a + b + c$ дељив са 8, и слично ако је неки од друга два паран.* □

3.3 Контрапримери Хасеовог принципа

Постоје многи примери једначина за које Хасеов принцип не важи.

Пример бр. 1

Посматрајмо следећу једначину

$$f(X) = (X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$$

Она има решења у $\mathbb{Q}_p$ за све $p \leq \infty$, али нема решења у $\mathbb{Q}$.

Доказ: Очигледно је да f има решење у $\mathbb{R}$ и да нема решења у $\mathbb{Q}$ јер 2,17 и 34 нису квадрати рационалних бројева. Остаје нам да покажемо да једначина има решење у сваком комплетирању поља $\mathbb{Q}$.
Случај: $p \neq 2, 17$
Ако је било који од $\left(\frac{2}{p}\right) = 1$ или $\left(\frac{17}{p}\right) = 1$ тада је $\alpha^2 \equiv 2\ (mod\ p)$ или $\alpha^2 \equiv 17\ (mod\ p)$ решиво у $\mathbb{Z}/p\mathbb{Z}$. Због тога постоји $\alpha \in \mathbb{Z}/p\mathbb{Z}$ такво да је $f(\alpha) \equiv 0\ (mod\ p)$. Извод $2a \not\equiv 0\ (mod\ p)$ јер је $p \neq 2$, и $\alpha \not\equiv 0\ (mod\ p)$, па се решења могу подићи користећи Хенселову лему.
Ако је $\left(\frac{2}{p}\right) = -1$ и $\left(\frac{17}{p}\right) = -1$, тада је $\left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{34}{p}\right) = 1$ јер је Лежандров симбол мутипликативан.
Случај: $p = 17$
Како је $6^2 \equiv 2\ (mod\ 17)$ тада је $f(6) \equiv 0\ (mod\ 17)$ и $f'(6) = 12 \not\equiv 0\ (mod\ 17)$.
Случај: $p = 2$
Како је $17 \equiv 1\ (mod\ 8)$ 17 је 2-адски квадрат на основу леме: a је 2-адски квадрат у $\mathbb{Z}_2$ акко $a \equiv 1\ (mod\ 8\mathbb{Z}_2)$.
Дакле, $(X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$ нема решења у $\mathbb{Q}$ иако има решења у $\mathbb{Q}_p$ за све $p \leq \infty$. □

Пример бр. 2

Један од најпознатијих примера у коме Хасеов принцип не важи дао је Селмер. Наиме, кубна једначина:

$$3x^3 + 4y^3 + 5z^3 = 0$$

има нетривијална решња у $\mathbb{R}$ и у сваком $\mathbb{Q}_p$, док у $\mathbb{Q}$ има само тривијална решења $(0,0,0)$.

Доказ: Очгледно је $(\sqrt[3]{5/3}, 0, -1)$ нетривијално решење у $\mathbb{R}$. Како бисмо показали да једначина има нетривијална решења у $\mathbb{Q}_p$ показаћемо да она има ненула решење по модулу p а затим ћемо подићи то решење p-адски користећи Хенселову лему.
Посматраћемо засебно следеће случајеве: $p = 3, p = 5$, и $p \neq 3, 5$.
$p = 3$
Да бисмо пронашли 3-адска решења узећемо да је $x = 0$ и $z = -1$, тј. посматраћемо следећу

једначину $4y^3 - 5 = 0$ или $y^3 = 5/4$. Иако је $5/4 \equiv -1\ (mod\ 9)$ и -1 је 3-адски куб: да бисмо користили Хенселову лему (у форми $|f(\alpha)|_3 < |f'(\alpha)|^2{}_3$) морамо наћи $\alpha \in \mathbb{Z}_3^x$ такво да $|\alpha^3 - 5/4|_3 < 1/9$, на пример: $\alpha^3 \equiv 5/4\ (mod\ 27)$. Ово важи за $\alpha = 2$, па је $5/4$ 3- адски куб и $(0, y, -1)$ је решење Селмерове једначине у $\mathbb{Q}_3$ где је $y^3 = 5/4$ у $\mathbb{Z}_3$.

$p \neq 3$

Ако је $p \neq 3$ и p-адски цели број a је ненула куб по модулу p тада је a куб у $\mathbb{Z}_p^x$ према Хенселовој леми за $X^3 - a$.

$p = 5$

Узећемо да је $y = -1$ и $z = -1$, тј. посматраћемо следећу једначину $3x^3 - 4 - 5 = 0$, или $x^3 = 3$. С обзиром да је $3 \equiv 2^3\ (mod\ 5)$ према Хенселовој леми за $X^3 - 3$, са приближним решењем 2 видимо да је 3 заправо 5-адски куб и да је $(x, -1, -1)$ решење Селмерове једначине где је $x^3 = 3$ у $\mathbb{Z}_5$.

$p \neq 3, 5$

Тада $3,5 \not\equiv 0\ (mod\ p)$. Посматраћемо сада групу $(\mathbb{Z}/(p))^x$ која је циклична група реда $p - 1$.[12] Интересује нас који део групе је попуњен кубовима?

- Ако је $p \equiv 1(mod\ 3)$ тада су кубови у $(\mathbb{Z}/(p))^x$ заправо подгрупа индекса 3.
- Ако је $p \not\equiv 1\ (mod\ 3)$ тада је $(3, p - 1) = 1$ дакле сваки број у $(\mathbb{Z}/(p))^x$ је куб.[12]

Ако је $3\ (mod\ p)$ куб, тада је 3 куб у $\mathbb{Z}_p$ на основу Хенселове леме за $X^3 - 3$, дакле $(x, -1, -1)$ је решење Селмерове једначине где је $x^3 = 3$ у $\mathbb{Q}_p$.

Уколико $3\ (mod\ p)$ није куб, тада нису сви бројеви из $(\mathbb{Z}/(p))^x$ кубови. Дакле $p \equiv 1\ (mod\ 3)$, тј. ненула кубови $mod\ p$ су подгрупа индекса 3 групе $(\mathbb{Z}/(p))^x$ са косет представницима $\{1,3,9\}$: за свако $a \not\equiv 0\ (mod\ p)$ имамо да је $a \equiv b^3, 3b^3$ *или* $9b^3\ (mod\ p)$ за неко $b \not\equiv 0\ (mod\ p)$.[12] Применићемо ово за $a = 5$.

- Ако је $5 \equiv b^3\ (mod\ p)$ тада је 5 куб у $\mathbb{Z}_p$ према Хенселовој леми за $X^3 - 5$, па можемо рећи да је $(-y, y, -1)$ решење Селмерове једначине где је $y^3 = 5$ у $\mathbb{Z}_p$
- Ако је $5 \equiv 3b^3\ (mod\ p)$ тада је 5/3 куб у $\mathbb{Z}_p$ према Хенселовој леми, па можемо рећи да је $(x, 0, -1)$ решење Селмерове једначине где је $x^3 = 5/3$.
- Ако је $5 \equiv 9b^3\ (mod\ p)$ тада је 5·3=15 куб у $\mathbb{Z}_p$ према Хенселовој леми, па је $(3t, 5, -7)$ решење Селмерове једначине где је $t^3 = 15$. Дакле, посматрамо једначину $3a^3 + 4b^3 + 5c^3 = 0$ где је $a = 3t, b = 5$ и $c = -7$. На основу хомогености, $(3t/7, 5/7, -1)$ је такође решење. □

Овим завршавамо доказ да Селмерова једначина има нетривијална решења у $\mathbb{Q}_p$. Доказ да једначина има само тривијално решење у $\mathbb{Q}$ може се пронаћи у [12].

Последица 3.3.1: Једначина $3x^3 + 4y^3 = 5$ има решења у $\mathbb{R}$ и у сваком $\mathbb{Q}_p$, али нема решења у $\mathbb{Q}$.

Доказ: Показали смо да у $\mathbb{R}$ и у сваком $\mathbb{Q}_p$ постоји решење једначине $3x^3 + 4y^3 + 5z^3 = 0$ где је $z = -1$, и за такво решење имамо да је $3x^3 + 4y^3 = 5$. Ако би једначина $3x^3 + 4y^3 = 5$ имала решење у $\mathbb{Q}$, то би значило да једначина $3x^3 + 4y^3 + 5z^3 = 0$ такође има решење у $\mathbb{Q}$ за $z = -1$ што је контрадикција са Примером бр. 2. □

Постоји још примера хомогених кубних полинома који такође имају само тривијална решења у $\mathbb{Q}$, а неки од тих полинома су:

$$x^3 + 5y^3 + 12z^3, x^3 + 4y^3 + 15z^3, x^3 + 3y^3 + 20z^3, x^3 + 3y^3 + 22z^3$$

Пример бр. 3

Међутим, Селмеров пример није најстарији пример а ни најједноставнији. Следећи пример за који Хасеов принцип не важи пронашли су Линд и Ричард. Наиме једначина:

$$x^4 - 17z^4 = 2y^2$$

има решења у $\mathbb{Q}_p$ за све $p \leq \infty$, али нема решења у $\mathbb{Q}$.

Доказ: Претпоставимо да једначина има решења у $\mathbb{Q}$. Без умањена општости та решења можемо записати као (x, y, z) где су x, y, z цели бројеви и x, z узајамно прости и нека је $y > 0$.
Нека је q непаран прост број такав да $q \mid y$, тада је $x^4 \equiv 17z^4 \ (mod\ q)$, дакле 17 је квадрат по модулу q. На основу квадратног закона реципроцитета то значи да је q квадрат по модулу 17. Како су 2 и -1 такође квадрати по модулу 17, закључујемо да сви прости бројеви који деле y су квадрати по модулу 17, па и y мора бити квадрат по модулу 17. Дакле $y \equiv {y_0}^2 (mod\ 17)$. Уврштавајући ово у једначину, добијамо $2{y_0}^4 \equiv x^4 (mod\ 17)$, самим тим 2 је четврти степен по модулу 17. Како ово није тачно, долазимо у контрадикцију, самим тим једначина нема решења у $\mathbb{Q}$. □

Глава 4

4 Системи квадратних Диофантових једначина

Селмеров пример (Поглавље 3.3) показује да се Хасеов принцип не може проширити на полиноме степена већег од 2. Међутим постоји и други начин како можемо генерализовати Хасеов принцип. Задржати степен полинома два, али дозволити системе једначина. Да ли Хасеов принцип важи за све системе

$$F_1(X,Y,Z,W) = 0, \quad F_2(X,Y,Z,W) = 0 \tag{4.0.1}$$

докле год су $F_1, F_2 \in \mathbb{Z}[X,Y,Z,W]$ ограничен на степен 2? Одговор је не, и главни циљ овог рада јесте представити интересантне контрапримере. Диофантов систем једначина који ћемо разматрати је облика

$$aU^2 + bV^2 + cW^2 = dZ^2, \quad UW = V^2 \tag{4.0.2}$$

где су $a,b,c,d \in \mathbb{Z}$, d бесквадратан, $a,c,d \neq 0$ и $b^2 - 4ac \neq 0$. Систем (4.0.2) је уско повезан са следећом нехомогеном једначином:

$$aX^4 + bX^2Y^2 + cY^2 = dZ^2 \tag{4.0.3}$$

Штавише следеће леме нам дозвољавају да пребацимо систем (4.0.2) у нехомогену једначину (4.0.3).

Лема 4.0.1 *Систем (4.0.2) има нетривијално решење у* $\mathbb{Z}^4$ *акко једначина (4.0.3) има нетривијално решење у* $\mathbb{Z}^3$. *Такође, систем (4.0.2) има нетривијално решење у* $\mathbb{R}^4$ *акко једначина (4.0.3) има нетривијано решење у* $\mathbb{R}^3$.

Доказ: ако је $(x_0,\ y_0,\ z_0)$ нетривијално решење једначине (4.0.3) у $\mathbb{Z}^3$ тада $(x_0^2, x_0y_0, y_0^2, z_0)$ нетривијално решење система (4.0.2).
Ако $(u_0,\ v_0,\ w_{0,}\ z_{0,})$ нетривијално решење система (4.0.2), тада су $(v_0,\ w_0,\ z_0\, w_0)$ и $(u_0,\ v_0,\ z_0\, u_0)$ решења једначине (4.0.3) у $\mathbb{Z}^3$. Најмање једно од њих мора бити нетривијално решење. Ово важи када се $\mathbb{Z}$ замени са било којим прстеном који садржи $\mathbb{Z}$ па важи и за $\mathbb{R}$. □

Лема 4.0.2 *Нека је* p *прост, и* $k \geq 2$. *Тада систем (4.0.2) има примитивно решње по модулу* p^k *акко једначина (4.0.3) има примитивно решење по модулу* p^k.

Доказ: ако је $(x_0,\ y_0,\ z_0)$ примитивно решење једначине (4.0.3) по модулу p^k тада је $(x_0^2, x_0y_0, y_0^2, z_0)$ примитивно решење система (4.0.2) по модулу p^k.
Ако $\left(u_0,\ v_0,\ w_{0,}\ z_0\right)$ примитивно решење система (4.0.2) по модулу p^k, тада су $(v_0,\ w_0,\ z_0\, w_0)$ и $(u_0,\ v_0,\ z_0u_0)$ решења једначине (4.0.3) по модулу p^k. Тврдња: најмање један од $u_0,\ v_0$ или w_0, мора бити узајамно прост са p^k. У супротном, $z_{0,}$ је узајамно прост са p^k, и с обзиром на $dz_0^2 \equiv au_0^2 + bv_0^2 + cw_0^2 \left(mod\ p^k\right)$ следи да $p^2 \mid d$ што је контрадикција са тим да је d бесквадратан.

На основу горе наведене тврдње, најмање један од $u_0,\ v_0,$ или $w_0,$ има инверз по модулу p^k. На пример, ако u_0 има инверз u_0^{-1} тада је $(1, v_0u_0^{-1}, z_0u_0^{-1})$ примитивно решење једначине (4.0.3) по модулу p^k. Исто тако ако v_0 или w_0 имају инверз по модулу p^k тада се $(v_0,\ w_0,\ z_0\, w_0)$ може модификовати тако да формира примитивно решење по модулу p^k. □

Напомена: Ако $p \nmid d$, тада горе наведено можемо проширити на $k = 1$.

4.1 Параметризација коника

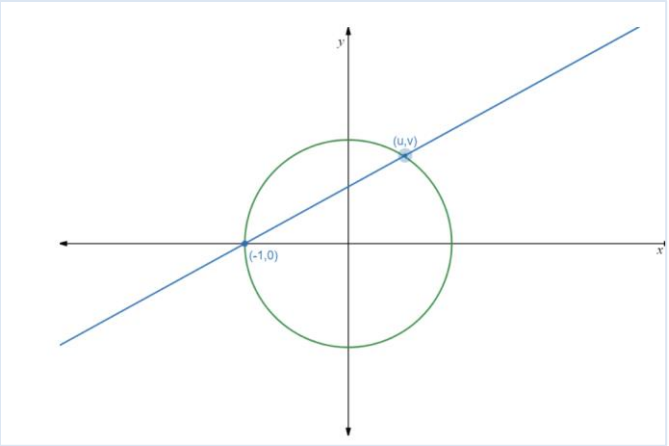
Дефиниција 4.1.1 *Троугао чији су мерни бројеви страница x,y,z природни бројеви који задовољавају релацију* $x^2 + y^2 = z^2$ *назива се Питагорин троугао (на основу Питагорине теореме такав троугао је правоугли). Природни бројеви x,y,z који су решења једначине* $x^2 + y^2 = z^2$ *представљају Питагорине тројке.*

Дефиниција 4.1.2 *Ако нека два од* x, y, z *који задовољавају једначину* $x^2 + y^2 = z^2$ *имају заједнички делилац* d *(већи од 1), онда је и трећи од њих дељив са* d*. Зато ћемо даље претпостављати да су бројеви* x, y, z *узајамно прости у паровима (у противном можемо скратити* $x^2 + y^2 = z^2$ *њиховим заједничким делиоцем* d*). Такво решење* (x, y, z) *дате једначине називамо примитивним решењем. Јасно је да налажењем свих примитивних решења* (x, y, z) *налазимо и сва остала, јер су она облика* $(\alpha x, \alpha y, \alpha z), \alpha \in N$.

Постоји неколико метода за проналажење Питагориних тројки, али један од стандардних метода је метод рационалне параметризације јединичне кружнице $\{(x, y) \in \mathbb{R} |\ x^2 + y^2 = 1\}$.

Дакле, нека је јединична кружница задата једначином $x^2 + y^2 = 1$ и нека је $P = (x_p,\ y_p)$ произвољна тачка на тој кружници. Узмимо било коју другу рационалну тачку на тој кружници и означимо је са $R = (u, v)$. Тада постоји јединствена права p која пролази кроз тачке P и R и чија је једначина: p: $y - y_p = \frac{y_p - v}{x_p - u}(x - x_p)$. (*) при чему су коефицијенти, као и коефицијенти правца праве $\frac{y_p - v}{x_p - u}$ рационални бројеви.

Како би поједноставили ситуацију, нека је $P = (-1,0)$ и посматрајмо праву p_t која пролази кроз тачке $(-1,0)$ и (u, v), као што је приказано на *Слици 1* испод. Приметимо да уколико права на којем лежи тачка $(-1,0)$ није вертикална, тада ће права p_t да сече кружницу у тачно једној тачки различитој од $(-1,0)$, означеној са (u, v).



Слика 1. Пресечне тачке кружнице $x^2 + y^2 = 1$ и праве p_t

Уколико задата права има коефицијент правца једнак t, тада увртавањем координата тачака $(-1,0)$ и (u, v) у формулу за коефицијент правца добијамо $t = \frac{v}{u+1}$. Дакле t је рационални број уколико су u и v рационални бројеви.
Увртавањем коефицијента правца и координата тачке $(-1,0)$ у једначину праве кроз једну тачку (*) добијамо да је задата права описана једначином $y = t(x + 1)$. Пресечне тачке са кружницом се добијају решавањем система

$$\begin{cases} x^2 + y^2 = 1 \\ y = t(x + 1) \end{cases}$$

Односно решавањем једначине $1 - x^2 = y^2 = t^2(x + 1)^2$. Па према томе мора бити или $x = 1$ и $y = 0$ или $1 - x = t^2(1 + x)$. Из другог случаја следи:

$$1 - x = t^2 + t^2 x$$

$$x(1 + t^2) = 1 - t^2$$

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

Увртавањем добијеног израза у једначину праве $y = t(x + 1)$ добијамо $y = \frac{2t}{t^2+1}$ чиме смо одредили координате пресечне тачке (u, v):

$$u = \frac{1 - t^2}{1 + t^2}, \qquad v = \frac{2t}{1 + t^2} \qquad (**)$$

Увртавањем се лако види да су u и v решења једначине $x^2 + y^2 = 1$. Покажимо још да су координате рационалне уколико је и t рационалан број. Штавише, вреди и јача тврдња која каже да су $u, v \in \mathbb{Q}$ акко $t \in \mathbb{Q}$. Заиста, ако је (x_0, y_0) рационално решење једначине $x^2 + y^2 = 1$, а T_0 одговарајућа тачка на кружници онда је коефицијент правца праве кроз тачку $(-1,0)$ и T_0 једнак $t = \frac{y_0}{x_0+1}$ па је самим тим је и рационалан број. Према томе показали смо да права са коефицијеном

правца t која пролази кроз тачку $(-1,0)$ пресеца јединичну кружницу у другој рационалној тачки акко је t рационалан и можемо описати све пресечне тачке користећи t.

Теорема 4.1.3 *Ако су m и n узајамно прости бројеви различите парности такви да је $m > n$ онда су формулама*

$$x = m^2 - n^2, \qquad y = 2mn, \qquad z = m^2 + n^2$$

дефинисане примитивне Питагорине тројке. □

Теорема 4.1.4 *Све примитивне Питагорине тројке (x, y, z) у којима је y парано, дефинисане су следећим формулама:*

$$x = m^2 - n^2, \qquad y = 2mn, \qquad z = m^2 + n^2$$

при чему су m и n узајамно прости бројеви различите парности и такви да је $m > n$. □

Напомена 4.1.5 Да би геметријска интерпретација задате ситуације била јаснија, посматрајмо следећи лимес:

$$\lim_{t\to\pm\infty}(u, v) = \lim_{t\to\pm\infty}\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = (-1,0)$$

Уочимо да када коефицијент правца праве, t, тежи ка $\pm\infty$, друга пресечна тачка праве са кружницом у ознаци (u, v) тежи ка $(-1,0)$. Стога дата права, односно сечица кружнице, тежи тангенти повученој кроз тачку $(-1,0)$ која је паралелна са y осом. Запишимо сада коефицијент правца праве у облику разломка $t = \frac{r}{s}$, при чему је $(r, s) = 1$. Тада записи по координатама (**) постају:

$$u = \frac{s^2 - r^2}{r^2 + s^2}, \qquad v = \frac{2rs}{r^2 + s^2}$$

Множењем са $r^2 + s^2$ добијамо фамилију целобројних решења:

$$(s^2 - r^2, 2rs, r^2 + s^2)$$

Па према Теореми 4.1.4 следи да добијена решења представљају примитивне Питагорине тројке.

Параметризација нас доводи до следећег идентитета у $\mathbb{R}[T]$:

$$(1 - \mathrm{T}^2)^2 + (2\mathrm{T})^2 = (1 + \mathrm{T}^2)^2 \tag{4.1.1}$$

где уколико T заменимо са n/m где су $n, m \in \mathbb{Z}$ добијамо Питагорине тројке:

$$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$$

па можемо посматрати једначину $ax^2 + by^2 = 1$ на било ком пољу F где $a, b \in F$ и $a, b \neq 0$.

Потребна нам је почетна тачка: потребни су нам $x_0, y_0 \in F$ такви да је $ax_0{}^2 + by_0{}^2 = 1$. Аналогни идентитет за (4.1.1) је приказан у следећој леми као (4.1.2).

Лема 4.1.6 *Нека је F поље и нека* $a, b \in F$ *и* $a, b \neq 0$. *Нека* $x_0, y_0 \in F$ *такви да је* $ax_0{}^2 + by_0{}^2 = 1$. *Тада у* $F[T]$ *важи:*

$$a(bx_0T^2 - 2by_0T - ax_0)^2 + b(-by_0T^2 - 2ax_0T + ay_0)^2 = (bT^2 + a)^2 \qquad (4.1.2)$$

и нека су $q_1, q_2, q_3 \in F[T]$ *полиноми степена највише 2, такви да се идентитет 4.1.2 може записати као:* $aq_1^2 + bq_2^2 = q_3^2$. *Најмање два од* q_1, q_2, q_3 *морају бити другог степена. Ако је* $char\ F \neq 2$, *сваки од* q_1, q_2, q_3 *је ненула полином и не постоје два која су асоцирана.*

Подсетимо се да ако су $f(x)$ и $g(x)$ два полинома са коефицијентима у пољу F, и ако постоји ненула елемент $c \in F$ такав да је $f(x) = cg(x)$ онда су полиноми $f(x)$ и $g(x)$ *асоцирани.*

Полиноми q_1, q_2, q_3 се могу пронаћи коришћењем метода параметризације, али то нам тренутно није фокус. Битно нам је само да важи: $aq_1^2 + bq_2^2 = q_3^2$.

Доказ: Препоставимо да је степен полинома $q_3 = 2$ док је $b \neq 0$. С обзиром на $aq_1^2 + bq_2^2 = q_3^2$ такође имамо и да је степен полинома $q_1 = 2$ или је степен полинома $q_2 = 2$. Претпоставимо да је $char\ F \neq 2$. С обзиром да су $a, b \neq 0$, и да x_0 и y_0 нису оба једнака 0, сваки од q_1, q_2, q_3 је ненула. Претпоставимо да су нека два од q_1, q_2, q_3 асоцирани. Тада они морају бити другог степена. Онда из једначине $aq_1^2 + bq_2^2 = q_3^2$ добијамо да су $q_1{}^2, q_2{}^2, q_3{}^2$ асоцирани. На основу Леме 4.1.7 испод следи да су q_1, q_2 константни умножци од q_3. Али или q_1или q_2 имау ненула линеарне чланове, што је контадикција. □

Лема 4.1.7 *Нека су* a *и* b *ненула елементи домена јединствене факторизације R. Ако су* a^n *и* b^n *асоцирани, тада су* a *и* b *такође асоцирани.* □

Постојање q_1, q_2, q_3 у Леми 4.1.6 зависи од постојања најмање једног решења једначине $ax_0{}^2 + by_0{}^2 = 1$. За $F = \mathbb{F}_p$ постојање таквог решења следи из Ојлеровог критеријума: нека је p непаран прост број и $a \in \mathbb{F}_p$ ненула. Из Ојлеровог критеријума следи да је a квадрат у $\mathbb{F}_p$ акко $a^{(p-1)/2} = 1$, и да a није квадрат у $\mathbb{F}_p$ акко $a^{(p-1)/2} = -1$. Ојлеров критеријум је последица добро познатог резултата да је мутипликативна група ненула елемената из $\mathbb{F}_p$ заправо циклична група реда $p - 1$.[1]

Лема 4.1.8 *Нека су* a *и* b *ненула елементи поља* $\mathbb{F}_p$ *гдје је* p *прост број. Тада постоје* $x_0, y_0 \in \mathbb{F}_p$ *такви да* $ax_0{}^2 + by_0{}^2 = 1$.

Доказ: Ако је $p = 2$, можемо узети да је $x_0 = 1$ и $y_0 = 0$. Ако је $p > 2$, онда је потребно решити $y^2 = f(x)$ где је $f(x) = b^{-1}(1 - ax^2)$. Ако не постоји решење, тада је $(\frac{f(t)}{p}) = -1$ за свако $t \in \mathbb{F}_p$. На основу Ојлеровог критеријума, $f(t)^{(p-1)/2} = -1$ за све $t \in \mathbb{F}_p$. Међутим ово је контрадикторно са чињеницом да полином $f(t)^{(p-1)/2} + 1$ степена $p - 1$ мора имати највише $p - 1$ корена. □

Доказ који смо навели овде нас доводи до Лагранжа који је у свом доказу, да је сваки позитиван цели број збир 4 квадрата, морао доказати решивост конгруенције $x^2 + y^2 + 1 \equiv 0\ (mod\ p)$.

4.2 Системи квадратних Диофантових једначина

Нека је p непран прост број. Сада ћемо се посветити проналаску неривијалних решења система

$$aU^2 + cW^2 = dZ^2, \qquad UW = V^2 \tag{4.2.1}$$

са вредностима у $F = \mathbb{F}_p$, где претпостављамо да су $a, c, d \neq 0$. Замењујући a и c са ad^{-1} и cd^{-1} можемо претпоставити да је $d = 1$, па се једначина $aU^2 + cW^2 = Z^2$ може параметризовати. Ово нам даје фамилију решења за прву једначину, и само је потребно утврдити да је бар једно од тих решења такође решење и $UW = V^2$.

Лема 4.2.1 *Нека су $f, g \in \mathbb{F}_p[X]$ ненула полиноми највише другог степена. Ако је $(\frac{f(t)}{p}) = (\frac{q(t)}{p})$ или $\left(\frac{f(t)}{p}\right) = -(\frac{q(t)}{p})$ за све $t \in \mathbb{F}_p$ тада су f и g асоцирани.*

Напомена: У овој леми користимо Лежандров симбол $\left(\frac{a}{p}\right)$. Дакле ако $a \in \mathbb{F}_p$, тада се Лежандров симбол може дефинисати на следећи начин:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ако је } a \text{ ненула квадрат у } \mathbb{F}_p, \\ -1 & \text{ако } a \text{ није квадрат у } \mathbb{F}_p, \\ 0 & \text{ако је } a = 0 \text{ у } \mathbb{F}_p. \end{cases}$$

Доказ: На основу Ојлеровог критеријума $\left(\frac{f(t)}{p}\right) = f(t)^{(p-1)/2}$ и $\left(\frac{q(t)}{p}\right) = q(t)^{(p-1)/2}$.
Дакле, ако је $\left(\frac{f(t)}{p}\right) = \left(\frac{q(t)}{p}\right)$ за све $t \in \mathbb{F}_p$ тада је свако $t \in \mathbb{F}_p$ корен полинома $f^{(p-1)/2} - q^{(p-1)/2}$. Подсетимо се да ненула полином из $\mathbb{F}_p$[T] степена d има највише d корена зато што је $\mathbb{F}_p$ поље. Степен полинома $f^{(p-1)/2} - q^{(p-1)/2}$ је највише $p - 1$, али полином има p корена, дакле $f^{(p-1)/2} - q^{(p-1)/2}$ је нула полином. Али с обзиром да је $\mathbb{F}_p[X]$ домен јединствене факторизације јер је $f^{(p-1)/2} = q^{(p-1)/2}$, полиноми f и g су асоцирани на основу Леме 4.1.7. Ако је $\left(\frac{f(t)}{p}\right) = -\left(\frac{q(t)}{p}\right)$, за све $t \in \mathbb{F}_p$, приметимо да је тада $\left(\frac{f(t)}{p}\right) = (\frac{rq(t)}{p})$ а све $t \in \mathbb{F}_p$,и бесквадратано $r \in \mathbb{F}_p$, па су f и rg асоцирани, а то значи да су онда и f и g асоцирани. □

Теорема 4.2.2 . *Нека је p непаран прост број, и нека $a, c, d \in \mathbb{F}_p$ и $a, c, d \neq 0$. Тада систем*

$$aU^2 + cW^2 = dZ^2, \qquad UW = V^2$$

има нетривијално решење у $\mathbb{F}_p$.

Доказ: Сводимо на случај када је $d = 1$.
Параметризација коника $aU^2 + cW^2 = Z^2$ као у Леми 4.1.6 (користећи Лему 4.1.8) нас доводи до ненула полинома $q_1, q_2, q_3 \in \mathbb{F}_p$[T] за које важи $aq_1^2 + cq_2^2 = q_3^2$, и где q_1и q_2 нису асоцирани.

На основу Леме 4.2.1 и чињенице да q_1и q_2 нису асоцирани, постоји $t \in \mathbb{F}_p$ такво да $\left(\frac{q_1(t)}{p}\right) \neq -(\frac{q_2(t)}{p})$. Дакле, $q_1(t)$ и $q_2(t)$ нису оба нула и $\left(\frac{q_1(t)q_2(t)}{p}\right) \neq -1$. Другим речима $q_1(t)q_2(t) = c^2$ за неко $c \in \mathbb{F}_p$. Стога, $U = q_1(t), W = q_2(t), Z = q_3(t), V = v$ је нетривијално решење система. □

Сада ћемо се фокусирати на p-локалну решивост система (4.2.1), где су a, c, d ненула цели бројеви. За почетак ћемо доказати једно веома познато тврђење из терије бројева (пропозиција испод).

Пропозиција 4.2.3 *Нека је p прост број и нека су N и $r > 0$ цели бројеви такви да $p \nmid rN$. Ако је N r-ти степен по модулу p тада је N r-ти степен по модулу p^k за све $k \geq 1$.*

Доказ: (По индукцији над k) Претпоставимо да је $N \equiv a^r \pmod{p^k}$.
Запишимо то као $N - a^r = cp^k$. Користећи развој бинома добијамо да је
$(a + xp^k)^r \equiv a^r + ra^{r-1}xp^k \pmod{p^{k+1}}$.
Дакле, $N - (a + xp^k)^r \equiv (c - ra^{r-1}x)p^k \pmod{p^{k+1}}$.
Уочимо да је $(p, a) = 1$ с обзиром на то да је $(p, N) = 1$. Дакле постоји x такво да $p \mid (c - ra^{r-1}x)$ и $N \equiv \left(a + xp^k\right)^r \pmod{p^{k+1}}$. □

Уводимо сада појам *јаког решења.*

Дефиниција 4.2.4 *Јако решење по модулу p^k система (4.2.1) је примитивно решење (u, v, w, z) придружених конруенција по модулу p^k такво да је најмање један од au, cw, dz различит од нуле по модулу простог p.*

Теорема 4.2.5 *Нека је p непаран прост број, и нека су a, c, d ненула цели бројеви. Ако систем (4.2.1) има јако решење по модулу p, тада систем има јако решење по модулу p^k за све k. Конкретно, систем је p-локално решив.*

Доказ: Нека је (u_0, v_0, w_0, z_0) јако решење по модулу p. Како је $au_0^2 + cw_0^2 = dz_0^2$, најмање 2 од au_0, cw_0, dz_0 морају бити различити од нуле по модулу p. Можемо претпоставити да је au_0 различит од нуле по модулу p. Фиксирајмо степен p^k од p. Како $p \nmid a$ и $p \nmid u_0$, можемо изабрати инверзне a^{-1}, $u_0^{-1} \in \mathbb{Z}$ по модулу p^k. Даље, нека је $v = v_0u_0^{-1}$, $w = w_0u_0^{-1}$ и $z = z_0u_0^{-1}$. Тада $(1, v, w, z)$ такође решава систем по модулу p. Дакле, $w \equiv v^2 \pmod{p}$, па је и $a + cv^4 \equiv dz^2 \pmod{p}$. Како је $a^{-1}(dz^2 - cv^4) \equiv 1 \pmod{p}$, и како је 1 четврти степен, Пропозиција 4.2.3 нам гарантује постојање $m \in \mathbb{Z}$ таквог да $a^{-1}(dz^2 - cv^4) \equiv m^4 \pmod{p^k}$. Другим речима, $am^4 + cv^4 \equiv dz^2 \pmod{p^k}$, па је (m^2, mv, v^2, z) решење по модулу p^k. То је такође и јако решење јер је m различити од нуле по модулу p. □

Сада наводимо последицу Теореме 4.2.2 и Теореме 4.2.5

Последица 4.2.6 *Нека је p непаран прост број такав да $p \nmid acd$, тада је систем (4.2.1) p-локално решив, тј. има примитивна решења по модулу p^k за све k.* □

Нека је p=2 и посматрајмо систем $U^2 + 3W^2 = 7Z^2,\ UW = V^2$. Овај систем има решење $(1,1,1,2)$ по модулу 2, Заправо, $(1,1,1,2)$ је решење по модулу 2^3. Међутим, систем нема примитивно решење по модулу 2^4.

Потешкоће са проширењем Теореме 4.2.5 на $p = 2$ леже у недостатку Пропозиције 4.2.3. Наиме, 3 јесте четврти степен по модулу $p = 2$, али није четврти степен по модулу $p = 2^k$ за $k > 1$. Следећа пропрозиција нам даје потребну варијанту Пропозиције 4.2.3.

Пропозиција 4.2.7 *Ако је* $N \equiv 1\ (mod\ 2^4)$*, тада је* N *четврти степен по модулу* 2^k *за све* $k \geq 1$.

Доказ: (Индукцијом)Претпоставимо да је $N \equiv a^4\ (mod\ 2^k)$ гдје је $k \geq 4$. То можемо записати као $N - a^4 = c2^k$. Користећи развој бинома добијамо $\left(a + x2^{k-2}\right)^4 \equiv a^4 + a^3x2^k\ (mod\ 2^{k+1})$. Дакле, $N - \left(a + x2^{k-2}\right)^4 \equiv (c - a^3x)2^k\ (mod\ 2^{k+1})$. Уочимо да је $(2, a) = 1$ с обзиром на то да је $(2, N) = 1$. Дакле постоји x такво да $2 \mid (c - a^3x)$ и $N \equiv \left(a + x2^{k-2}\right)^4\ (mod\ 2^{k+1})$. □

Сада можемо увести следећу теорему:

Теорема 4.2.8 *Нека су* a, c, d *ненула цели бројеви. Ако систем (4.2.1) има јако решење по модулу* 2^4*, тада систем има јако решење по модулу* 2^k *за све* k. □

Постоје ситуације у којима нема разлике између примитивних и јаких решења, то нам показује следећа лема и њена последица.

Лема 4.2.9 *Нека је* p *прост,* $k \geq 2$ *и* a, c, d *ненула цели бројеви такви да* $p^2 \nmid acd$. *Тада је свако примитивно решење система (4.2.1) по модулу* p^k *јако решење.*

Доказ: Нека је (u, v, w, z) примитивно решење по модулу p^k такво да није јако решење. Изводимо контрадикцију у случају када $p \nmid u$, а остали случајеви су слични. Како (u, v, w, z) није јако решење, $p \mid a$, па $p \nmid cd$. Дакле p дели и w и z јер (u, v, w, z) није јако решење. Из $au^2 + cw^2 \equiv dz^2\ (mod\ p^2)$ добијамо $au^2 \equiv 0\ (mod\ p^2)$, што значи да $p^2 \mid a$ а то је контрадикција. □

Последица 4.2.10 *Нека је* p *прост и* a, c, d *ненула цели бројеви такви да* $p^2 \nmid acd$. *Ако је* p *непаран, тада је систем (4.2.1)* p*-локално решив акко има јако решење по модулу* p. *За парно* p*, систем (4.2.1) је* p*-локално решив акко има јако решење по модулу* 2^4.

Доказ: ($\Leftarrow$) следи из Тереме 4.2.5 и Теореме 4.2.8.
($\Longrightarrow$) Нека је систем *(4.2.1)* p-локално решив, тада постоји примитивно решење по модулу p^4. На основу Леме 4.2.9 постоји јако решење по модулу p^4. У случају када је p паран, можемо приметити да је такво решење такође и јако решење по модулу p. □

4.3 Контрапримери

Циљ ове секције је идентификовати контрапримере Хасеовог принципа: то ће бити системи једначина који су локално решиви, али нису глобално решиви.

Пропозиција 4.3.1. *Претпоставимо су испуњени следећи услови:*

(1) q *и* d *су узајамно прости ненула цели бројеви, и* q *је позитиван;*
(2) $q \equiv 1 \pmod{16}$*;*
(3) d *је квадрат по модулу* p *за сваки прост број* p *који дијели* q *и*
(4) q *је четврти степен по модулу* p *за сваки непаран прост број* p *који дели* d

Тада је следећи систем локално решив.

$$U^2 - qW^2 = dZ^2, \qquad UW = V^2$$

Доказ: Приметимо да је $(u, v, w, z) = \left(q^{1/2}, q^{1/4}, 1, 0\right)$ реално решење. За све $p \nmid 2qd$, систем је p локално решив на основу Последице 4.2.6. Такође, приметимо да је $(u, v, w, z) = (1,1,1,0)$ јако решење по модулу 16. На основу Теореме 4.2.8 систем је 2-локално решив. Претпоставимо сада да $p \mid q$, дакле p је непаран. Узмимо m такво да $m^2 \equiv d \pmod{p}$. Тада је $(u, v, w, z) = (m, 0,0,1)$ решење по модулу p. Како су q и d узајамно прости, $p \nmid d$, па је због тога решење и јако решње. На основу Теореме 4.2.5 систем је p локално решив.
Претпоставимо сада да непаран прост p дели d. Узмимо m такво да $m^4 \equiv q \pmod{p}$. Тада је $(u, v, w, z) = (m^2, m, 1, 0)$ решење по модулу p, а како $p \nmid q$ решење је и јако решње. На основу Теореме 4.2.5 систем је p-локално решив. □

Сада ћемо пронаћи системе који немају нетривијална $\mathbb{Z}$ решења, а за то ће нам бити потребна следећа лема

Лема 4.3.2 *Нека је* d *ненула бесквадратан цео број и нека је* $q \equiv 1 \pmod{8}$ *прост број који не дијели* d*. Ако систем* $U^2 - qW^2 = dZ^2,\ UW = V^2$ *има нетривијално решење у* $\mathbb{Z}$ *тада је* d *четврти степен по модулу* q*.*

Доказ: Из хомогености следи да ако систем има нетривијално решење онда он има и примитивно решење (u, v, w, z). Приметимо да u и w морају бити узајамно прости с обзиром на то да је $d \in \mathbb{Z}$ бесквадратан. Ако $p \mid u$ и $p \mid w$ тада $p \mid v$ и $p^2 \mid dz^2$, па $p^2 \mid d$ што је контрадикција. На исти начин можемо показати да су u и z узајамно прости и да су w и z такође узајамно прости. Такође, с обзиром да је $u^2w^2 = v^4$ и u и w су узајамно прости, u^2 и w^2 морају бити четвртог степена. Нека је сада p непаран прост број који дели z. Тада је $u^2 \equiv qw^2 (mod\ p)$. Нека је w^{-1} инверз за w по модулу p. Дакле $q \equiv (uw^{-1})^2 \pmod{p}$, тј. $\left(\frac{q}{p}\right) = 1$ (Лежандров симбол). Како је $q \equiv 1 \pmod{4}$, на основу квадратног закона реципроцитета важи и да је $\left(\frac{p}{q}\right) = 1$ из чега следи да за све непарне p, $p \mid z$. Како је $q \equiv 1 \pmod{8}$, такође имамо и да је $\left(\frac{2}{q}\right) = 1$ и да је $\left(\frac{-1}{q}\right) = 1$. Због мултипликативне особине Лежандровог симбола, следи да је $\left(\frac{z}{q}\right) = 1$, што значи да је z^2 ненула четврти степен по модулу q.

Дакле имамо да је $u^2 \equiv dz^2 \ (mod\ q)$, и знамо да су u^2 и z^2 четврти степени по модулу q, па следи да је d четврти степен по модулу q. □

Дакле, да бисмо добили контрапримере потребно је да d не буде четврти степен по модулу q.

Сада посматрајмо систем хомогених Диофантових једначина:

$$U^2 - qW^2 = dZ^2, \qquad UW = V^2 \tag{4.3.1}$$

где су задовољени следећи услови:

(1) q прост број такав да $q \equiv 1 \ (mod\ 16)$;
(2) d је ненула, бесквадратан и није дељив са q;
(3) d је квадрат, али такав да није четврти степен по модулу q и
(4) q је четврти степен по модулу p за сваки непаран прост број p који дијели d

Пропозиција 4.3.1 и Лема 4.3.2 нам дају следећи резултат:

Теорема 4.3.3 *Систем (4.3.1) је локално решив, али није глобално решив, тј. систем нема нетривијалних* $\mathbb{Z}$ *решења.* □

Пример 4.3.4 Линдов и Ричардов пример, први познати контрапример Хасеовог принципа је следећи специјалан случај Теореме 4.3.3:

$$U^2 - 17W^2 = 2Z^2, \qquad UW = V^2$$

Ово је контрапример с обзиром да $2 \in (F_{17}^x)^2$ али $2 \notin (F_{17}^x)^4$.[1]

Пример 4.3.5. Нека је q прост број такав да $q \equiv 1 \ (mod\ 16)$ и такав да 2 није четврти степен по модулу q. У овом случају је $\left(\frac{2}{q}\right) = 1$, па следећи систем представља контрапример Хасеовог принципа

$$U^2 - qW^2 = 2Z^2, \qquad UW = V^2$$

Заправо, треба само претпоставити да је $q \equiv 1 \ (mod\ 8)$ пошто је $(1, 1, 1, 2)$ јако решење по модулу 16 ако је $q \equiv 9 \ (mod\ 16)$. Такође приметимо да је овај скуп примера бесконачан. Заправо, густина простих бројева q за $q \equiv 1 \ (mod\ 8)$ таквих да 2 није четврти степен по модулу q је $1/8$. Ово се види применом Чеботаријеве теореме о густини на проширење $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ чија је Галоаова група група диедара реда 8.[1]

Пример 4.3.6 Ако $d \neq 2$ следећи систем представља контрапример Хасеовог принципа

$$U^2 - 17W^2 = 19Z^2, \qquad UW = V^2$$

Глава 5

5 Теорија елиптичких кривих

5.1 Увод у елиптичке криве

Сада ћемо укратко дефинисати елиптичке криве како би што лакше разумели још једну групу контрапримера Хасеовог принципа а ти контрапримери одговарају нетривијалним елементима Тејт-Шафаревичевих група одређених елиптичких кривих. За више детаља, читалац се упућује на [15].

Алгебарске криве представљају скуп тачака у равни које се могу дефинисати алгебарским изразом: $f(x,y)=0$. Елиптичке криве представљају фамилију *глатких* алгебарских кривих, па је њихов први извод дефинисан у свакој тачки домена криве. Потребно је нагласити да елиптичке криве немају никакве везе са елипсама или другим конусним пресецима. Конусни пресеци су алгебарске криве другог реда, а елиптичке криве су алгебарске криве трећег реда. Ред криве је највећи степен агебарског израза који је дефинише. Алгебарске криве трећег реда могу се јавити у различитим облицима и дефинишу се над алгебарском структуром коју називамо поље.

Нека је K поље. Елиптичка крива E над пољем K (у ознаци E/K) је несингуларна пројективна кубна крива над K са бар једном (K-рационалном) тачком. Она има афину једначину облика:

$$F(x,y)=ax^3+bx^2y+cxy^2+dy^3+ex^2+fxy+gy^2+hx+iy+j=0 \qquad (5.1.1)$$

где $a,b,c,\dots.j\in K$, а несингуларност значи да је у свакој тачки на кривој, посматраној у пројективној равни $\mathbb{P}^2(\overline{K})$ над алгебарским затворењем од K, бар један парцијални извод функције F различит од нуле. Свака једначина облика (5.1.1) може се трансформацијама свести на облик

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

који називамо Вајерштрасова форма. Даље, ако је карактеристика поља K, $char\ K\neq 2{,}3$, онда се једначина може свести на облик

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

који називамо кратка Вајерштрасова форма. Подсетимо се, карактеристика поља K је најмањи природан број n, такав да је $1+1+\cdots+1=n\cdot 1=0$, где су 0,1 неутрални елементи за сабирање, односно множење у K.
Због услова о несингуларности, кубни полином $f(x)=x^3+ax+b$ нема вишеструких нула (у алгебарском затворењу $\overline{K}$), а то је еквивалетно услову да је дискриминанта $D=-4a^3-27b^2\neq 0$.

Дакле, елиптичку криву над пољем K (карактеристике различите од 2 и 3) можемо замишљати као скуп тачака $(x, y) \in K \times K$, који задовољавају једначину $E: y^2 = x^3 + ax + b$, где су $a, b \in K$ и $D = 4a^3 + 27b^2 \neq 0$, плус "тачка у бесконачности O". Тај скуп ћемо означавати са $E(K)$.

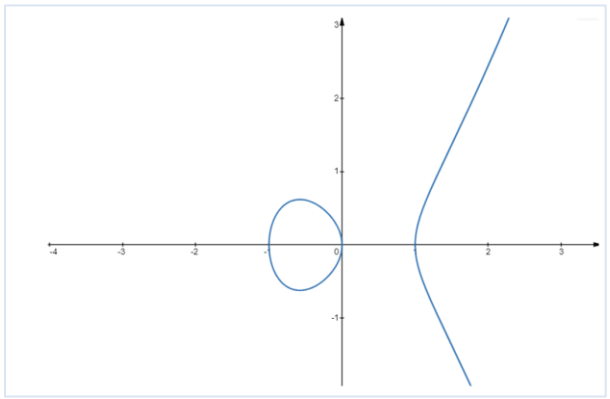
Објаснимо сада појам тачке у бесконачности O. Уколико елиптичку криву прикажемо у пројективној равни, тачка у бесконачности се појављује природно.
Пројективну раван $\mathbb{P}^2(K)$ добијемо тако што на скупу $K^3 \setminus \{(0,0,0)\}$ уведемо релацију еквиваленције $(X, Y, Z) \sim (kX, kY, kZ), k \in K, k \neq 0$. Ако у афиној једначини елиптичке криве уведемо смену: $x = \frac{X}{Z}, y = \frac{X}{Z}$, добијамо пројективну криву:

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

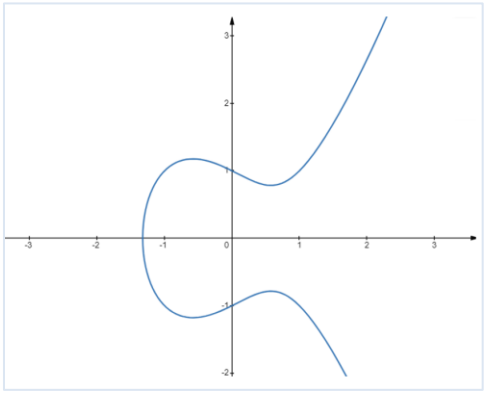
ако је $Z \neq 0$, онда класа еквиваленције (X, Y, Z) има представника $(x, y, 1)$, па ту класу еквиваленције можемо поистоветити са (x, y). Међутим, уколико је $Z = 0$, тада та класа еквиваленције има представника $(0,1,0)$ и ту класу можемо поистоветити са тачком у бесконачности O.

Нека је E елиптичка крива. Једно од најважнијих својстава елиптичких кривих јесте да се над њима може дефинисати бинарна операција, тако да тачке на елиптичкој кривој са задатом операцијом чине Абелову групу. Ову операцију обично називамо сабирањем.Тачка у бесконачности O ће бити неутрални елемент, тако да је $P + O = O + P = P, \forall P \in E$.

Нека је $K = \mathbb{R}$ поље реалних бројева. Тада елиптичку криву над пољем $\mathbb{R}$ (без тачке у бесконачности) можемо приказати као подскуп у равни. Полином $f(x) = x^3 + ax + b$ може имати или 1 или 3 корена. У зависности од тога, график припадајуће елиптичке криве има једну или две компоненте, као што је приказано на слици испод.



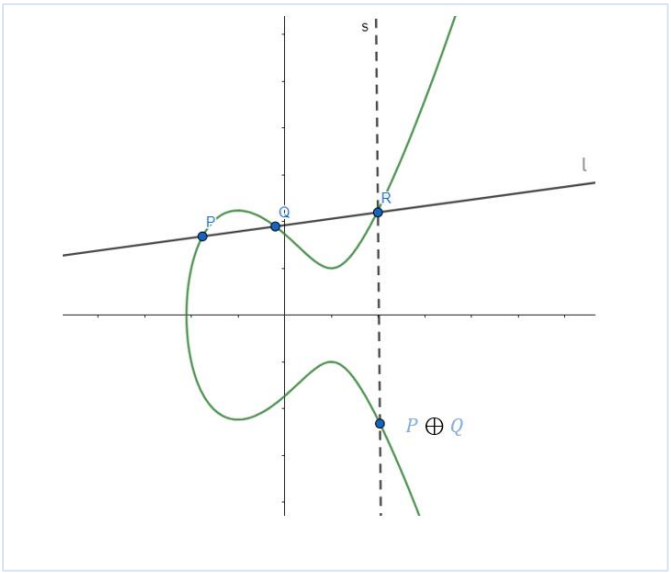
Слика 2. $y^2 = x^3 - x$, *две компоненте*



Слика 3. $y^2 = x^3 - x + 1$, *једна компонента*

Посматрајмо сада две различите тачке $P(x_1, y_1), Q(x_2, y_2) \in E(\mathbb{R})$. Познато је да се кроз две тачке у равни може провући тачно једна права. Поставимо праву l тако да садржи те две тачке. Очигледно је да права l сече график елиптичке криве. Коефицијент праве l је $k = \tan\alpha = \frac{y_2 - y_1}{x_2 - x_1}$.

У општем случају, права l ће пресећи график елиптичке криве у још једној тачки. Означимо ту тачку са R. Сада, постављамо праву s, тако да она садржи тачку R и тако да је паралелна са y-осом, при чему је нормална на x-осу. Пресек праве s и графика елиптичке криве означимо са $-R$. Очигледно је ова тачка симетрична тачки R у односу на x-осу. На овај начин дефинисано је сабирање тачака елиптичке криве, односно елемената скупа $E(\mathbb{R})$. Тачка $-R$ представља збир тачака P и Q и такође се налази на графику елиптичке криве. Из наведеног може се закључити да је скуп $E(\mathbb{R})$ затворен у односу на сабирање. Збир два елемента $P, Q \in E(\mathbb{R})$ записује се као $P \oplus Q$ или $P + Q$. (*Слика 4.*)



Слика 4. Графичка интерпретација сабирања две тачке елиптичке криве

Ако је $P = Q$, онда би уместо праве l, повукли тангенту кроз тачку P. По дефиницији стављамо да је $P + O = O + P = P, \forall P \in E(\mathbb{R})$. Дакле, операција сабирања на скупу $E(\mathbb{R})$ се уводи "геометријски", тако да су 3 тачке на кривој E колинеарне акко је сума једнака неутралном елементу O. Дакле, могу се формулисати следећа правила приликом сабирања тачака елиптичких кривих. Нека је $P = (x_1, y_1), Q = (x_2, y_2)$. Тада је:

1) $-O = O$
2) $-P = (x_1, -y_1)$
3) $O + P = P$
4) ако је $Q = -P$ онда је $P + Q = O$
5) ако је $Q \neq -P$ онда је $P + Q = (x_3, y_3)$ где је $x_3 = \lambda^2 - x_1 - x_2,\ y_3 = -y_1 + \lambda(x_1 - x_3)$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & x_2 \neq x_1 \\ \dfrac{3x_1^2 + a}{2y_1}, & x_2 = x_1 \end{cases}$$

λ је коефицијент правца праве кроз P и Q, односно тангенте у тачки P у случају $P = Q$.

Показује се да је $(E(K), +)$ Абелова група. Сва својства Абелове групе су очигледна, осим асоцијативности чији је доказ нешто компликованији.

Напомена: елиптичке криве над пољем $\mathbb{Z}_p$, где је p прост број, се дефинишу аналогно као над пољем реалних бројева, али се операције изводе по модулу p.

5.2 Изогенија, Галоаова кохомологија, Селмерова и Тејт-Шафаревичева група

Сада ћемо навести основне дефиниције изогенија и Галоаове кохомологије, како би лакше разумели дефиницију Селмерове и Тетј-Шафаревичеве групе. За више детаља, читалац се упућује на [15].

Дефиниција 5.2.1 *Нека су E и E' две алгебарске криве над пољем K. Пресликавање $\phi: E \to E'$ је рационално пресликавање ако је дефинисано рационалним функцијама: $\phi = (u, v), u, v \in K(E')$, такво да u и v нису обоје нула, тј. $\phi(P) = (u(P), v(P))$ за $P \in E(K)$. ϕ је морфизам, ако је дефинисан на целој E' (или се може проширити).*

Дефиниција 5.2.2 *Изогенија између две елиптичке криве је морфизам: $\phi: E \to E'$ који пресликава $O \in E$ у $O' \in E'$. Две елиптичке криве E и E' су изогене ако постоји изогенија $\phi: E \to E'$ таква да је $\phi(E') \neq 0$, односно ако је ϕ нетривијално.*

Дефиниција 5.2.3 *За свако $m \in \mathbb{N}$, изогенија множења са m на $E(K)$ је дефинисана на следећи начин:*

$$[m]: E(K) \to E(K)$$
$$P \to \underbrace{P + \cdots + P}_{m}$$

Дефиниција 5.2.4 *Нека је $m \in \mathbb{Z}$ и $m \geq 2$. m-торзиона подгрупа од $E(K)$ је дефинисана са*

$$E(K)\,[m] = \{P \in E(K): [m]P = O\}.$$

Са $E_{tors}(K)$ ћемо означавати тачке коначног реда у E, тј. $E_{tors}(K) = \bigcup_{m=2}^{\infty} E(K)\,[m]$.

Теорема 5.2.5 (Мордел-Вејлова) *Ако је K бројевно поље и E/K елиптичка крива, тада је група $E(K)$ коначно генерисана.* □

Из фундаменталне теореме о коначно генерисаним Абеловим група следи да је $E(K) \cong E_{tors}(K) \times \mathbb{Z}^r$, где је $E_{tors}(K)$ коначна група и r ненегативан цео број. r се назива рангом групе $E(K)$.

Теорема 5.2.6 (Мордел-Вејлова, слабија верзија) *Ако је K бројевно поље и E/K елиптичка крива, и $m \geq 2$ тада је $E(K)/m\,E(K)$ коначна група.* □

Доказ ове теореме се може пронаћи у [15].

Дефиниција 5.2.7 *Нека је K савршено поље и нека је $\overline{K}$ алгебарско затворење поља K, и нека је $Gal(\overline{K}/K)$ Галоаова група поља $\overline{K}$ над K. Група $Gal(\overline{K}/K)$ је инверзни лимес група $Gal(L/K)$ када L пролази кроз сва коначна Галоаова раширења поља K. Према томе, $Gal(\overline{K}/K)$ је профинитна група, па има топологију чија се база отворених скупова састоји од колекције нормалних подгрупа са коначним индексом у $Gal(\overline{K}/K)$.*

Дефиниција 5.2.8 $Gal(\overline{K}/K)$ *модул је Абелова група A, таква да је дејство $Gal(\overline{K}/K)$ непрекидно на A у односу на профинитну топологију на $Gal(\overline{K}/K)$ и дискретну топологију на A.*

Дефиниција 5.2.9 *Нулта кохомолошка подргрупа $Gal(\overline{K}/K)$ модула A је група $Gal(\overline{K}/K)$ инваријатних елемената у A:* $H^0(\,Gal(\overline{K}/K), A) = \{a \in A : a^\sigma = a \text{ за свако } \sigma \in Gal(\overline{K}/K)\}$.

Дефиниција 5.2.10 *Група непрекидних 1-коциклова из $Gal(\overline{K}/K)$ у A је група* $Z^1_{cont}(Gal(\overline{K}/K), A) = \{\xi : Gal(\overline{K}/K) \to A : \xi \text{ непрекидно и } \xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau)\}$.

Дефиниција 5.2.11 *Група 1-кограница из $Gal(\overline{K}/K)$ у A је група* $B^1(Gal(\overline{K}/K), A) = \{\xi : Gal(\overline{K}/K) \to A : \text{ако постоји } a \in A, \text{такво да } \xi(\sigma) = a^\sigma - a \text{ за све } \sigma \in A\}$.

Како A има дискретну топологију, свака кограница је аутоматски непрекидна, па се може лако проверити да је $B^1(Gal(\overline{K}/K), A)$ подгрупа (заправо, нормална подргрупа) $Z^1_{cont}(Gal(\overline{K}/K), A)$.[14]

Дефиниција 5.2.12 *Прва кохомолошка група $Gal(\overline{K}/K)$ модула A је група :* $H^1(\,Gal(\overline{K}/K), A) = Z^1_{cont}(Gal(\overline{K}/K), A)/B^1(Gal(\overline{K}/K), A)$.

$Gal(\overline{K}/K)$ дејствује на тачке $E(\overline{K})$ на следећи начин: $\sigma(O) = O,\ \sigma(x, y) = (\sigma(x), \sigma(y))$ где је $P = (x, y) \in E(\overline{K})$ и $\sigma \in Gal(\overline{K}/K)$.

Свака ненула изогенија ϕ индукује тачан низ $Gal(\overline{K}/K)$ модула облика

$0 \to E(\overline{K})[\phi] \to E(\overline{K}) \xrightarrow{\phi} E'(\overline{K}) \to 0$ где је $E(\overline{K})[\phi] = ker\phi$.

Овај низ се може проширити на низ између кохомолошких група:

$$0 \to H^0(Gal(\overline{K}/K), E(\overline{K})[\phi]) \to H^0(Gal(\overline{K}/K), E(\overline{K})) \xrightarrow{\phi} H^0(Gal(\overline{K}/K), E'(\overline{K})) \xrightarrow{\delta}$$

$$\xrightarrow{\delta} H^1(Gal(\overline{K}/K), E(\overline{K})[\phi]) \to H^1(Gal(\overline{K}/K), E(\overline{K})) \xrightarrow{\phi} H^0(Gal(\overline{K}/K), E'(\overline{K}))$$

па из дефиниције нулте кохомолошке групе, следи да је:

$$0 \to E(K)[\phi] \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(Gal(\overline{K}/K), E(\overline{K})[\phi]) \to$$

$$\to H^1(Gal(\overline{K}/K), E(\overline{K})) \xrightarrow{\phi} H^0(Gal(\overline{K}/K), E'(\overline{K}))$$

Штавише, из овог низа можемо извести фундаментални кратки тачан низ

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(Gal(\overline{K}/K), E(\overline{K})[\phi]) \to H^1(Gal(\overline{K}/K), E(\overline{K}))[\phi] \to 0 \qquad (5.2.1)$$

Дефиниција 5.2.13 *Нека је E/K елиптичка крива. Хомогени простор елиптичке криве E/K је глатка крива C/K дефинисана над пољем K заједно са транзитивним дејством алгебарске групе E на C. Другим речима хомогени простор елиптичке криве E/K је пар (C, μ), при чему је C/K глатка крива дефинисана над K и $\mu: C \times E \to C$ је морфизам варијетета дефинисан над K који има следећа својства:*

- $\mu(p, O) =$ P *за све* $p \in$ C ;
- $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ *за све* $P, Q \in$ E *и* $p \in$ C;
- *За све* $p, q \in$ C *постоји јединствени* P $\in$ E *таква да је* $\mu(p, P) = q$.

Дефиниција 5.2.14 *Два хомогена простора C/K и C'/K елиптичке криве E/K су еквивалентна ако постоји изоморфизам $\Phi: C \to C'$ који је дефинисан над K, и који се слаже са дејством групе* E *на* C *и* C′*, тј. $\Phi(p + P) = \Phi(p) + P$ за све $P \in$ E *и* $p \in$ C. *Колекција свих класа еквиваленције хомогених простора елиптичке криве E/K назива се Вејл-Шателе група и означава се са $WC(E/K)$.*

Тврђење 5.2.15 *Нека је E/K елиптична крива, тада постоји бијекција скупова $WC(E/K) \to H^1(Gal(\overline{K}/K)\ ), E(\overline{K}))$.* □

Тврђење 5.2.16 *Нека је C/K хомогени простор елиптичке криве E/K. Тада C/K припада тривијалној класи у $C(E/K)$ акко $C(K) = \emptyset$.* □

Сада ћемо прецизније дефинисати Селмерову и Тејт-Шафаревичеву групу.

Позивамо се на кратки тачан низ (5.2.1)

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(Gal(\overline{K}/K), E(\overline{K})[\phi]) \to H^1(Gal(\overline{K}/K), E(\overline{K}))[\phi] \to 0$$

тј.

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(Gal(\overline{K}/K), E[\phi]) \to H^1(Gal(\overline{K}/K), E)[\phi] \to 0$$

где смо $E(\overline{K})$ заменили са E, тј. ако пишемо E, без поља, мислимо на групу $E(\overline{K})$.

група $H^1(Gal(\overline{K}/K), E)$ се може поистоветити са $WC(E/K)$. Нека је M_K скуп свих нееквивалентних апсолутних вредности на K. Све групе изнад, које су дефинисане над пољем K, можемо утопити у аналогну групу дефинисану над локалним пољем K_v, за све $v \in M_K$. Приметимо да ако $E(K)$ има неку тачку, тада је та тачка дефинисана и над $\prod_{v \in M_K} E(K_v)$.

Аналогно важи и за кохомолошке групе из наведених тачних низова. Са G_v ћемо означавати подгрупу од $Gal(\overline{K}/K)$ која фиксира v, па онда делује и на K_v и $E(K_v)$. Пребацивањем K у K_v добија се кратки тачан низ:

$$0 \to E'(K_v)\ /\phi(E(K_v)) \xrightarrow{\delta} H^1(G_v, E[\phi]) \to H^1(G_v, E)[\phi] \to 0$$

Група $H^1(G_v; E[\phi])$ је коначна(ово је један од кључних корака у доказу Мордел-Вејлова, слабије верзије) те се $H^1(Gal(\overline{K}/K), E[\phi])$ може утопити у њу. Означимо са $G := Gal(\overline{K}/K)$, па се спајањем тачних низова над K и K_v може добити следећи комутативни дијаграм:

$$\begin{array}{ccccccccc} 0 & \to & E'(K)\ /\phi(E(K)) & \xrightarrow{\delta} & H^1(G, E[\phi]) & \to & WC(E/K)[\phi] & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \prod_{v \in M_k} E'(K_v)\ /\phi(E(K_v)) & \xrightarrow{\delta} & \prod_{v \in M_k} H^1(G_v, E[\phi]) & \to & \prod_{v \in M_k} WC(E/K_v)[\phi] & \to & 0, \end{array}$$

где смо заменили $H^1(G; E)$ са $WC(E/K)$. Један од главних циљева теорије елиптичких кривих јесте налажење слике количника $E'(K)/\phi(E(K))$ у групи $H^1(G, E[\phi])$, што је еквивалентно са налажењем језгра пресликвања

$$H^1(G, E[\phi]) \to WC(E/K)[\phi]$$

Ово је еквивалентно са проверавањем да ли одређени хомогени простори садрже рационалну K тачку. Овај проблем се може посматрати над локалним пољима. Наиме, на аналоган начин као за глобална поља, проблем налажења локалног језгра

$$Ker\ (H^1(G_v, E[\phi]))\ \to\ WC(E/K_v)[\phi])$$

се своди на налажење K_v, рационалне тачке на одређеним хомогеним просторима.

Сада можемо увести дефиницију Селмерове и Тејт-Шафаричеве групе

Дефиниција 5.2.17 *Нека је $\phi: E/K \to E'/K$ изогенија елиптичких кривих. Тада је ϕ -Селмерова група E/K подгрупа од $H^1(Gal(\overline{K}/K), E[\phi])$ дефинисана са*

$$S^{\phi}(E/\text{К}) = Ker\ \{H^1(Gal(\overline{K}/K), E[\phi])\ \to \prod_{v \in M_K} WC(E/\text{К}_v)\}.$$

Тејт-Шафаревичева група E/K је подгрупа од $WC(E/K)$ дефинисана са

$$\text{Ш}(E/\text{К}) = Ker\{WC(E/\text{К}) \to \prod_{v \in M_K} WC(E/\text{К}_v)\}.$$

Тејт-Шафаревичева група може да се види као група класа еквиваленције хомогених простора за E/K чији хомогени простори садрже К_v рационалну тачку за свако $v \in M_K$.За $K = \mathbb{Q}$ елементи $\text{Ш}(E/\mathbb{Q})$ се могу замишљати као класе хомогених простора који не задовољавају Хасеов принцип. Селмерову групу можемо замишљати као свуда локално решиве хомогене просторе. Тачније, то су 1-коциклови који се пресликавају у такве хомогене просторе. Додатно, нетривијалне елементе од

Ш$(E/\text{К})$ можемо замишљати као хомогене просторе који имају локалну тачку свуда, али немају глобалну.

Теорема 5.2.18 $\phi: E/K \to E'/K$ *изогенија елиптичких кривих дефинисаних над* K. *Тада важи:*

1. Постоји тачан низ $0 \to E'(K)/\phi(E(K)) \to S^{\phi}(E/\text{К}) \to \text{Ш}(E/\text{К})[\phi] \to 0$

2. Група $S^{\phi}(E/\text{К})$ *је коначна.* □

Како добити елементе Ш$(E/\text{К})[\phi]$? Дајемо скицу једног примера:

Пример 5.2.19 Нека је E елиптичка крива дефинисана са: $E: y^2 = x^3 + px$, и нека је $p \equiv 1\ (mod\ 8)$ такав да 2 није четврти степен по модулу p, тада је ранг од $E(\mathbb{Q}) = 0$, те је Ш$(E/\text{К})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

Доказ: Елементи Ш$(E/\text{К})[2]$ су хомогени простори: $y^2 = 4px^4 - 1$ и $\pm y^2 = 2px^4 - 2$. Можемо показати да $C: y^2 = 2 - 2px^4$ нема тачке у $\mathbb{Q}$. Претпоставимо супротно, тј. нека је (x, y) тачка на кривој, и нека је $x = r/t$, где су r, t узајамно прости бројеви. Тада је $y^2 = \frac{2t^4 - 2pr^4}{t^4}$, па како именилац и бројилац немају заједнички фактор, $2t^4 - 2pr^4$ мора бити квадрат (парног) целог броја. Дакле, постоји цели број m такав да је $2m^2 = t^4 - pr^4$. Нека је q прост број који дели m. Тада је $t^4 \equiv pr^4\ (mod\ q)$, па је $\left(\frac{p}{q}\right) = 1$, па на основу квадратног закона реципроцитета важи да је $\left(\frac{q}{p}\right) = 1$, те да је $\left(\frac{2}{p}\right) = 1$ па су сви прости фактори од m квадрати по модулу p. Дакле m^2 је четврти степен по модулу p. Једначина $2m^2 \equiv t^4 (mod\ p)$ даље показује да је 2 четврти степен по модулу p, што је контрадикција са почетном хипотезом. Дакле, крива C нема тачака у $\mathbb{Q}$.

5.3 Веза између система квадратних једначина и елиптичких кривих

Посматрајмо сада систем квадратних једначина

$$aU^2 + bV^2 + cW^2 = dZ^2, \qquad UW = V^2 \tag{5.3.1}$$

где су $a, b, c, d \in \mathbb{Z}$, такви да $a, c, d \neq 0$ и $b^2 - 4ac \neq 0$.

Систем (5.3.1) заправо дефинише несингуларну пројективну криву рода 1, дат као пресек квадратних површи. Такве криве рода 1 настају природно у поступку спуста 2. реда који се користи за проналажење генератора и ранга за групу рационалних тачака E($\mathbb{Q}$) елиптичке криве E. Систем (5.3.1) је прилагођен случају где је E дефинисано над $\mathbb{Q}$ и поседује најмање једну $\mathbb{Q}$ - рационалну торзију 2.реда, а питање постојања нетривијалних $\mathbb{Z}$-решења играју важну улогу у поступку спуста 2. реда .[1]

Веза између система (5.3.1) и елиптичких кривих се јавља када је (5.3.1) контрапример Хасеовом принципу. У том случају, (5.3.1) представља елемент реда 2 Тејт–Шафаревич групе Ш$(E/\text{К})$ елиптичне криве E дефинисане једначином $y^2 = x^3 - 2bdx^2 + (b^2 - 4ac)d^2x$.

Линдов и Ричардов контрапример $U^2 - 17W^2 = 2Z^2,\ UW = V^2$, представља елемент реда 2 у Тејт-Шафаревичевој групи где је E дефинисан једначином $y^2 = x^3 - 2^4 17x$.

Велики део проучавања локалне решивости разматран у главном делу рада се проширује на систем (5.3.1). На пример, Последицу 4.2.6 можемо генерализовати на следећи начин:

Теорема 5.3.1 *Систем (5.3.1) је p-локално решив за све просте $p \nmid 2acd(b^2 - 4ac)$.*

За доказ ове теореме, биће нам потребне следеће две леме.

Лема 5.3.2 *Нека је p непаран прост број, и посматрајмо систем*

$$aU^2 + bV^2 + cW^2 = dZ^2, \qquad UW = V^2$$

где $a, b, c, d \in \mathbb{F}_p$ и $acd(b^2 - 4ac) \neq 0$. Систем има нетривијална $\mathbb{F}_p$ решења.

Доказ: Множењем прве једначине са d^{-1}, сводимо на случај $d = 1$. Сада користимо технику попуњавања квадрата на $f(X, Y) = aX^2 + bXY + cY^2$. Нека су $q_1, q_2, q_3 \in \mathbb{F}_p[T]$ дати као у Леми 4.1.6 примењеној на $aX^2 + \left(c - \frac{b^2}{4a}\right)Y^2 = Z^2$, па је $aq_1^2 + \left(c - \frac{b^2}{4a}\right)q_2^2 = q_3^2$.
Ако је $q_1' = q_1 - \frac{b}{2a}q_2$ тада је $f(q_1', q_2) = a(q_1 - \frac{b}{2a}q_2)^2 + b\left(q_1 - \frac{b}{2a}q_2\right)q_2 + c{q_2}^2 = a{q_1}^2 + \left(c - \frac{b^2}{4a}\right){q_2}^2 = {q_3}^2$. Како q_1 и q_2 нису асоцирани, q_1' је ненула, и q_1' и q_2 не могу бити асоцирани. На основу Леме 4.2.1 постоји $t \in \mathbb{F}_p$ такво да $\left(\frac{q_1'(t)}{p}\right) \neq -\left(\frac{q_2(t)}{p}\right)$, па је $q_1'(t)q_2(t) = s^2$ за неко $s \in \mathbb{F}_p$, и $q_1'(t)$ и $q_2(t)$ нису оба 0, па је $(q_1'(t), s, q_2(t), q_3(t))$ нетривијално решење. □

Лема 5.3.2 нам даје решења по модулу p. Како би дошли до $\mathbb{Z}_p$ решења, потребан нам је специјални случај Хенселове леме.

Лема 5.3.3 *Нека је p прост број који не дели $2ac(b^2 - 4ac)$, где $a, b, c \in \mathbb{Z}$. Ако $f(T) = aT^4 + bT^2 + c$ има корен по модулу p, тада f има корен у $\mathbb{Z}_p$.*

Доказ: Нека је $t \in \mathbb{Z}$ такво да $f(t) \equiv 0\ (mod\ p)$. Претпоставимо да $f'(t) \equiv 0\ (mod\ p)$, где је $f' = 4aT^3 + 2bT$. Другим речима, $-4at^3 \equiv 2bt\ (mod\ p)$. Приметимо да $t \not\equiv 0\ (mod\ p)$, јер је $f(0) = c$ и $p \nmid c$. Такође p је непаран прост број, па $-2at^2 \equiv b\ (mod\ p)$. Дакле, $0 \equiv -(4a)at^4 - (4a)bt^2 - (4a)c \equiv -b^2 + 2b^2 - 4ac \equiv b^2 - 4ac\ (mod\ p)$, што је контрадикција са нашом претпоставком. Дакле, $f'(t) \not\equiv 0\ (mod\ p)$, па доказ сада следи директно из Хенселове леме. □

Доказ Теореме 5.3.1: Нека је (u_0, v_0, w_0, z_0) примитивно решење система (5.3.1) по модулу p (Лема 5.3.2). Ако p дели и u_0 и w_0, тада p мора делити и v_0 и z_0 што је контрадикција са претпоставком да је (u_0, v_0, w_0, z_0) примитивно решење. На основу симетрије између U и W можемо претпоставити да су w_0 и p узајамно прости тј. да је w_0 јединица у $\mathbb{Z}_p$.
Нека је $u = u_0 w_0^{-1}$, $v = v_0 w_0^{-1}$, и $z = z_0 w_0^{-1}$ у $\mathbb{Z}_p$. Тада је $(u, v, 1, z)$ решење система по модулу p. Дакле, $u \equiv v^2$, па је $av^4 + bv^2 + c \equiv dz^2\ (mod\ p)$.
Размотримо прво случај када је $z \equiv 0\ (mod\ p)$. У овом случају v је корен по модулу p полинома $f(T) = aT^4 + bT^2 + c$, па на основу Лема 5.3.3 постоји $t \in \mathbb{Z}_p$ такво да је $f(t) = 0$ тј.$(t^2, t, 1, 0)$ је

решење система у $\mathbb{Z}_p$.
Претпоставимо сада да $z \not\equiv 0 \ (mod\ p)$. Тада је z корен по модулу p полинома
$f(T) = dT^2 - (av^4 + bv^2 + c)$, па је $f'(z) = 2dz \not\equiv 0 \ (mod\ p)$.
На основу Хенселове леме постоји $t \in \mathbb{Z}_p$ такво да је $f(t) = 0$, тј. $(v^2, v, 1, t)$ је решење система у $\mathbb{Z}_p$. □

6 Литература

[1] W. Aitken, F. Lemmermeyer, *Counterexamples to the Hasse principle*.

[2] Владимир Балтић, *Теорија бројева, Припреме за ЈБМО, 11. јун 2004*.

[3] В.Мићић, З.Каделбург, Д. Ђукић, *Увод у теорију бројева*, Друштво математичара Србије, Материјал за младе математичаре, свеска 15, четврто допуњено издање, Београд 2004.

[4] Иван Матић, *Увод у теорију бројева*, Предавања, Осијек, 2011.

[5] Горан Ђанковић, *Теорија бројева*, предавања, Математички факултет, 2018 https://vdocuments.mx/teorija-brojeva-djankovictb2018pdf

[6] Филип Најман, *Артиметичка геометрија*, Природословно математички факултет, Математички одсјек, 2015/2016.

[7] Bjorn Poonen, *Introduction to arithmetic geometry*, Notes from 18.782, Fall 2009.

[8] Keith Conrad, *Hensel's lema*, https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf

[9] Fernando Q. Gouvêa, *p-adic Numbers*: *An introduction*, Third Edition, Springer.

[10] Amélie Schinck, *The Local-Global Principle in Number Theory*, A Thesis in The Department of Mathematics and Statistics, September 2001.

[11] Keith Conrad, *The Local-Global principle*, https://kconrad.math.uconn.edu/blurbs/gradnumthy/localglobal.pdf

[12] Keith Conrad, *Selmer's example*, https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf

[13] Martin Bright, *Counterexamples to the Hasse principle*, 16 April.

[14] Alvaro Gonzalez Hernandez, *Local fields and the Hasse principle*, MSc in Mathematical Sciences, Trinity Term 2021.

[15] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd Edition, Springer, 2009.

[16] Sameer Kailasa, *On the Tate-Shafarevich Group of a Number Field*, https://math.uchicago.edu/~may/REU2016/REUPapers/Kailasa.pdf

[17] Филип Најман, *Елиптичке кривуље над пољима алгебарских бројева*, Природословно математички факултет, Математички одсјек, 2013.

[18] Андреј Дујелла, *Алгоритми за елиптичке кривуље*, https://www.researchgate.net/publication/260351103_Algoritmi_za_elipticke_krivulje