МАТЕМАТИЧКА ГИМНАЗИЈА

МАТУРСКИ РАД

из предмета

Математика

на тему

Елиптичке криве

Ученик:
Никола Јешић, IV_d

Ментори:
Стеван Гајовић,
Милош Ђорић

Београд, мај 2018.

Садржај

1 Увод

Теорија и решавање Диофантових[1] једначина је један од најстаријих проблема у математици. То су једначине облика

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

при чему тражимо решења у скупу рационалних или целих бројева. При решавању обично тражимо одговор на следећа питања:

- Има ли решења у скупу целих бројева?
- Има ли решења у скупу рационалних бројева?
- Има ли бесконачно много решења у скупу целих бројева?
- Има ли бесконачно много решења у скупу рационалних бројева?

Једна од најпознатијих Диофантових једначина је Велика Фермаова[2] теорема која каже да једначина

$$x^n + y^n = z^n, \quad n \geq 3$$

нема нетривијалних целобројних решења. Ова једначина је мучила математичаре преко 350 година и један од кључних делова у доказу који је извео Ендру Вајлс[3] 1995. године је управо било коришћење уопштења теорије којом ћемо се ми бавити у овом раду. Ми ћемо моћи да докажемо Велику Фермаову теорему за случајеве $n = 3, 4$.
Елиптичке криве имају великих примена како у теорији бројева, тако и у криптографији тако да је њихово проулавање изузетно корисно и значајно.

[1] Diophantus (око 250. г.)– грчки математичар.
[2] P. Fermat (1601-1665)– француски математичар.
[3] A. J. Wiles (1953-)– британски математичар.

2 Диофантове једначине

Дефиниција 2.1. Диофантова једначина је полиномска једначина са целобројним коефицијентима једне или више променљивих.

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

2.1 Диофантове једначине са једном променљивом

Диофантове једначине са једном променљивом су заправо полиноми једне променљиве са целобројним коефицијентима и знамо све што се тиче њиховиих рационалних решења. То нам говори Гаусова[4] лема.

Теорема 2.1.1. Ако је рационалан број $x = \frac{p}{q}$ решење једначине $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$ са целобројним коефицијентима, где су p и q узајамно прости, онда $p|a_0$ и $q|a_n$.

Доказ. Ако заменимо $x = \frac{p}{q}$ у једначину и помножимо је са q^n добијамо

$$a_n p^n + a_{n-1}p^{n-1}q + ... + a_1 pq^{n-1} + a_0 q^n = 0$$

Сви сабирци осим првог имају чинилац q, а сви осим последњег чинилац p, па уз $(p, q) = 1$ следи $p|a_0$ и $q|a_n$. □

Дакле, за Диофантове једначине са једном променљивом постоји алгоритам помоћу кога у коначном времену налазимо сва рационална решења.

2.2 Диофантове једначине са две променљиве првог степена

Диофантова једначина са две променљиве првог степена је једначина облика

$$ax + by + c = 0$$

где су a,b и c цели бројеви, бар један од њих различит од нуле. О рационалним решењима овакве једначине такође знамо све, има их бесконачно много и она су облика

$$(t, -\frac{c + at}{b}), \quad t \in \mathbb{Q},$$

за нпр. $b \neq 0$. Ако $(a, b) \nmid c$ целобројних решења нема, а у супротном их налазимо на следећи начин: Познато је да постоје цели бројеви α и β тако да важи

$$a\alpha + b\beta = (a, b)$$

Овиме добијамо једно целобројно решење полазне једначине $(x_0, y_0) = (\frac{-c\alpha}{(a,b)}, \frac{-c\beta}{(a,b)})$, помоћу кога градимо опште решење које гласи:

$$(x_0 + bt, y_0 - at), \quad t \in \mathbb{Z}$$

.

Дакле за Диофантове једначине са две променљиве првог степена, постоји поступак помоћу кога налазимо сва рационална решења.

[4] J. K. F. Gauss (1777-1855) – немачки математичар.

2.3 Диофантове једначине са две променљиве другог степена

Дефиниција 2.2. Тачка у (x, y) равни је рационална тачка ако су јој обе координате рационални бројеви.

Дефиниција 2.3. Права у (x, y) равни је рационална права ако њена једначина има рационалне коефицијенте, тј. права $ax + by + c = 0$ је рационална ако су a,b,c рационални бројеви.

Диофантова једначина другог степена са две променљиве је једначина облика

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

што је заправо једначина конике. Конику ћемо звати рационалном ако се њена једначина може записати помоћу рационалних коефицијената. Посматрајмо пресек рационалне конике са рационалном правом. У општем случају постоје две тачке пресека које очигледно не морају бити рационалне, међутим ако је једна тачка пресека рационална онда је то и друга (ово важи на основу Вијетових[5] формула). Ово својство конике нам пружа веома једноставан начин да пронађемо сва рационална решења. Наиме, пронађемо једну рационалну тачку O на коници и изаберемо било коју рационалну праву p у равни паралелну тангенти на конику у O. Затим сапајамо сваку рационалну тачку са p са O. Те нове праве су рационалне и секу конику у рационалним тачкама. Очигледно постоји бијекција између скупа рационалних тачака са p и скупа рационалних тачака са конике, не укључујући O (O се слика у бесконачну тачку).
Показаћемо ово на примеру кружнице.

$$x^2 + y^2 = 1$$

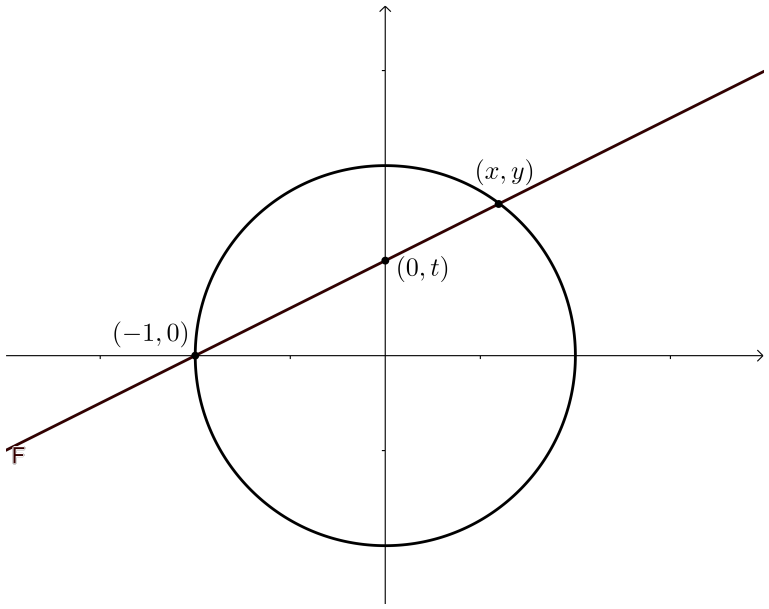
Уочимо тачку O $(-1, 0)$ и пројектујмо кружницу на y осу. Нека слика пројекције има координату $(0, t)$. Тада права која је спаја са O има једначину $y = t(1+x)$. Пронађимо пресек те праве и кружнице.

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

Једно решење је тачка O па када скратимо са $1 + x$ добијамо координате друге тачке пресека:

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

Заправо смо добили једну од могућих параметризација круга и на сличан начин се свака коника која има рационално решење може параметризовати.



Слика 1: Параметризација круга

[5] F. Viete (1540-1603)– француски математичар.

Остало нам је још да проверимо да ли коника има рационално решење. Ако посматрамо једначину

$$ax^2 + by^2 = c$$

да бисмо прешли на решавање у $\mathbb{Z}$ уводимо смену $x = X/Z$ и $y = Y/Z$. Постоји општи метод који даје одговор на претходно питање и то помоћу Лежандрове[6] теореме која тврди да једначина

$$aX^2 + bY^2 = cZ^2$$

има нетривијално целобројно решење ако и само ако конгруенција

$$aX^2 + bY^2 \equiv cZ^2 \pmod{m}$$

има решење узајамно просто са m, где је m број који на одређени начин зависи од a, b и c. Ми се овиме нећемо дубље бавити али радознали читаоци могу погледати матурски рад Уроша Миленковића.

Што се тиче Диофантових једначина другог степена са две променљиве преостало нам је да прокоментаришемо проналажење целобројних решења. Теорија Пелове[7] једначине потпуно решава проблем једначина облика:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

али се ми нећемо дубље бавити тиме.

[6] A. M. Legendre (1752-1833)– француски математичар.
[7] J. Pell (1611-1685)– енглески математичар.

3 Кубичне криве

Једначина облика

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

је једначина кубичне криве и њено проучавање је главна тема овог рада. Наш циљ је да нађемо сва њена рационална и сва њена целобројна решења.
Шта се добија у пресеку рационалне праве и кубике? У општем случају то су три тачке од којих ни једна не мора бити рационална, међутим, као код коника, ако су две рационалне онда је то и трећа. Такође, ако у рационалној тачки повучемо тангенту на криву, она ће је сећи у рационалној тачки (рачунамо да права која тангира криву сече криву у тачки додира бар два пута)
Проучавање ових кривих је веома старо. Нпр. Бахе[8] је, решавајући проблем представљања броја као разлике квадрата и куба:

$$y^2 - x^3 = c$$

извео поступак за проналажење бесконачно много рационалних решења полазећи од једног (x, y), тзв. формула дуплирања:

$$(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3})$$

На пример за једначину

$$y^2 - x^3 = -2$$

полазећи од решења $(3, 5)$ можемо их добити бесконачно:

$$(3,5), (\frac{129}{100}, \frac{-383}{1000}), (\frac{2340922881}{7660^2}, \frac{113259286337292}{7660^3}), ...$$

Ми ћемо уопштити његову методу, а ово пресликавање ће нам бити веома важно и прожимаће цео рад.

3.1 Пројективна геометрија

Увешћемо основне појмове пројективне геометрије да би смо могли да лакше манипулишемо нашим кривама, а и неки појмови ће деловати природније кроз знања из пројективне геометрије.

3.1.1 Хомогене координате

Наша крива коју проучавамо је готово увек у нехомогеном облику. Нпр. посматрајмо криву:

$$y^2 + y^3 + x^3 = 1.$$

Из разлга које ћемо увидети у наставку поглавља, било би лепше када би крива била у хомогеном облику, па ћемо је таквом и направити. Нека је $x = \frac{X}{Z}$ и $y = \frac{Y}{Z}$. Сада крива постаје:

$$Y^2Z + Y^3 + X^3 = Z^3.$$

Одмах примећујемо главно својстно хомогених координата, ако је (a, b, c) решење једначине, то је и (ta, tb, tc) за сваки реалан број t. Ово нас наводи да дефинишемо следећу релацију $\sim$.

[8] C. G. Bachet (1581-1638) – француски математичар

Дефиниција 3.1. На скупу уређених тројки $\mathbb{R}^3$ уводимо релацију еквиваленције:

$$[a,b,c] \sim [a',b',c'] \iff (\exists t \in \mathbb{R}^*)([a,b,c] = [ta', tb', tc'])$$

Шта се десило са решењима полазне једначине при њеној хомогенизацији? Уочавамо да нова једначина има решења $(0,0,0), (1,-1,0), (-1,1,0)$. Прво је решење било које хомогене једначине и оно нам није занимљиво, али како да тумачимо друге два решења? Када бисмо желели да се вратимо у обичне координате, делили би смо са нулом, што значи да би координате те две тачке биле бесконачне. Управо тако ћемо их и тумачити, крива има пресек са бесконачношћу, што ће после дефинисања пројективне равни бити потпуно природна ствар.

3.1.2 Пројективна раван

Дефиниција 3.2. Еуклидска (афина) раван је скуп тачака:

$$\mathbb{A}^2 = \{(x,y) \mid x,y \in \mathbb{R}\}$$

Дефиниција 3.3. Пројективна раван је скуп тачака:

$$\mathbb{P}^2 = \frac{\{[a,b,c] \mid a,b,c \in \mathbb{R},\ [a,b,c] \neq [0,0,0]\}}{\sim}$$

Аналогно се дефинише и пројективни простор било ког реда.

Дефиниција 3.4. Пројективни n-простор је скуп тачака:

$$\mathbb{P}^n = \frac{\{[a_0,a_1,...,a_n] \mid a_i \in \mathbb{R},\ \exists i, a_i \neq 0\}}{\sim}$$

Како изгледају праве у пројективној равни?

Дефиниција 3.5. Права у пројективној равни је скуп тачака $[X,Y,Z]$ који задовољава:

$$aX + bY + cZ = 0$$

где a, b и c нису сви 0.

Дефиниција 3.6. У пројективној равни, праву $Z = 0$ називамо бесконачна права.

Тачке са $Z \neq 0$ чине праву у Еуклидској равни $ax + by + c = 0$, док је тачка са нултом Z координатом пресек праве са бесконачном правом. Увођењем пројективне равни, добијамо једно веома корисно својство, сваке две (различите) праве се секу у тачно једној тачки. Заиста, ако се две праве секу у Еуклидској равни, оне ће и у пројективној равни имати само тај пресек. Ако су две (различите) праве паралелне у Еуклидској равни:

$$p_1 : ax + by + c = 0, \quad p_2 : tax + tby + d = 0, \quad tc \neq d, \quad t \neq 1$$

онда у пројективној равни имају само једну тачку пресека: $[b,-a,0]$.
Дакле две паралелне праве се секу у бесконачној тачки и ту тачку садрже само праве паралелне њима. Другим речима, постоји бесконачна тачка за сваки правац у Еуклидској равни. Ако посматрамо праве кроз координатни почетак у облику $Ax = By$ и $Cx = Dy$, оне су једнаке ако и само ако је $\frac{A}{B} = \frac{C}{D}$. Ово нас наводи на још једну дефиницију пројективне равни:

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$$

Дакле, да резимирамо:

$[a,b,c]$	$\mapsto$	$\begin{cases}\left(\frac{a}{c},\frac{b}{c}\right)\in\mathbb{A}^2, c\neq 0\\ [a,b]\in\mathbb{P}^1, c=0\end{cases}$
$(x,y)\in\mathbb{A}^2$	$\mapsto$	$[x,y,1]$
$[A,B]\in\mathbb{P}^1$	$\mapsto$	$[A,B,0]$

Лако је видети да су пресликавања инверзна:

$$[a,b,c]\mapsto\left(\frac{a}{c},\frac{b}{c}\right)\mapsto\left[\frac{a}{c},\frac{b}{c},1\right]=[a,b,c]$$

па смо овиме комплетирали дефинисање пројективне равни.

3.1.3 Пројективна трансформација

Када желимо да уведемо смену координата над кривом $C: F(X,Y,Z)=0$ правимо замену:

$$X=m_{11}X^{'}+m_{12}Y^{'}+m_{13}Z^{'},$$
$$Y=m_{21}X^{'}+m_{22}Y^{'}+m_{23}Z^{'},$$
$$Z=m_{31}X^{'}+m_{32}Y^{'}+m_{33}Z^{'}.$$

Тако добијамо нову криву $C^{'}: F^{'}(X^{'},Y^{'},Z^{'})=0$. Овако смо добили пресликавање са C на $C^{'}$. Ако обезбедимо још и то да је матрица $M=(m_{ij})$ инвертибилна и $M^{-1}=N=(n_{ij})$ добијамо пресликавање са $C^{'}$ на C:

$$X^{'}=n_{11}X+n_{12}Y+n_{13}Z,$$
$$Y^{'}=n_{21}X+n_{22}Y+n_{23}Z,$$
$$Z^{'}=n_{31}X+n_{32}Y+n_{33}Z.$$

Промену координата у $\mathbb{P}^2$ дату инверзном 3×3 матрицом називамо пројективна трансформација. Ако матрица има рационалне коефицијенте постојаће бијекција између $C(\mathbb{Q})$ и $C^{'}(\mathbb{Q})$ тако да је проблем налажења рационалних тачака на C еквивалентан проблему налажења рационалних тачака на $C^{'}$. Ово својство ћемо максимално екплоатисати при проучавању елиптичких кривих.

3.2 Вајерштрасова нормална форма

При проучавању кубичне криве желимо да је преведемо у одређени облик у коме ћемо моћи лакше да оперишемо њоме. Тај облик је такозвана Вајерштрасова нормална форма и крива ће, у зависности како нам одговара изгледати:

$$y^2=x^3+ax+b,\qquad y^2=x^3+ax^2+bx+c.$$

Свака кубична крива која има бар једнну рационалну тачку се може погодном пројективном трансформацијом и мало алгебарске сналажљивости превести у горе наведени облик.
Идеја је да поставимо осе онако како нам одговарају. Процес изгледа отприлике овако. Пребацимо криву у хомогени облик. Бирамо да је тачка $O=[1,0,0]$ (тако да није превојна тачка, да би тангента имала још један пресек са кривом) и да је права $Z=0$ тангента на C у O. Она сече криву у новој тачки [0,1,0] и праву $X=0$ бирамо за тангенту у тој тачки. Најзад било коју трећу праву узимамо за $Y=0$ и пишемо $x=\frac{X}{Z}$ и $y=\frac{Y}{Z}$.
Показаћемо ово и на примеру. Превешћемо криву

$$f(u,v)=u^3+uv^2+v^3+u+v-2=0$$

у Вајерштрасову нормалну форму. У хомогеном облику она је записана као

$$F(U,V,W)=U^3+UV^2+V^3+UW^2+VW^2-2W^3=0$$

Тачка $O = [1, 0, 1]$ припада кривој и тангенту у њој бирамо за праву $Z = 0$

$$\frac{\partial F}{\partial U}(O)(U-1) + \frac{\partial F}{\partial V}(O)V + \frac{\partial F}{\partial W}(O)(W-1) = 0$$

$$4U + V - 4W = 0$$

Дакле бирамо

$$Z = 4U + V - 4W.$$

Сада тражимо пресек тангенте са кривом. Убацујемо у формулу $V = -4(U - W)$:

$$U^3 + 16U(U-W)^2 - 64(U-W)^3 + UW^2 - 4(U-W)W^2 - 2W^3 = 0.$$

O је двострука нула ове једначине па се она своди на

$$(U-W)^2(-47U + 66W) = 0$$

Одавде видимо да је $Q = [66, -76, 47]$ и тангента на C у Q има једначину:

$$21053U + 9505V - 14194W = 0,$$

па бирамо:

$$X = 21053U + 9505V - 14194W.$$

Како је O на правој $U + V - W = 0$ бирамо

$$Y = U + V - W$$

која је очигледно различита од X и Z. Коначно, добили смо пројективне трансформације:

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 21053 & 9505 & -14194 \\ 1 & 1 & -1 \\ 4 & 1 & -4 \end{bmatrix} \begin{bmatrix} U \\ V \\ W \end{bmatrix}$$

$$\begin{bmatrix} U \\ V \\ W \end{bmatrix} = \begin{bmatrix} 1/6859 & -22/19 & -1563/6859 \\ 0 & 4/3 & -1/3 \\ 1/6859 & -47/57 & -1114/1985 \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}$$

Сада добијамо нову криву:

$$C' : F(X, Y, Z) = XY^2 + aX^2Z + bXYZ + cY^2Z + dXZ^2 + eYZ^2 + gZ^3 = 0,$$

где је:

$$a = 122536011/1774335401915$$

$$b = -1492216408/983011303$$

$$c = -28388/40845345$$

$$d = -226218384460168/704411154560255$$

$$e = 4539285716595356/9756387182275$$

$$g = 6989284338276485910259/20973842127031592625$$

После дехомогенизације добијамо једначину

$$(x + c)y^2 + (bx + e)y + ax^2 + dx + g = 0.$$

Сменом $x \mapsto x - c$ једначина постаје

$$xy^2 + (b_1x + e_1)y + a_1x^2 + d_1x + g_1 = 0,$$

односно када помножимо са x,

$$(xy)^2 + (b_1x + e_1)xy + a_1x^3 + d_1x^2 + g_1x = 0.$$

Сада уводимо смену $xy \mapsto y$, па добијамо једначину

$$y^2 + (b_1x + e_1)y + a_1x^3 + d_1x^2 + g_1x = 0.$$

Сада уводимо нову смену $y \mapsto y - \frac{1}{2}(b_1x + e_1)$ па једначина добија облик

$$y^2 = Ax^3 + Bx^2 + Cx + D.$$

Да бисмо изједначили коефицијенте уз y^2 и x^3, уводимо смену $x \mapsto Ax$, $y \mapsto A^2y$. Након спровођења овог поступка, полазна једначина постаје:

$$y^2 = x^3 - x^2 - 2x - 32.$$

3.3 Сингуларне кубичне криве

Дефиниција 3.7. Тачка (x, y) кубичне криве је сингуларна тачка ако су у јој парцијални изводи по обе координате једнаки нули.

Дефиниција 3.8. Елиптичка крива је кубична крива која нема сингуларних тачака и има бар једну тачку (у неким пољима је ово својство неопходно).

Сингуларне криве немају свуда добро дефинисану тангенту. Једначина тангенте у тачки $P = (x_0, y_0)$ на кривој гласи:

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

где је крива записана као $F(x, y) = y^2 - f(x)$, па услов сингуларности у тачки P значи:

$$\frac{\partial F}{\partial x} = -f'(x) = 0, \quad \frac{\partial F}{\partial y} = 2y = 0,$$

а како је $y^2 = f(x)$ важи:

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

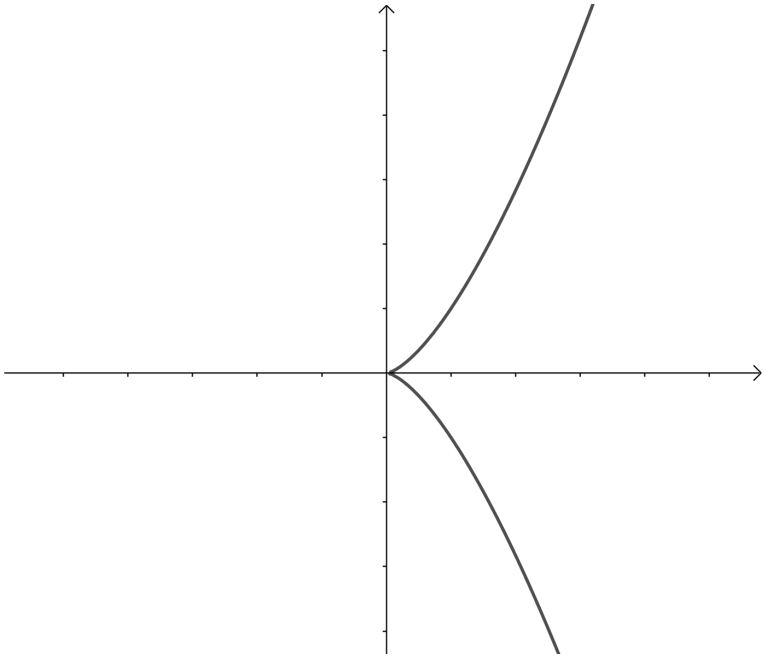
тј. $f(x)$ има нулу бар реда два.
Ово својство сингуларних кривих доводи до правог разлога зашто оне нису занимљиве за проучавање као елиптичке криве. Знамо све о њима. Лакше баратамо са њима чак и од коника. То произилази из тога што их веома лако параметризујемо.
Ако $f(x)$ има троструку нулу, може се свести на облик

$$y^2 = x^3,$$

па ову криву решавамо очигледном параметризацијом

$$x = t^2, \quad y = t^3,$$

чиме потпуно решавамо проблем налажења рационалних тачака.



Слика 2: Крива $y^2 = x^3$

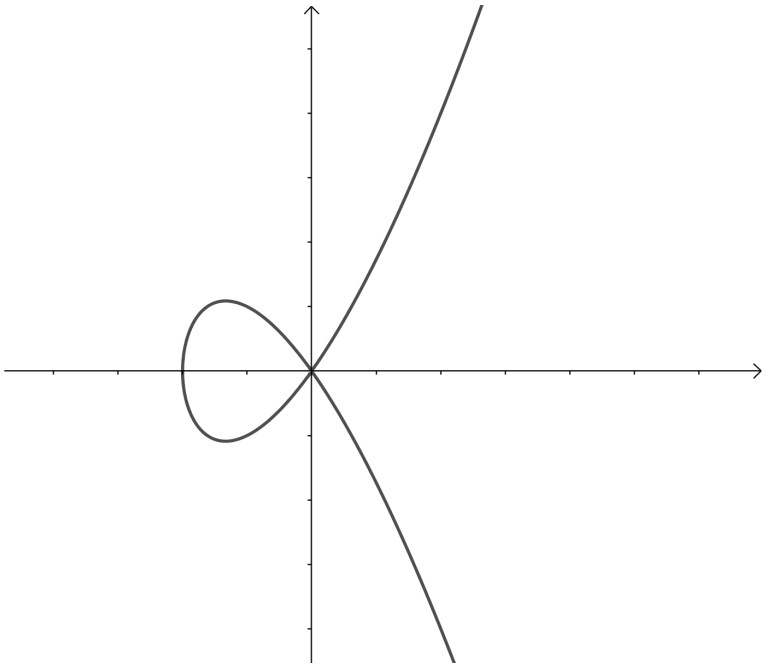
Ako $f(x)$ има две различите нуле од којих је једна двострука, може се свести на облик:

$$y^2 = x^2(x + m),$$

па ако ставимо $\frac{y}{x} = t$, добијамо $t^2 = x + m$ тј.

$$x = t^2 - m, \quad y = t^3 - mt,$$

па је овиме крива потпуно решена.

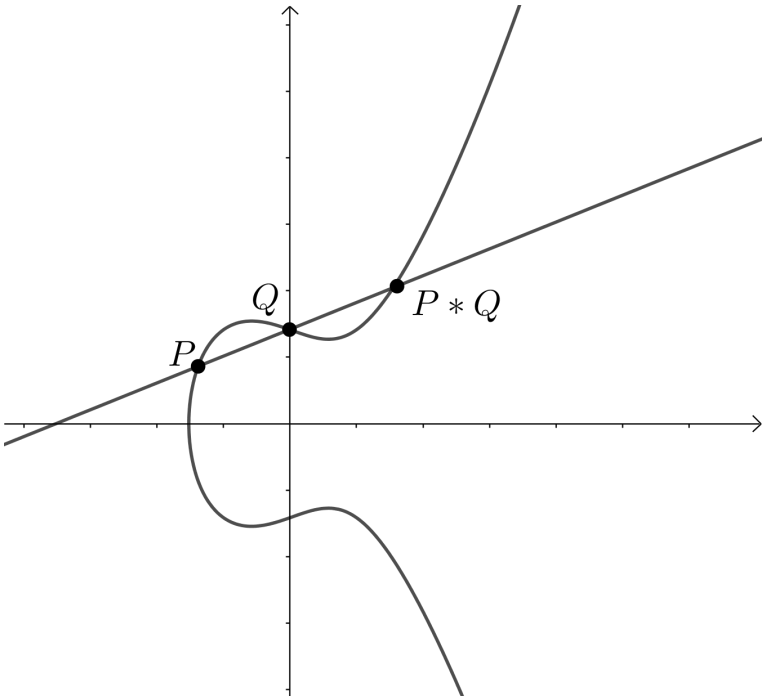


Слика 3: Крива $y^2 = x^2(x + 2)$

3.4 Групни закон елиптичке криве

Ако знамо за две рационалне тачке на кубичној кривој, можемо добити трећу када продужимо праву која садржи прве две до трећег пресека са кривом. Ово нас инспирише да посматрамо

својства ове операције коју у наставку обележавамо са $*$.
Логично питање које се поставља је, да ли је $(C, *)$ група. Испоставља се да није, међутим уз мало дораде можемо је учинити да то постане.

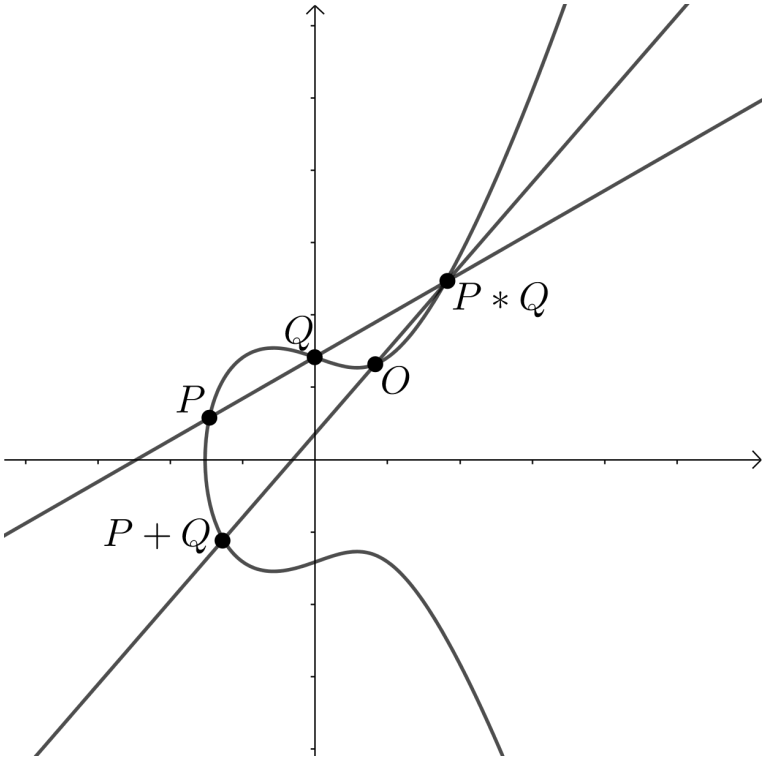


Слика 4: Операција $*$

Над C, са унапред задатом тачком O дефинишемо следећу операцију:

$$P + Q = O * (P * Q).$$

Како је $P+Q = Q+P$ наше сабирање је комутативно. Такође, $P+O = P$ тако да се O понаша као неутрал. Ако тангента у O сече криву у S, тачка пресека праве PS и криве ће се понашати као $-P$, па смо тиме нашли инверз сваке тачке. Асоцијативност се доказује уз помоћ формула из наредног дела, али пошто је то само компликован рачун, ми га овде прескачемо. Дакле $(C, +)$ је Абелова група.



Слика 5: Операција $+$

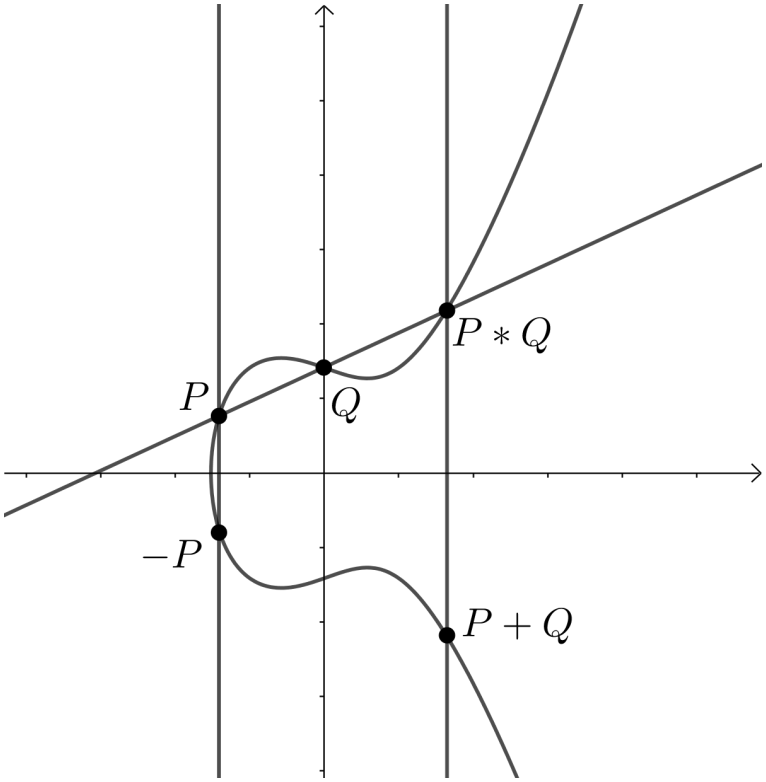
Криву посматрамо у облику

$$C : y^2 = x^3 + ax^2 + bx + c,$$

што у хомогеном облику изгледа:

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

Шта је пресек криве са бесконачном правом $Z = 0$? Када то заменимо у једначину добијамо $X^3 = 0$ тако да крива има једну бесконачну тачку и у њој сече бесконачну праву три пута, то је бесконачна тачка чији је правац y оса. Управо ту тачку узимамо за неутрал O групе $(C, +)$. Сада наша операција добија мало лепши облик. За $P * Q = (x, y),\ P + Q = (x, -y)$. Такође, за $P = (x, y),\ -P = (x, -y)$. У наставку ћемо извести експлицитне формуле за рачунање координата.



Слика 6: Операција + са бесконачном тачком као неутралом

3.4.1 Експлицитна формула за $P_1 + P_2$

Нека је:

$$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2),\ P_1 * P_2 = (x_3, y_3),\ P_1 + P_2 = (x_3, -y_3).$$

Нека је $P_2 \notin \{P_1, -P_1, O\}$ Сада P_1, P_2 и $P_1 * P_2$ леже на правој

$$y = \lambda x + \nu,\ \lambda = \frac{y_2 - y_1}{x_2 - x_1},\ \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

Треба да нађемо трећу тачку пресека ове праве и C.

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$$

па када све пребацимо на једу страну добијамо:

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2).$$

Ова једначина има три нуле и то су x_1, x_2 и x_3, па применом Вијетових правила добијамо:

$$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu$$

3.4.2 Експлицитна формула за $P + P = 2P$

Када тачку $P \neq O$ сабирамо саму са собом, тражимо пресек њене тангенте са C, то ће бити тачка $P * P$. Нека је:

$$P = (x_1, y_1),\ P * P = (x_2, y_2),\ P + P = (x_2, -y_2).$$

Нека је права на којој леже P и $P * P$ права: $y = \lambda x + \nu$. Из $y^2 = 2f(x)$ закључујемо да је $2ydy = f'(x)dx$ па важи:

$$\lambda = \frac{dy}{dx} = \frac{f'(x_1)}{2y_1}, \quad \nu = y_1 - \lambda x_1$$

Сада примењујемо исту процедуру као и код обичног сабирања па добијамо:

$$x_2 = \lambda^2 - a - 2x_1, \quad y_2 = \lambda x_2 + \nu$$

па после замене y^2 са $f(x)$ добијамо општи облик Бахеове формуле дуплирања:

$$x(2P) = \frac{f'(x)^2}{4f(x)} - a - 2x = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}, \quad P = (x, y)$$

4 Тачке коначног реда

Посматраћемо елиптичку криву C дату у Вајерштрасовом облику:

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

где је тачка у бесконачности O неутрал у групном закону. Ако ставимо $X = d^2x$, $Y = d^3y$ тада једначина постаје $Y^2 = X^3 + d^2aX^2 + d^4bX + d^6c$ па бирањем довољно великог d можемо поништити имениоце, тако да на даље сматрамо да су a, b, c цели бројеви.

Дефиниција 4.0.1. Елемент P групе има ред m ако важи:

$$mP = \underbrace{P + P + \cdots + P}_{m} = O$$

при чему $m'P \neq O$ за све природне бројеве $1 \leq m' \leq m$. Ако такво m постоји, P има коначан ред, у супротном P има бесконачан ред.

Испоставиће се да тачке коначног реда елиптичке криве чиние групу и оне ће нам бити од велике важности за даље проучавање елиптичких кривих.

4.1 Тачке реда два

Које тачке задовољавају $2P = O$ и $P \neq O$? Ово је еквивалентно услову $P = -P \neq O$, тј. важи $(x, y) = (x, -y)$. То су тачке са y координатом нула, односно тачке:

$$P_1 = (\alpha_1, 0),\ P_2 = (\alpha_2, 0),\ P_3 = (\alpha_3, 0)$$

где су α_1, α_2 и α_3 нуле полинома $f(x)$. Како C није сингуларна, ове три тачке су различите. Решења једначине $2P = O$ чине подгрупу. Група $\{O, P_1, P_2, P_3\}$ је производ две цикличне групе реда два.[9] Овиме смо доказали следећу теорему.

Теорема 4.1.1. Нека је C елиптичка крива

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

(а) Тачка $P = (x, y) \neq O$ на C је реда два ако и само ако важи $y = 0$
(б) C има тачно четири тачке реда који дели 2. Те четири тачке формирају групу која је производ две цикличне групе реда два.

4.2 Тачке реда три

За тачке реда три, доказаћемо сличну теорему.

Теорема 4.2.1. Нека је C елиптичка крива

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

(а) Тачка $P = (x, y) \neq O$ на C је реда три ако и само ако је x нула полинома

$$g_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2).$$

(б) C има тачно девет тачка реда који дели 3. Те тачке формирају групу која је производ две цикличне групе реда три.[10]

[9] Ово важи ако радимо над алгебарски затвореним пољем, тј. над пољем где полином степена n има n нула у том пољу

[10] Ово важи ако радимо над алгебарски затвореним пољем, тј. над пољем где полином степена n има n нула у том пољу

Доказ. Које тачке имају ред три? За њих важи $3P = O$, што је еквивалентно са $2P = -P$ тако да тачка реда три задовољава $x(2P) = x(-P) = x(P)$. Са друге стране, ако $P \neq O$ задовољава $x(2P) = x(P)$ тада је $2P = P$, тј. $P = O$ што смо искључили, или је $2P = -P$, тј. $3P = O$. Дакле $P \neq O$ је реда три ако и само ако $x(2P) = x(P)$ што је по формули за дуплирање из другог поглавља еквивалентно са:

$$x = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c},$$

што је после множења еквивалентно са $g_3(x) = 0$ чиме смо доказали део под (а).
Приметимо да важи:

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = \frac{f'(x)^2}{4f(x)} - a - 2x,$$

па добијамо нови израз за $g_3(x)$:

$$g_3(x) = 2f(x)f''(x) - f'(x)^2.$$

Одавде је:

$$g_3'(x) = 2f(x)f'''(x) = 12f(x)$$

Ако би $g_3(x)$ и $g_3'(x)$ имали заједничку нулу онда би је имали и $f(x)$ и $f'(x)$ што је у контрадикцији са тим да је крива несингуларна. Дакле $g_3(x)$ има 4 различите нуле, $\beta_1, \beta_2, \beta_3, \beta_4$ тако да је скуп тачака реда три:

$$(\beta_1, \pm\sqrt{f(\beta_1)}), (\beta_2, \pm\sqrt{f(\beta_2)}), (\beta_3, \pm\sqrt{f(\beta_3)}), (\beta_4, \pm\sqrt{f(\beta_4)})$$

Овиме је теорема доказана. □

4.3 Дискриминанта

Циљ овог поглавља је да докажемо теорему која нам говори како да нађемо све тачке коначног реда. За то ће нам бити потребно познавање дискриминанте.

Дефиниција 4.3.1. Дискриминанта D полинома трећег степена, који има нуле $\alpha_1, \alpha_2, \alpha_3$ је

$$D = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2$$

Дискриминанта је број који нам говори да ли полином има неке две нуле једнаке. Дискриминанта од $f(x)$ која нас занима износи:

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Следећа теорема је једно важно својство дискриминанте и ми ћемо је доказати за случај који нама треба.

Теорема 4.3.1. За сваки полином $f(x)$ са целобројним коефицијентима постоје полиноми са целобројним коефицијентима $s(x)$ и $r(x)$, тако да важи:

$$D = r(x)f(x) + s(x)f'(x)$$

Доказ. У нашем случају важи следеће:

$$D = [(18b - 6a^2)x - (4a^3 - 15ab + 27c)]f(x) + [(2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2)]f'(x)$$

□

Уз помоћ овога доказаћемо следећу лему:

Лема 4.3.1. Нека је $P = (x, y)$ тачка на нашој елиптичкој кривој, таква да P и $2P$ имају целобројне координате. Тада је или $y = 0$ или $y \mid D$.

Доказ. Претпоставимо да је $y \neq 0$ докажимо да $y \mid D$. Због $y \neq 0$ важи $2P \neq O$ па је $2P = (X, Y)$. Из формуле за дуплирање имамо:

$$2x + X = \lambda^2 - a, \quad \lambda = \frac{f'(x)}{2y}$$

. Како су x, X, a целобројни, то је и λ, тако да $y \mid f'(x)$. Како је $y^2 = f(x)$, онда и $y \mid f(x)$ па због теореме 4.3.1 важи и $y \mid D$ □

Напоменимо само да важи и јаче тврђење, наиме важи $y^2 \mid D$.

4.4 Тачке коначног реда имају целобројне координате

Преостао нам је још један корак пре него што докажемо главну теорему ове главе, тврђење да тачке коначног реда имају целобројне координате. Доказ није кратак тако да ћемо само објаснити главну идеју. Један од начина да докажемо да је неки број цео је и то да његов именилац није дељив ни једним простим бројем. Вођени тиме, за рационалан број облика $x = \frac{m}{n}p^\nu$, где су m, n и p узајамно прости у паровима, дефинишемо његов ред као:

$$\mathrm{ord}(\frac{m}{n}p^\nu) = \nu.$$

Посматрајмо сада тачку (x, y) на кривој и нека важи:

$$x = \frac{m}{np^\alpha}, \qquad y = \frac{u}{wp^\beta},$$

и нека је $\alpha > 0$ и m, n и p као и u, w и p су узајамно прости у паровима. Када ово заменимо у једначину криве, добијамо:

$$\frac{u^2}{w^2p^{2\beta}} = \frac{m^3 + am^2np^\alpha + bmn^2p^{2\alpha} + cn^3p^{3\alpha}}{n^3p^{3\alpha}}.$$

Како је $\alpha > 0$ и $p \nmid m$ важи

$$p \nmid (m^3 + am^2np^\alpha + bmn^2p^{2\alpha} + cn^3p^{3\alpha})$$

одакле добијамо

$$-3\alpha = \mathrm{ord}(\frac{m^3 + am^2np^\alpha + bmn^2p^{2\alpha} + cn^3p^{3\alpha}}{n^3p^{3\alpha}}) = \mathrm{ord}(\frac{u^2}{w^2p^{2\beta}}) = -2\beta.$$

Дакле $2\beta = 3\alpha$, па постоји природан број ν такав да важи $\alpha = 2\nu$ и $\beta = 3\nu$. До истог закључка бисмо дошли и да смо пошли од услова $\beta > 0$. На даље је идеја да се уочи група

$$C(p^\nu) = \{(x, y) \in C(\mathbb{Q}) : \quad \mathrm{ord}(x) \leq -2\nu,\ \mathrm{ord}(x) \geq -3\nu\}$$

и да се одређеним алгебарским манипулацијама, које ми нећемо овде наводити, докаже да тачке коначног реда заиста имају целобројне координате.

4.5 Нагел-Луцова теорема

Коначно, имамо све састојке потребне да бисмо доказали Нагел[11]-Луцову[12] теорему.

Теорема 4.5.1. Нека је

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

елиптичка крива, где су коефицијенти a b и c цели бројеви, и нека је D дискриминанта полинома $f(x)$,

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Нека је $P = (x, y)$ рационална тачка коначног реда. Тада су x и y цели бројеви и или је $y = 0$ па је P тачка реда два, или важи $y \mid D$

Доказ. У одељку 4.4 смо видели да тачка P има целобројне координате. Ако је P реда два, важи $y = 0$ па смо у том случају готови. У супротном важи $2P \neq O$, па како је и $2P$ тачка коначног реда, и она има целобројне координате. Сада из леме 4.3.1 следи да $y \mid D$. □

Сада ћемо урадити један пример. Нађимо све тачке коначног реда криве

$$y^2 = x^3 + 8.$$

Дискриминанта је $D = -1728 = -3^3 \cdot 2^6$ па имамо

$$y^2 \in \{1, 4, 16, 64, 9, 36, 144, 576\}$$

па добијамо 8 једначина

$$1 = x^3 + 8,\ 4 = x^3 + 8,\ 16 = x^3 + 8,\ 64 = x^3 + 8$$

$$9 = x^3 + 8,\ 36 = x^3 + 8,\ 144 = x^3 + 8,\ 576 = x^3 + 8$$

и за тачке реда два $x^3 + 8 = 0$. Само трећа, пета и девета једначина имају решење па добијамо да су тачке коначног реда ове криве $\{O, (2, 4), (2, -4), (1, 3), (1, -3), (-2, 0)\}$.
За крај овог поглавља, навешћемо још један важан резултат у вези тачака коначног реда, Мазурову[13] теорему која нам мало ближе говори како група рационалних тачака може да изгледа.

Теорема 4.5.2. Нека је C елиптичка крива и нека G_t група рационалних тачака коначног реда ове криве. Тада важи:

$$G_t = \frac{\mathbb{Z}}{n\mathbb{Z}}, \quad n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$$

или

$$G_t = \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2n\mathbb{Z}}, \quad n \in \{1, 2, 3, 4\}$$

[11] T. Nagell (1895-1988) – норвешки математичар.
[12] E. Lutz (1914-2008) – француски математичар.
[13] B. C. Mazur (1937-) – амерички математичар.

5 Група рационалних тачака

Главни циљ у овом поглављу ће бити доказивање Морделове[14] теореме која тврди да је група рационалних тачака елиптичке криве коначно генерисана. Доказ је веома дугачак, па ћемо прескочити неке делове, али ћемо добар део и сами доказати.

5.1 Леме и теорема о спусту

За почетак, дефинишимо функцију висина (H) над рационалним бројевима, са којом ћемо у наставку доста баратати.

$$H(\frac{m}{n}) = max\{|m|, |n|\}.$$

Она нам на неки начин говори о томе колико је дати рационалан број компликован. Примећујемо да је скуп тачака које имају висину мању од датог фиксног броја, коначан. Ово је тзв. својство коначности висине и користиће нам у појединим тренутцима. За тачку $P = (x, y)$ на кривој дефинишемо висину као

$$H(P) = H(x).$$

Такође, дефинишемо функцију h ради лакшег записа ако то буде потребно

$$h(x) = \ln(H(x)).$$

Приметимо да је и скуп рационалних тачака на кривој чија је висина мања од неког унапред задатог броја, коначан. Дефинишемо и висину бесконачне тачке

$$H(O) = 1$$

Сада наводимо четири кључне леме које желимо да докажемо.

Лема 1: За сваки реалан број M, скуп

$$\{P \in C(\mathbb{Q}) \ : \ h(P) \leq M\}$$

је коначан.
Ову лему смо навели у ранијем тексту.

Лема 2: Нека је P_0 фиксирана тачка на C. Тада постоји константа k_0 која зависи од P_0, a, b и c, тако да важи

$$h(P + P_0) \leq 2h(P) + k_0,$$

за све $P \in C(\mathbb{Q})$
Ову лему ћемо доказати у наредном делу.

Лема 3: Постоји константа k која зависи од a, b и c, тако да важи

$$h(2P) \geq 4h(P) - k,$$

за све $P \in C(\mathbb{Q})$
Доказ ове леме захтева мало компликованији рачун па ћемо га прескочити.

Лема 4: Индекс $(C(\mathbb{Q}) \ : \ 2C(\mathbb{Q}))$ је коначан.

Овде треба имати у виду да $2C(\mathbb{Q})$ означава подгрупу $C(\mathbb{Q})$ која се састоји од тачака које су два пута нека друга тачка. За сваку комутативну групу G, множење са m

$$G \to G, \quad P \to \underbrace{P + P + \cdots + P}_{m} = mP$$

хомоморфизам. Сада наводимо, без доказа, кључну ставку за доказ Морделове теореме. Теорема о спусту.

[14] J. L. Mordell (1888-1972) – америчко-британски математичар.

Теорема 5.1.1. Нека је G комутативна група и нека постоји функција

$$h : G \to [0, \infty)$$

са следећим својствима.
(а) За сваки реалан број M, скуп $\{P \in G \ : \ h(P) \leq M\}$ је коначан.
(б) За све $P_0 \in G$. Тада постоји константа, тако да важи

$$h(P + P_0) \leq 2h(P) + k_0,$$

за све $P \in G$
(в) Постоји константа k тако да важи

$$h(2P) \geq 4h(P) - k,$$

за све $P \in G$
(г) Подгрупа $2G$ има коначан индекс у G.
Тада је G коначно генерисана.

Доказ није тежак али је потребно познавање неких појмова из теорије група па ћемо га у овом раду прескочити.

5.2 Висина $P + P_0$

Леме које смо навели су растуће тежине и у овом поглављу ћемо доказати лему 2. Циљ је да некако повежемо висине P,P_0 и $P + P_0$. Нека је $P = (x, y)$ рационална тачка на кривој и нека су

$$x = \frac{m}{M}, \quad y = \frac{n}{N}$$

где је $(m, M) = 1$ и $(n, N) = 1$ и $M, N > 0$. Када ово убацимо у једначину елиптичке криве добијамо

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M} + c,$$

односно када се ослободимо именилаца

$$M^3n^2 = N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3.$$

Како N^2 дели десну страну једнакости и како је $(n, N) = 1$ закључујемо да важи $N^2 \mid M^3$. Из једначине такође следи да $M \mid N^2$. Сада су сви сабирци осим N^2m^3 дељиви са M^2 тако да $M^2 \mid N^2$ тј. $M \mid N$. Међутим, сада су сви сабирци осим N^2m^3 дељиви са M^3 тако да закључујемо да $M^3 \mid N^2$. Дакле, $N^2 \mid M^3$ и $M^3 \mid N^2$ што значи да је $M^3 = N^2$. Због овога у наставку пишемо

$$P = (x, y) = (\frac{m}{e^2}, \frac{n}{e^3}).$$

Сада ћемо се позабавити висином тачке P. Важи $H(P) = max\{|m|, e^2\}$, тј. $|m| \leq H(P)$ и $e^2 \leq H(P)$.
Покушајмо да ограничимо висину y, тј. висину n. Када у једначину убацимо координате тачке и ослободимо се именилаца, добијамо

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6.$$

Сада ћемо искористити неједнакост троугла

$$|n^2| \leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6|,$$

односно

$$|n^2| \leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3$$

Дакле, добили смо оцену:

$$|n| \leq KH(P)^{3/2}, \quad K = \sqrt{1+|a|+|b|+|c|}.$$

Сада ћемо доказати лему 2. Случај $P_0 = O$ тривијално важи тако да у наставку претпостављамо $P \neq O$. Нека је $P_0 = (x_0, y_0)$ и $P \notin \{P_0, -P_0, O\}$ и нека је $P + P_0 = (X, Y)$. Наш циљ је да ограничимо висину X. Из формула израчунатих раније имамо

$$X + x + x_0 = \lambda^2 - a, \quad \lambda = \frac{y - y_0}{x - x_0}$$

Када изједначимо ова два израза, добијамо

$$X = \frac{(y-y_0)^2}{(x-x_0)^2} - a - x - x_0$$

$$= \frac{(y-y_0)^2 - (x-x_0)^2(x+x_0+a)}{(x-x_0)^2}$$

Када ово измножимо и заменимо $y^2 - x^3$ са $ax^2 + bx + c$ добијамо

$$X = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

при чему сматрамо да су A, B, C, D, E, F, G цели бројеви јер можемо множити бројилац и именилац последњег израза док они то не постану. Наведени коефицијенти зависе само од a, b, c, x_0 и y_0. Сада мењамо у једначину $x = \frac{m}{e^2}$ и $y = \frac{n}{e^3}$

$$X = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

Сада радимо исти поступак као раније.

$$H(X) \leq max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}.$$

Применићемо следеће већ израчунате оцене

$$e \leq H(P)^{1/2}, \quad n \leq KH(P)^{3/2}, \quad m \leq H(P)$$

и применити неједнакост троугла.

$$|Ane + Bm^2 + Cme^2 + De^4| \leq |Ane| + |Bm^2| + |Cme^2| + |De^4|$$

$$\leq (|AK| + |B| + |C| + |D|)H(P)^2$$

$$|Em^2 + Fme^2 + Ge^4| \leq |Em^2| + |Fme^2| + |Ge^4|$$

$$\leq (|E| + |F| + |G|)H(P)^2.$$

Дакле

$$H(P + P_0) = H(X) \leq max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}H(P)^2$$

Након логаритмовања видимо да заиста постоји константа k_0 за коју важи

$$h(P + P_0) \leq 2h(P) + k_0.$$

Ако је $P \in \{P_0, -P_0, O\}$ за константу бирамо максимум k_0 и највеће вредности $h(P+P_0) - 2h(P)$ за ове три тачке. Овим је лема 2 доказана □

5.3 Лема 4

Сада ћемо се позабавити лемом 4, да група $2C(\mathbb{Q})$ има коначан индекс у $C(\mathbb{Q})$. На даље означавамо $C(\mathbb{Q}) = G$. Да бисмо избегли коришћење алгебарске теорије бројева, претпоставићемо да $f(x)$ има једну рационалну нулу x_0. Водећи коефицијент полинома $f(x)$ је 1 па $x_0 \in \mathbb{Z}$. Сада можемо увесту смену координата тако да померимо x_0 у координатни почетак. Једначина криве изгледа овако:

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

где је $T = (0, 0)$ рационална тачка реда два. Дискриминанта сада износи

$$D = b^2(a^2 - 4b),$$

и како крива није сингуларна, $b \neq 0$ и $a^2 \neq 4b$.

5.3.1 Корисни хомоморфизам

Већ смо видели да формула за дуплирање тачке није баш једноставна, тако да ће нам бити корисно да је разбијемо на две мање операције. Посматраћемо криву $\bar{C}$ која је дефинисана на следећи начин:

$$\bar{C} \ : \ y^2 = x^3 + \bar{a}x^2 + \bar{b}x, \quad \bar{a} = -2a, \quad \bar{b} = a^2 - 4b.$$

На први поглед, ова крива нема ништа заједничко са претходном, али разлог због ког нам је значајна увиђамо када још јендом применимо исту процедуру.

$$\bar{\bar{C}} \ : \ y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x, \quad \bar{\bar{a}} = -2\bar{a} = 4a, \quad \bar{\bar{b}} = \bar{a}^2 - 4\bar{b} = 16b$$

Дакле нова крива $\bar{\bar{C}}$ је дата једначином $y^2 = x^3 + 4ax^2 + 16bx$ и готово је иста као полазна крива, а што је најважније, групе G и $\bar{\bar{G}}$ су изоморфне. Сада желимо да нађемо хомоморфизме са C на $\bar{C}$ и са $\bar{C}$ на $\bar{\bar{C}}$ тако да њихова композиција буде множење са два. Важи следеће тврђење.

Тврђење: Нека су C и $\bar{C}$ елиптичке криве дате једначинама:

$$C \ : \ y^2 = x^3 + ax^2 + bx$$

$$\bar{C} \ : \ y^2 = x^3 + \bar{a}x^2 + \bar{b}x, \quad \bar{a} = -2a, \quad \bar{b} = a^2 - 4b$$

и нека је $T = (0, 0)$ тачка са C. Тада:
(а) Постоји хомоморфизам $\phi : C \to \bar{C}$ дефинисан на следећи начин

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right), & P = (x, y) \neq O, T \\ \bar{O}, & P \in \{O, T\} \end{cases}$$

Језгро ϕ је $\{O, T\}$.

(б) Применом исте процедуре на $\bar{C}$, добијамо пресликавање $\bar{\phi} : \bar{C} \to \bar{\bar{C}}$. Крива $\bar{\bar{C}}$ је изоморфна са C преко пресликавања $(x, y) \to (x/4, y/8)$. Зато, постоји хомоморфизам $\psi : \bar{C} \to C$ дефинисана на следећи начин

$$\psi(\bar{P}) = \begin{cases} \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}\right), & \bar{P} = (\bar{x}, \bar{y}) \neq \bar{O}, \bar{T} \\ O, & \bar{P} \in \{\bar{O}, \bar{T}\} \end{cases}$$

Композиција $\psi \circ \phi : C \to C$ је множење са два, тј. $\psi \circ \phi(P) = 2P$.

5.3.2 Доказ

Рационалне тачке са C сликају у рационалне тачке са $\bar{C}$, али када изаберемо неку тачку на $\bar{C}$ не мора да значи да она потиче од рационалне тачке са C. Ако применимо ϕ на тачке из G добијамо подгрупу рационалних тачака са $\bar{G}$. Означићемо је са $\phi(G)$. Следеће тврђење нам говори како она изгледа.

Тврђење: Све ознаке имају значење које смо до сада навели. Тада важи:
(а) $\bar{O} \in \phi(G)$
(б) $\bar{T} = (0,0) \in \phi(G)$ ако и само ако је $\bar{b} = a^2 - 4b$ потпун квадрат.
(в) Нека је $\bar{P} = (\bar{x}, \bar{y}) \in \bar{G}$ где је $\bar{x} \neq 0$. Тада $\bar{P} \in \phi(G)$ ако и само ако је $\bar{x}$ квадрат неког рационалног броја.

Желимо да покажемо да $2G$ има коначан индекс у G. Прво ћемо показати која је идеја у доказу да су индекси $(\bar{G} : \phi(G))$ и $(G : \psi(\bar{G}))$ коначни. Доказује се да је $(\bar{G} : \phi(G)) \leq 2^{s+1}$ и $G : \psi(\bar{G}) \leq 2^{r+1}$, где су s и r редом бројеви простих делилаца $\bar{b}$ и b. Очигледно је довољно да наведемо само једно од ова два тврђења и ми ћемо навести друго. Идеја је да нађемо хомоморфизам који је бијекција и слика $G/\psi(G)$ у неку коначну групу.

Нека је $\mathbb{Q}^*$ мултипликативна група рационалних бројева и нека је $\mathbb{Q}^{*2}$ подгрупа ове групе дефинисана као

$$\mathbb{Q}^{*2} = \{u^2 : u \in \mathbb{Q}^*\}.$$

Дефинишимо пресликавање $\alpha : G \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ као

$$\alpha(O) = 1$$

$$\alpha(T) = b \pmod{\mathbb{Q}^{*2}}$$
$$\alpha(x, y) = x \pmod{\mathbb{Q}^{*2}},$$

Важи следеће тврђење.

Тврђење: (а) Пресликавање α описано горе је хомоморфизам.
(б) Језгро α је $\psi(\bar{G})$. Због тога постоји хомоморфизам који је бијекција

$$\frac{G}{\psi(\bar{G})} \to \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$$

(в) Нека су $p_1, p_2, \cdots, p_t$ различити прости бројеви који деле b. Тада се слика α садржи у подгрупи $\mathbb{Q}^*/\mathbb{Q}^{*2}$ која се састоји од елемената

$$\{\pm p_1^{m_1}, p_2^{m_2}, \cdots, p_t^{m_t} \ : \ m_i \in \{0, 1\}\}.$$

(г) Индекс $(G : \psi(\bar{G}))$ је највише 2^{t+1}.
За комплетирање доказа користи се позната лема из теорије група.

Лема: Нека су A и B Абелове групе, и посматрамо хомоморфизме $\phi : A \to B$ и $\psi : B \to A$. Нека важи

$$\psi \circ \phi(a) = 2a, \quad \phi \circ \psi(b) = 2b$$

за све $a \in A$ и све $b \in B$. Тада важи следеће

$$(A : 2A) \leq (A : \psi(B))(B : \phi(A))$$

Навели смо како отприлике иде пут до доказа Морделове теореме. Доказ је дугачак па смо неке ствари прескочили, али када се све наведено лепо уклопи доказ је комплетан.

5.4 Примена Морделове теореме

Са $\mathbb{Z}_m$ ћемо означавати групу $\mathbb{Z}/m\mathbb{Z}$. То је група бројева по модулу m. Може се доказати да је група рационалних тачака елиптичке криве изоморфна са:

$$G \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r} \oplus \mathbb{Z}_{p_1^{\nu 1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu s}}.$$

Одавде следи да постоје генератори $P_1, ..., P_r, Q_1, ...Q_s$ такви да се свака тачка P са криве може записати у облику:

$$P = n_1 P_1 + \cdots + n_r P_r + m_1 Q_1 + \cdots + m_s Q_s$$

где су n_i и m_j цели бројеви. Број r зовемо ранг и ако је он једнак нули група је коначна. Заправо, група

$$\mathbb{Z}_{p_1^{\nu 1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu s}}$$

представља баш групу тачака коначног реда елиптичке криве. Овај случај ће нас највише занимати, јер ћемо углавном решавати задатке који имају коначан број решења. Само нам је остао један проблем. Како да израчунамо ранг? Теорија група нам даје следећи одговор.

$$2^r = \frac{\#\alpha(G) \cdot \#\bar{\alpha}(\bar{G})}{4}$$

где је α пресликавање описано у претходном делу овог поглавља, при чему $\#$ означава број различитих елемената одређеног скупа.

Желимо да видимо колико елемената има $\alpha(G)$. Нека је $P = (x, y)$ тачка са криве. Већ смо видели да она може бити записана у облику

$$x = \frac{m}{e^2}, \quad y = \frac{n}{e^3}.$$

Ако је $m = 0$, важи $P = T$ па је $\alpha(P) = b$, дакле $b \in \alpha(G)$. Такође, ако је $a^2 - 4b = d^2$ за $d \in \mathbb{Z}$, једначина $x(x^2 + ax + b) = 0$ има рационално решење, па у том случају $\frac{-a+d}{2}$ и $\frac{-a-d}{2}$ такође припадају $\alpha(G)$. За сада смо узели у обзир све тачке реда два. Нека је сада $m, n \neq 0$. Из једначине криве следи

$$n^2 = m(m^2 + ame^2 + be^4).$$

Нека је

$$b_1 = sgn(m) \cdot (m, b), \;\; m = b_1 m_1, \;\; b = b_1 b_2, \;\; (m_1, b_2) = 1, \;\; m_1 > 0$$

Када ово заменимо у једначину добијамо:

$$n^2 = b_1^2 m_1 (b_1 m_1^2 + a m_1 e^2 + b_2 e^4)$$

Дакле $b_1^2 \mid n^2$, тј. $b_1 \mid n$ па пишемо $n = n_1 b_1$. Када ово заменимо у једначину, добијамо

$$n_1^2 = m_1 (b_1 m_1^2 + a m_1 e^2 + b_2 e^4)$$

Како је $(m_1, b_2) = 1$ и $(m_1, e) = 1$ чиниоци са десне стране једнакости су узајамно прости, а како им је производ квадрат, оба морају бити квадрати. Дакле

$$m_1 = M^2, \quad b_1 m_1^2 + a m_1 e^2 + b_2 e^4 = N^2, \quad n_1 = MN, \quad (M, N) = 1$$

Када још елиминишемо m_1 добијамо веома важну једначину на коју ћемо се увек враћати при решавању задатака

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4 \quad (*)$$

Тачка P сада има координате

$$x = \frac{b_1 M^2}{e^2}, \quad y = \frac{b_1 MN}{e^3}.$$

Подсећамо се да је $\alpha(P) = x \pmod{\mathbb{Q}^{*2}}$ односно у нашем случају $\alpha(P) = b_1$. Сада видимо да је процедура за налажење $\#\alpha(G)$ следећа: факторишемо $b = b_1 b_2$ на чиниоце на све могуће начине и за сваки пар (b_1, b_2) решимо одговарајућу једначину облика $(*)$ по (M, e, N). Ако она има бар једно решење, $b_1 \in \alpha(G)$. На сличан начин налазимо и $\#\bar{\alpha}(\bar{G})$ тако да заправо имамо процедуру како да пронађемо ранг.

Сада ћемо урадити два примера.

Пример 1. Наћи све рационалне тачке криве $C : y^2 = x^3 - x$.

Видимо да је $a = 0$ и $b = -1$. Дакле $-1 \in \alpha(G)$. Како је $a^2 - 4b = 4$, $\frac{0+2}{2} = 1 \in \alpha(G)$. Сада смо већ покупили све факторизације броја b тако да је $\alpha(G) = \{1, -1\}$ па је $\#\alpha(G) = 2$.
Сада желимо да нађемо $\bar{\alpha}(\bar{G})$. Посматрамо криву $\bar{C} : y^2 = x^3 + 4x$ сада је $a = 0$ и $b = 4$. Како је b квадрат, важи $1 \in \bar{\alpha}(\bar{G})$. Сада факторишемо b, па $b_1 \in \{1, -1, 2, -2, 4, -4\}$ али пошто радимо $(\mathrm{mod}\ \mathbb{Q}^{*2})$ и пошто смо први случај већ обрадили остају нам вредности $b_1 \in \{-1, 2, -2\}$. Сада решавамо три једначине облика $(*)$.

$$N^2 = -M^4 - 4e^4,$$

$$N^2 = 2M^4 + 2e^4,$$

$$N^2 = -2M^4 - 2e^4.$$

Прва и трећа једначина очигледно немају решења, а друга има решење $(M, e, N) = (1, 1, 2)$. Дакле $\bar{\alpha}(\bar{G}) = \{1, 2\}$, односно $\#\bar{\alpha}(\bar{G}) = 2$. $r = \log_2(\frac{2 \cdot 2}{4}) = 0$ па су једине рационалне тачке оне које имају коначан ред.
Тачке коначног реда проналазимо по стандардној процедури помоћу Нагел-Луцове теореме. Ако је $y = 0$, имамо једначину $x^3 - x = 0$ одакле добијамо решења $(0, 0)$, $(1, 0)$ и $(-1, 0)$. Ако је $y \neq 0$ важи да $y^2 \mid D$, тј. $y^2 \mid 4$. Добијамо једначине

$$x^3 - x = 4,$$

$$x^3 - x = 1.$$

Ове једначине немају решења, тако да коначно добијамо:

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

Овиме је задатак завршен. □

Пример 2 Наћи све рационалне тачке криве $C : y^2 = x^3 + x$.

Видимо да је $a = 0$ и $b = 1$. Дакле $1 \in \alpha(G)$. Треба још проверити факторизацију броја b на $(b_1, b_2) = (-1, 1)$. Добијамо једначину

$$N^2 = -M^4 - e^4$$

која нема решења па је $\#\alpha(G) = 1$.
Сада желимо да нађемо $\bar{\alpha}(\bar{G})$. Посматрамо криву $\bar{C} : y^2 = x^3 - 4x$ сада је $a = 0$ и $b = -4$. Како је $-b$ квадрат, важи $-1 \in \bar{\alpha}(\bar{G})$. Како је $a^2 - 4b = (-4) \cdot (-4) = 16$, Добијамо да и 2 и -2 припадају $\bar{\alpha}(\bar{G})$. Сада факторишемо b, $b_1 \in \{1, -1, 2, -2, 4, -4\}$ али пошто радимо $(\mathrm{mod}\ \mathbb{Q}^{*2})$ и када избацимо случајеве које смо већ обрадили, остаје нам вредност $b_1 = 1$. Како је $\alpha(O) = 1$, мора важити и $1 \in \bar{\alpha}(\bar{G})$. Дакле $\bar{\alpha}(\bar{G}) = \{1, -1, 2, -2\}$, односно $\#\bar{\alpha}(\bar{G}) = 4$. $r = \log_2(\frac{1 \cdot 4}{4}) = 0$ па су једине рационалне тачке оне које имају коначан ред.
Тачке коначног реда проналазимо по стандардној процедури помоћу Нагел-Луцове теореме. Ако је $y = 0$, имамо једначину $x^3 + x = 0$ одакле добијамо решење $(0, 0)$. Ако је $y \neq 0$ важи да $y \mid D$, тј. $y \mid -4$. Добијамо једначине

$$x^3 + x = 1,$$

$$x^3 + x = 4,$$
$$x^3 + x = 16$$

Ове једначине немају решења, тако да коначно добијамо:

$$C(\mathbb{Q}) = \{O, (0,0)\}$$

Овиме је задатак завршен а само напомињемо да смо успут доазали и да крива

$$\bar{C} : y^2 = x^3 - 4x$$

такође има ранг нула. □

6 Програмски пакет SAGE

Као што смо неколико пута до сада приметили, при раду са елиптичким кривама често бројеви могу постати изузетно велики, што доводи до потешкоћа у ручном раду са њима. Зато ћемо користити помоћ рачунара. Употребићемо SageMath софтвер познатији као SAGE ("System for Algebra and Geometry Experimentation"). То је бесплатан open-source софтвер који покрива скоро све области математике: теорију бројева, графове, комбинаторику, алгебру, криптографију, па је изузетно погодан и за рад са елиптичким кривама.

6.1 Дефинисање елиптичке криве

Постоји више начина за дефинисање елиптичке криве у SAGE-у, а ми ћемо навести неколико основних које ћемо користити у даљем раду.

6.1.1 Вајерштрасова нормална форма

Елиптичка крива се може дефинисати када је у облику тзв. дуге Вајерштрасове нормалне форме који изгледа овако:

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

Сада се крива дефинише командом:

```
E=EllipticCurve([a_1,a_2,a_3,a_4,a_6])
```

Ако је крива записана у краткој Вајерштрасовој нормалној форми у облику:

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

криву дефинишемо следећом командом

```
E=EllipticCurve([a,b])
```

6.1.2 Дефинисање криве путем полинома

Ако нам тако одговара, криву можемо записати и помоћу полинома. Нпр криву $y^2 = x^3 + 1$ можемо дефинисати помоћу нехомогеног полинома на следећи начин:

```
P.<x,y>=QQ[];
p=y^2-x^3-1;
E=EllipticCurve(p)
```

Ако желимо да дефинишемо криву $y^2+y+2xy^2-x^3-2x^2-1 = 0$ дефинишемо помоћу хомогеног облика $ZY^2 + YZ^2 + 2XY^2 - X^3 - 2ZX^2 - Z^3 = 0$, мораћемо да дефинишемо и једну тачку на њој, нпр. тачку $P = (1, 1, 1)$. Овај начин нам даје трансформацију у Вајерштрасову нормалну форму. Команда изгледа овако:

```
R.<x,y,z> = QQ[];
cubic = z*y^2+y*z^2+2*x*y^2-x^3-2*z*x^2-z^3;
P = [1,1,1];
E = EllipticCurve_from_cubic(cubic, P, morphism=True);
E
-> Scheme morphism:
  From: Closed subscheme of Projective Space of dimension 2 over
Rational Field defined by:
  -x^3 + 2*x*y^2 - 2*x^2*z + y^2*z + y*z^2 - z^3
  To:   Elliptic Curve defined by y^2 - 2276766726*x*y -
```

```
875154115527458874759912976*y = x^3 + 43371280369600923*x^2 over
Rational Field
  Defn: Defined on coordinates by sending (x : y : z) to
        (-19609/158601998160000*x^2 + 137893/396504995400000*x*y -
969661/3965049954000000*y^2 - 13337/99126248850000*x*z +
46837/247815622125000*y*z - 33739/991262488500000*z^2 :
-5577903214129/158601998160000*x^2 + 48823377430993/396504995400000*x*y
- 411443597638381/3965049954000000*y^2 -
3096752644231/49563124425000*x*z + 51856165554479/495631244250000*y*z -
26112927303919/991262488500000*z^2 : 1/469192351880294390723616000*x^2
- 7/11729808797007359768090400000*x*y +
49/11729808797007359768090400000*y^2 +
1/5864904398503679884045200000*x*z - 7/29324521992518399420226000000*y*z
+ 1/29324521992518399420226000000*z^2)
```

На овом примеру заправо видимо зашто нам је рачунар од велике важности.

6.2 Остале команде

Остале команде које ће нам бити потребне показаћемо на примеру. Изучићемо криву

$$y^2 = x^3 - x^2 - 180x + 900.$$

За почетак дефинишемо криву.

```
E=EllipticCurve([0, -1, 0, -180, 900])
```

Ранг рачунамо на следећи начин

```
E.rank()
-> 1
```

Дакле крива има ранг 1. Сада рачунамо групу тачака коначног реда, тачке коначног реда и генераторе групе тачака коначног реда.

```
E.torsion_subgroup();
E.torsion_points();
E.torsion_subgroup().gens()
-> Torsion Subgroup isomorphic to Z/4 + Z/2 associated to the Elliptic
Curve defined by y^2 = x^3 - x^2 - 180*x + 900 over Rational Field
[(-15 : 0 : 1), (0 : -30 : 1), (0 : 1 : 0), (0 : 30 : 1),
 (6 : 0 : 1), (10 : 0 : 1), (20 : -70 : 1), (20 : 70 : 1)]
 ((0 : 30 : 1), (6 : 0 : 1))
```

Тачке са целобројним координатама, са позитивном y координатом рачунамо на следећи начин

```
E.integral_points();
->[(-15 : 0 : 1), (-10 : 40 : 1), (-8 : 42 : 1), (0 : 30 : 1),
 (5 : 10 : 1), (6 : 0 : 1), (10 : 0 : 1), (12 : 18 : 1),
 (20 : 70 : 1), (60 : 450 : 1), (90 : 840 : 1),(1700 : 70070 : 1)]
```

Следећа команда избацује низ генератора.

```
E.gens()
-> [(-10 : 40 : 1)]
```

Могуће је рачунати дисктиминанту и што је још важније, њену факторизацију на просте чиниоце.

```
E.discriminant();
E.discriminant().factor()
-> 70560000
2^8 * 3^2 * 5^4 * 7^2
```

Посматрајмо сада криву $y^2 = x^3 + 24$. Једноставна крива која има ранг 2.

```
Elliptic Curve defined by y^2 = x^3 + 24 over Rational Field
2
[(-2 : 4 : 1), (1 : 5 : 1)]
Torsion Subgroup isomorphic to Trivial group associated to the Elliptic
Curve defined by y^2 = x^3 + 24 over Rational Field
[(-2 : 4 : 1), (1 : 5 : 1), (10 : 32 : 1), (8158 : 736844 : 1)]
```

Показаћемо још како се сабирају тачке.

```
P=E(1,5);
Q=E(-2,4);
for i in range (1,5):
        P=P+Q
        P
    -> (10/9 : -136/27 : 1)
(457/49 : 9913/343 : 1)
(-85334/34225 : -18459536/6331625 : 1)
(73085377/363609 : -624807708677/219256227 : 1)
```

7 Задаци

Сада ћемо применити све научено до сада како бисмо урадили неке задатке.

Задатак 1. Пронаћи све природне бројеве n за које важи да је збир првих n квадрата потпун квадрат.

Решење: Према познатој формули рачунамо збир првих n квадрата

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Ова вредност треба да је једнака квадрату природног броја па је природно посматрати криву

$$Y^2 = \frac{X(X+1)(2X+1)}{6} = \frac{X^3}{3} + \frac{X^2}{2} + \frac{X}{6}.$$

Да бисмо пребацили криву у облик који смо користили у петој глави, уводимо смену координата $y = 72Y$ и $x = 18X$ па једначина добија облик

$$y^2 = x^3 + 18x^2 + 72x.$$

Желимо да пронађемо сва њена природна решења и то она (x, y) тако да важи $18 \mid x$ и $72 \mid y$. Користићемо SAGE да бисмо ово урадили.

```
E=EllipticCurve([0,18,0,72,0]);
E.integral_points()
->[(-12 : 0 : 1), (-9 : 9 : 1), (-8 : 8 : 1), (-6 : 0 : 1),
(0 : 0 : 1), (6 : 36 : 1), (12 : 72 : 1), (288 : 5040 : 1)]
```

Само последње две тачке задовољавају услове тако да су једина решења $n \in \{1, 24\}$ □

Задатак 2. *(ИМО 1986.)* Нека је d природан број такав да важи $d \notin \{2, 5, 13\}$. Доказати да је из скупа $\{2, 5, 13, d\}$ могуће изабрати два различита броја a и b тако да $ab - 1$ није потпун квадрат.

Решење На први поглед ово изгледа као обичан задатак из теорије бројева који нема никакве везе са елиптичким кривама, али када мало размислимо, веза ће бити очигледна. Како важи

$$2 \cdot 5 - 1 = 9, \quad 2 \cdot 13 - 1 = 25, \quad 5 \cdot 13 - 1 = 64$$

заправо желимо да докажемо да бар један од бројева $2d - 1$, $5d - 1$ и $13d - 1$ није потпун квадрат. Да би ово важило, довољно је да докажемо да њихов производ није квадрат односно да једначина

$$n^2 = (2d - 1)(5d - 1)(13d - 1) = 130d^3 - 101d^2 + 20d - 1$$

нема решења у скупу природних бројева. Сада увиђамо везу са елиптичким кривама. Једначина наведена горе је управо једначина елиптичке криве и ми желимо да докажемо да она нема решења у скупу природних бројева. Уводимо смену координата $y = 130n$ и $x = 130d$ да бисмо криву превели у облик где су коефицијенти уз y^2 и x^3 једнаки, који SAGE прихвата. Сада једначина има облик

$$y^2 = x^3 - 101x^2 + 2600x - 130^2 = (x - 10)(x - 26)(x - 65).$$

Сада позивамо рачунар у помоћ.

```
P.<x,y>=QQ[];
p=y^2-(x-10)*(x-26)*(x-65);
E=EllipticCurve(p); E.rank();
E.torsion_subgroup()
```

```
-> 0
Torsion Subgroup isomorphic to Z/2 + Z/2 associated to the Elliptic
Curve defined by y^2 = x^3 - 101*x^2 + 2600*x - 16900 over Rational
Field
```

Дакле крива има ранг 0 што значи да су једине рационалне тачке оне које имају коначан ред. Такође видимо да група тачака коначног реда има облик

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$$

односно група тачака коначног реда је сачињена само од тачака реда два. Дакле једина решења су

$$(x, y) \in \{O, (10, 0), (26, 0), (65, 0)\}$$

што одговара вредностима $d \in \{\frac{1}{2}, \frac{1}{5}, \frac{1}{13}\}$ што би значило да d није цео број. Овим је тврђење задатка доказано. □

Задатак 3. *(Велика Фермаова теорема за $n = 3$)* Доказати да једначина

$$x^3 + y^3 = z^3$$

нема нетривијалних решења у скупу целих бројева.

Решење Задатак решавамо директном применом SAGE-а

```
R.<x,y,z> = QQ[];
cubic = x^3+y^3-z^3;
P = [1,-1,0];
E = EllipticCurve_from_cubic(cubic, P, morphism=False);
E.rank();
E.torsion_subgroup();
-> 0
Torsion Subgroup isomorphic to Z/3 associated to the Elliptic Curve
defined by y^2 + 2*x*y + 1/3*y = x^3 - x^2 - 1/3*x - 1/27 over Rational
Field
```

Дакле крива има ранг нула и група рационалних тачака је изоморфна са $\mathbb{Z}/3\mathbb{Z}$, а те тачке одговарају тривијалним решењима. □

Задатак 4. *(Велика Фермаова теорема за $n = 4$)* Доказати да једначина

$$x^4 + y^4 = z^4$$

нема нетривијална решења у скупу рационалних бројева.

Решење Доказаћемо општије тврђење, да једначина

$$x^4 + y^4 = z^2$$

нема нетривијална решења у скупу рационалних бројева. Нека је (x, y, z) нетривијално решење, тј. $x, y, z \neq 0$. Једначина је еквивалентна са

$$\frac{x^4}{y^4} + 1 = \frac{z^2}{y^4}$$

Уводимо смену промењљивих $s = x/y$, $t = z/y^2$. Једначина постаје

$$s^4 + 1 = t^2.$$

Нека је $r = s^2$, па када ово помножимо са претходном једначином и заменимо $a = st$ добијамо

$$a^2 = r^3 + r.$$

Ово је заправо крива из примера 2 и њена једнина рационална тачка (нерачунајући O) је $(r, a) = (0, 0)$ што повлачи да је $x = 0$ чиме је тврђење задатка доказано. □

Задатак 5. Доказати да једначина

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

нема нетривијална решења у скупу рационалних бројева.

Решење Поступамо слично као и у претходном задатку. Нека је (x, y, z) нетривијално решење, тј. $x, y, z \neq 0$. Једначина је еквивалентна са

$$\frac{x^4}{y^4} - 1 = \frac{z^2}{y^4}$$

Уводимо смену променљивих $s = x/y$, $t = z/y^2$. Једначина постаје

$$s^4 - 1 = t^2.$$

Нека је $r = s^2$, па када ово помножимо са претходном једначином и заменимо $a = st$ добијамо

$$a^2 = r^3 - r.$$

Ово је заправо крива из примера 1 и њене једине рационалне тачке (нерачунајући O) су $(r, a) \in \{(0, 0), (1, 0), (-1, 0)\}$ што повлачи да је један од бројева x, z једнак нула чиме је тврђење задатка доказано. □

Задатак 6. Доказати да за сваки природан број N, постоји природан број m такав да једначина

$$x^3 + y^3 = m$$

има бар N целобројних решења.

Решење Идеја је да пронађемо једначину која има бесконачно много рационалних решења, па да ослобађањем од именилаца њених решења то постану решења неке друге једначине. Посматраћемо криву

$$X^3 + Y^3 = 9.$$

Помоћу пројективне трансформације уводимо смену

$$x = \frac{12}{X + Y}, \qquad y = \frac{12(X - Y)}{X + Y}$$

па једначина постаје

$$y^2 = x^3 - 48$$

Ова крива има тачку $P = (4, 4)$. Рачунамо: $2P = (28, -148)$, $3P = (\frac{73}{9}, \frac{595}{27})$. Пошто тачке коначног реда имају целобројне координате, закључујемо да тачка P има бесконачан ред па и крива има бесконачно много рационалних тачака.

Изаберимо сада N рационалних тачака са криве: $P_1, P_2, ..., P_N$. За тачку $R = \left(\frac{a}{b}, \frac{c}{d}\right)$ са криве, $(a, b) = (c, d) = 1$ важи

$$a^3d^3 + b^3c^3 = 9b^3d^3$$

па као много пута до сада закључујемо да важи $b = d$. Дакле можемо писати

$$P_i = \left(\frac{a_i}{d_i}, \frac{c_i}{d_i}\right), \quad i = 1, ..., N$$

Сада бирамо

$$m = 9(d_1 d_2 \cdots d_N)^3$$

и посматрамо тачке

$$Q_i = (d_1 \cdots d_{i-1} a_i d_{i+1} \cdots d_N, d_1 \cdots d_{i-1} c_i d_{i+1} \cdots d_N), \quad i = 1, ..., N$$

Свака од тачака Q_i представља решење једначине

$$x^3 + y^3 = 9(d_1 d_2 \cdots d_N)^3$$

па је овиме тврђење задатка доказано. □

Задатак 7. *(Румунски мастер 2016.)* Назовимо кубним низом низ целих бројева задат формулом

$$a_n = n^3 + an^2 + bn + c,$$

где су a, b и c целобројне константе а a_n пролази кроз све целе бројеве (укључујући негативне).

(а) Показати да постоји кубни низ такав да су једини потпуни квадрати у том низу a_{2015} и a_{2016}.

(б) Одредити све могуће вредности израза $a_{2015} \cdot a_{2016}$ за кубни низ који испуњава услов из дела (а).

Решење Посматраћемо криву $C: \ y^2 = x^3 + ax^2 + bx + c$. Транслацијом криве добијамо одговарајућу криву за коју доказујемо тврђење за a_0 и a_1. Прво ћемо урадити део под (б). Дакле крива има две целобројне тачке P и Q. Доказаћемо да једна од њих има ред два.

Претпоставимо супротно, да ни P ни Q немају ред два. Тада крива има још тачно две целобројне тачке (неукључујући O), $-P$ и $-Q$. Сада сабирамо P и Q по познатој формули.

$$x(P+Q) = \frac{(y_P - y_Q)^2}{(x_P - X_Q)^2} - a - x_P - x_Q = (y_P - y_Q)^2 - a - 1,$$

јер је $\{x_P, x_Q\} = \{0, 1\}$. По формулама из треће главе и $y(P+Q) \in \mathbb{Z}$. Дакле $P+Q$ има целобројне координате па важи једна од следеће четири једнакости

$$P + Q = P, \quad P + Q = Q, \quad P + Q = -P, \quad P + Q = -Q$$

Како је $P, Q \neq O$ прве две једнакости нису могуће па нека без умањења општости важи $P+Q = -P$ (*).

Аналогно, ако саберемо P и $-Q$, добијамо да је $P + (-Q) = -P$ или $P + (-Q) = Q$. Ако важи прва, комбиновањем са (*) добијамо $2Q = O$ па је то контрадикција. Дакле $2P = -Q$ и $2Q = P$. Сада је

$$\{x(2P), x(2Q)\} = \{0, 1\}$$

Примењујемо формулу дуплирања за тачке $x = 0$ и $x = 1$.

$$\frac{b^2 - 4ac}{4c} = 1, \qquad \frac{1 - 2b - 8c + b^2 - 4ac}{4 + 4a + 4b + 4c} = 0$$

$$b^2 - 4ac = 4c, \qquad 1 - 2b - 8c + b^2 - 4ac = 0$$

Када заменимо прву једначину у другу добијамо

$$1 = 2b + 4c$$

што је контрадикција јер су b и c цели бројеви.

Дакле на C постоји тачка реда два па је њена y координата нула па је и једина могућа вредност

$$a_0 \cdot a_1 = 0.$$

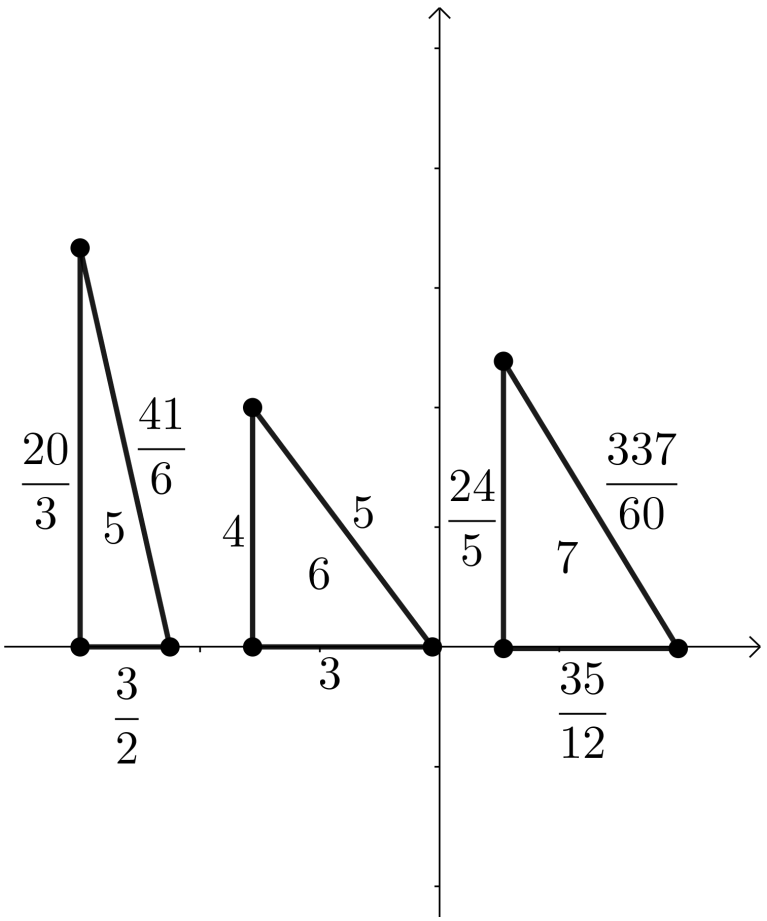
Што се тиче дела (а), лако се показује да крива

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

задовољава услове задатка.

Проблем конгруентних бројева

За крај, позабавићемо се једним проблемом који потиче још из старе Грчке. За природан број n кажемо да је конгруентан ако постоји правоугли троугао чије су дужине страница рационални бројеви, а површина једнака n. На слици су дати примери неких конгруентних бројева.



Слика 7: Примери конгруентних бројева

Тврђење 1. Природан број n је конгруентан ако и само ако постоји рационалан број x такав да су бројеви x, $x+n$ и $x-n$ квадрати рационалних бројева различити од нуле.

Доказ. Нека је n конгруентан број. Тада постоје $a, b, c \in \mathbb{Q}$ за које важи

$$a^2 + b^2 = c^2, \quad \frac{ab}{2} = n$$

Ако додамо и одузмемо другу једначину првој добијамо и поделимо са 4

$$\left(\frac{a+b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 + n, \quad \left(\frac{a-b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 - n$$

па $x = \left(\frac{c}{2}\right)^2$ задовољава услов задатка.
Нека сада постоји $x \in \mathbb{Q}$ такав да су бројеви x, $x+n$ и $x-n$ квадрати рационалних бројева.Тада постоје $u, v, w \in \mathbb{Q}$ тако да важи

$$u = \sqrt{x}, \quad v = \sqrt{x+n}, \quad w = \sqrt{x-n}.$$

Сада бирамо странице троугла на следећи начин

$$a = v + w, \quad b = v - w, \quad c = \sqrt{a^2 + b^2} = \sqrt{2v^2 + 2w^2} = \sqrt{4x} = 2u$$

Површина овог троугла износи

$$\frac{ab}{2} = \frac{v^2 - w^2}{2} = n$$

□

Сада је природно како ћемо повезати конгруентне бројеве и елиптичке криве. Посматраћемо криву

$$E_n : \ y^2 = x(x-n)(x+n) = x^3 - n^2x$$

Ако је n конгруентан из тврђења 1 следи да ће на кривој постојати рационална тачка са $y \neq 0$ односно рационална тачка која није реда два. Сада ћемо доказати да важи и обрнуто.

Тврђење 2. Природан број n је конгруентан ако и само ако на елиптичкој кривој E_n постоји рационална тачка $P = (x, y)$ са $y \neq 0$.

Доказ. Посматраћемо тачку $2P$. Користимо формулу дуплирања да бисмо израчунали њену x координату. За криву $y^2 = x^3 + ax^2 + bx + c$ важи

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

односно у нашем случају

$$x(2P) = \frac{x^4 + 2n^2x^2 + n^4}{4x^3 - 4n^2x} = \frac{(x^2 + n^2)^2}{(2y)^2}$$

Такође важи

$$x(2P) + n = \frac{x^4 + 2n^2x^2 + n^4 + 4x^3n - 4n^3x}{4x^3 - 4n^2x} = \frac{(x^2 + 2nx - n^2)^2}{(2y)^2}$$

$$x(2P) - n = \frac{x^4 + 2n^2x^2 + n^4 - 4x^3n + 4n^3x}{4x^3 - 4n^2x} = \frac{(x^2 - 2nx - n^2)^2}{(2y)^2}$$

Дакле n јесте конгруентан. □

Приметимо да смо кроз примере 1. и 2. из пете главе већ доказали да 1 и 2 нису конгруентни бројеви. Чињеница да 1 није конгруентан значи да ниједан квадрат није конгруентан, јер би онда и њему сличан n-пута мањи троугао имао рационалне странице и површину 1. Дакле у наставку можемо сматрати да n није квадрат. Сада ћемо рећи нешто више о групи рационалних тачака криве E_n.

Тврђење 3. Природан број n је конгруентан ако и само ако је ранг криве E_n позитиван.

Доказ. Ако је ранг позитиван постоји бесконачно много рационалних тачака са $y \neq 0$ па је овај смер тривијалан. Доказујемо други смер. Претпоставимо супротно, да је ранг E_n једнак нули. То значи да су једине рационалне тачке, тачке коначног реда. Сада ћемо искористити Мазуову теорему. У групи $Z/n\mathbb{Z}$ постоји само једна тачка реда два па овај случај није могућ. Дакле преостале су нам следеће четири могућмости за групу рационалних тачака G_t

$$G_t = \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}, \ \ G_t = \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}, \ \ G_t = \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{6\mathbb{Z}}, \ \ G_t = \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{8\mathbb{Z}}$$

1. случај: Нека је $G_t = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} = \{[0,0], [0,1], [0,2], [0,3], [1,0], [1,1], [1,2], [1,3]\}$. Како је $[0,2]$ тачка реда два и како важи

$$[0,1] + [0,1] = [0,2]$$

следи да на кривој E_n постоји тачка $P = (x, y)$ са $y \neq 0$ за коју важи $x(2P) \in \{-n, 0, n\}$. Добијамо три једначине

$$\frac{x^4 + 2n^2x^2 + n^4}{4x^3 - 4n^2x} = -n,$$

$$\frac{x^4+2n^2x^2+n^4}{4x^3-4n^2x}=0,$$
$$\frac{x^4+2n^2x^2+n^4}{4x^3-4n^2x}=n.$$

Прве две једначине очигледно немају решења а како n није квадрат нема их ни трећа па закључујемо

$$G_t \neq \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}$$

2. случај: Нека је $G_t = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} = \{[0,0],[0,1],[0,2],[0,3],[0,4],[0,5],[0,6],[0,7],[1,0],$ $[1,1],[1,2],[1,3],[1,4],[1,5],[1,6],[1,7]\}$. Како је $[0,4]$ тачка реда два и како важи

$$[1,2]+[1,2]=[0,4]$$

аналогно као и у претходном случају добијамо контрадикцију и закључујемо да важи

$$G_t \neq \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{8\mathbb{Z}}$$

3. случај: Нека је $G_t = \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z} = \{[0,0],[0,1],[0,2],[0,3],[0,4],[0,5],[1,0],[1,1],[1,2],[1,3],[1,4],[1,5]\}$. Како $[0,2]$ има ред три, крива ће имати тачку реда три, односно тачку $P=(x,y)$ за коју важи

$$3x^4+4ax^3+6bx^2+12cx+(4ac-b^2)=0$$

односно у нашем случају

$$3x^4-6n^2x^2+n^4=0$$

Уведимо смену $t=\frac{x^2}{n^2}$. Једначина постаје

$$3t^2-6t+1=0.$$
$$t_{1/2}=\frac{6\pm\sqrt{36-12}}{2}=3\pm\sqrt{6}$$

Дакле

$$x=\pm n\sqrt{3\pm\sqrt{6}}.$$

Ни једно од ова четири решења није рационално тако да добијамо контрадикцију и важи

$$G_t \neq \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{6\mathbb{Z}}$$

Коначно, једино што је преостало је да важи

$$G_t = \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

Ово значи да су једине рационалне тачке на кривој тачке $\{(0,0),(-n,0),(n,0)\}$ што је у контрадикцији са тим да је n конгруентан. □

За крај, пронаћи ћемо који су од првих 100 бројева конгруентни.

```
for i in range(1,101):
    a=-i*i
    E=EllipticCurve([a,0])
    if E.rank()>0:
        print(i)
    ->5,6,7,13,14,15,20,21,22,23,24,28,29,30,31,34,37,38,39,41,45,46,47,
    52,53,54,55,56,60,61,62,63,65,69,70,71,77,78,79,80,84,85,86,87,
    88,92,93,94,95,96
```

8 Закључак

Циљ овог матурског рада био је да представи елиптичке криве и посматра их са становишта теорије бројева. Осварили смо могућност да решавамо велику класу Диофантових једначина, а успут смо се и упознали са софтвером *SAGE*. Урадили смо много тога, али смо тек загребали по површини теорије о елиптичким кривама. Наставак ове приче било би њихово проучавање на другим пољима где би нека тврђења која смо доказали и даље важила. Такође, важно је напоменути да елиптичке криве имају велику примену у рачунарству, а посебно у криптографији и алгоритми који се користе, засновани су на принципима којима смо се бавили кроз овај матурски рад.

За крај желео бих да изразим велику захвалност

- **Стевану Гајовићу** – мом ментору, на изузетном стрпљењу, времену које ми је посветио док сам писао овај рад, свим сугестијама, добронамерним критикама и пренетом знању.
- **Милошу Ђорићу** – мом професору анализе са алгебром, који ми је својим несебичним залагањем и преношењем знања током све четири године у Математичкој гимназији још више учвстио већ постојећу љубав према математици.

9 Литература

[1] Joseph H. Silverman, John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1995.

[2] Filip Najman, *Eliptičke krivulje nad poljima algebarskih brojeva*, Prirodoslovno matematički fakultet, 2013.

[3] Allan J. MacLeod, *Elliptic Curves in Recreational Number Theory*, University of West Scotland, 2016.

[4] Keith Conrad, *The Congruent Number Problem*, University of Connecticut, 2007.

[5] J.S.Milne, *Elliptic Curves*, University of Michigan, 1996.

[6] Andrej Dujella, *Eliptičke krivulje u kriptografiji*, Prirodoslovno matematički fakultet, 2013.

[7] `https://web.math.pmf.unizg.hr/~duje/ecc/eccseminar.html`

[8] `http://planetmath.org/mazurstheoremontorsionofellipticcurves`

[9] `https://sage.math.leidenuniv.nl/home/pub/25/`

[10] `http://srb.imomath.com/`