0.1 Krive trećeg reda

Kriva trećeg reda u afinoj ravni $\mathbb{A}^2_K$ zadata je polinomijalnom jednačinom trećeg reda

$$f(x,y) \equiv f_3(x,y) + f_2(x,y) + f_1(x,y) + f_0 = 0$$

gde su f_i homogene komponente polinoma f stepena i $(i = 0,1,2,3)$. Dakle,

$$\begin{aligned} f_3(x,y) &= a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3 \\ f_2(x,y) &= a_{20}x^2 + a_{11}xy + a_{02}y^2 \\ f_1(x,y) &= a_{10}x + a_{01}y \\ f_0(x,y) &= a_{00} \end{aligned}$$

gde je označavanje koeficijenata razumljivo: prvi indeks označava stepen x, drugi stepen y.

Da bi uspešno sproveli klasifikaciju ovih krivih, neophodno je da detaljnije razmotrimo neke pojmove koji su se javljali već kod krivih drugog reda.

Ireducibilnost

Neka je $\mathcal{C} : f(x,y) = 0$ algebarska kriva stepena n. Ako je polinom f rastavljiv tj. ako dopušta pravu faktorizaciju $f = g \cdot h$, $\deg g$, $\deg h < \deg f = n$ tada je kriva $\mathcal{C} = \mathcal{G} \cup \mathcal{H}$ unija dve algebarske krive manjeg stepena. Kažemo da je kriva $\mathcal{C}$ *reducibilna* ili *svodljiva*, a krive $\mathcal{G}$ i $\mathcal{H}$ su njene *komponente*. Ako je pak polinom f nerastavljiv, kriva $\mathcal{C}$ je *ireducibilna* ili *nesvodljiva*. Zbog jednoznačnosti faktorizacije u prstenu polinoma $K[x,y]$, svaka se kriva može rastaviti u uniju svojih ireducibilnih komponenti. Komponenta $g = 0$ može imati višestrukost $k > 1$ ako je k višestrukost nerastavljivog faktora g u polinomu f.

Primer. Kvadrika u kompleksnoj ravni je reducibilna ako i samo ako je unija dve prave (koje mogu biti i podudarne). Ireducibilne kvadrike su samo elipsa, hiperbola i parabola.

Singularne tačke

Neka je sad $A(x_0,y_0)$ tačka krive $\mathcal{C}$, tj. $f(x_0,y_0) = 0$. Translacijom afine ravni (tj. zamenom koordinatnog početka) možemo smatrati da je $A = O(0,0)$, dakle $f(0,0) = 0$.

Jednačinu krive zapišimo kao zbir homogenih komponenti

$$f(x,y) = f_n(x,y) + f_{n-1}(x,y) + \cdots + f_k(x,y) = 0$$

gde je n stepen krive, a $k \leq n$ najmanji stepen za koji je $f_k(x,y) \neq 0$. Ovaj se stepen naziva višestrukošću polinoma f u nuli ili višestrukošću tačke O na krivoj $\mathcal{C}$. Tačka $O(0,0)$ je *regularna tačka* krive $\mathcal{C}$ ako je $k = 1$, inače (ako je $k \geq 2$) kažemo da je to *singularna tačka* krive $\mathcal{C}$, višestrukosti $k \geq 2$.

Primer. Posmatrajmo tzv. kasp krivu (eng. *cusp* - tačka preokreta, šiljak, rus. *točka vozvrata*) $y^2 = x^3$. Očigledno, $f_3 = -x^3$, $f_2 = y^2$ pa je tačka O singularna tačka višestrukosti 2.

Ako potražimo analogiju u matematičkoj analizi, vidimo da je singularna tačke krive $f(x, y) = 0$ upravo ona tačka u kojoj su oba parcijalna izvoda jednaka nuli: $\frac{\partial f}{\partial x} = 0, \frac{\partial f}{\partial y} = 0$, tj. tačka za koju ne važe uslovi teoreme o implicitnoj funkciji. Skup singularnih tačaka krive $f(x, y) = 0$ u afinoj ravni $\mathbb{A}^2_K$ se može okarakterisati kao skup rešenja sistema jednačina

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

Primetimo da ovaj sistem opisuje samo konačne, a ne i beskonačno daleke tačke. Da bi proverili da li je i neka od beskonačno dalekih tačaka naše krive singularna, moramo preći u drugu afinu kartu.

Primer. Kriva $y = x^3$ u konačnoj ravni $\mathbb{A}^2_K$ nema singularnih tačaka, jer sistem

$$\begin{aligned} x^3 - y &= 0 \\ 3x^2 &= 0 \\ -1 &= 0 \end{aligned}$$

nema rešenja. Da bi videli šta se dešava na beskonačno dalekoj pravoj $\mathbb{P}^1_K$, homogenizujmo jednačinu. Dobijamo jednačinu $X^3 - YZ^2 = 0$ koja u afinoj karti $Y \neq 0$ prelazi u jednačinu $z^2 = x^3$ "cusp"-krive i sistem

$$\begin{aligned} x^3 - z^2 &= 0 \\ 3x^2 &= 0 \\ -2z &= 0 \end{aligned}$$

ima jedinstveno rešenje $x = 0$, $z = 0$. To je singularna tačka te krive čije su homogene koordinate $(0 : 1 : 0)$. U polaznoj afinoj karti $Z \neq 0$ ova se tačka ne vidi jer leži na beskonačno dalekoj pravoj $Z = 0$. To je beskonačno daleka tačka koordinatne prave $x = 0$.

Procedura nalaženja singularnih tačaka može se sprovesti i direktno preko homogenih koordinata u projektivnoj ravni. Ako je $F(X, Y, Z)$ homogenizacija polinoma $f(x, y)$ u odnosu na koordinate $x = \frac{X}{Z}, y = \frac{Y}{Z}$, tada je skup singularnih tačaka odredjen sistemom

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

Primer. U prethodnom primeru, taj sistem je $X^3 - YZ^2 = 3X^2 = -Z^2 = -2YZ = 0$ što nam daje rešenje $X = 0, Z = 0$ i sledstveno $Y = 1$ tj. jedinstvenu singularnu tačku $(0 : 1 : 0)$.

Jedno klasično svojstvo homogenih polinoma, Ojlerovu formulu, koristićemo u daljem. Moguće je da ste je već koristili u matematičkoj analizi.

Tvrdjenje (Ojlerova formula).

Tangenta

Uočimo proizvoljnu pravu kroz koordinatni početak

$$\begin{cases} x = \alpha t \\ y = \beta t \end{cases}$$

sa koeficijentom nagiba (α, β). Očigledno, kriva i ta prava seku se u tački O. Prava je *tangenta* krive $\mathcal{C}$ u tački $(0,0)$ ako je višestrukost preseka u toj tački veća od 1 (po Bezuovoj teoremi višestrukost može biti najviše n) tj. ako je $f_1(\alpha, \beta) = 0$. U običnoj regularnoj tački tangenta je odredjena jednoznačno i višestrukost preseka tangente sa krivom jednaka je 2. Regularna tačka je *prevojna tačka* (eng. *inflection point,* rus. *točka peregiba*) ako je višesturkost preseka u toj tački veća od 2. U singularnoj tački tangenta nije jednoznačno odredjena, a skup svih tangenti u toj tački je *tangentni prostor* u toj tački, pa je u tom smislu tangentni prostor krive u regularnoj tački dimenzije 1, a u singularnoj tački dimenzije 2 (cela ravan).

Primer. Na krivoj $y = x^3$, $f_3(x,y) = x^3, f_2(x,y) = 0, f_1(x,y) = -y$. Tačka $O(0,0)$ je regularna tačka jer u toj tački f_1 nije identički 0. Tangenta u toj tački je prava $y = 0$. Višestrukost preseka sa krivom je 3 jer je u toj tački $f_2 = 0$ (u stvari, $f_2 \equiv 0$). Zato je to prevojna tačka. U tački $A(1,1)$ jednačina krive je $(y-1) = (x-1)^3 + 3(x-1)^2 + 3(x-1)$, pa je $f_3 = (x-1)^3$, $f_2 = 3(x-1)^2$, $f_1 = 3(x-1) - (y-1)$. Tangenta je $3x - y - 2 = 0$, odnosno $y = 3x - 2$, ali je višestrukost preseka sa krivom jednaka 2. Treća tačka preseka odredjena je rešenjem jednačine $x^3 - 3x + 2 = 0$ različitim od 1, a to je -2 odnosno tačka $(-2, -6)$.

Nadjimo višestrukost preseka u toj tački. Ako zamenimo parametarske jednačine prave u jednačinu krive, dobijamo polinom

$$f(\alpha t, \beta t) = f_n(\alpha, \beta)t^n + f_{n-1}(\alpha, \beta)t^{n-1} + \cdots + f_k(\alpha, \beta)t^k = 0$$

stepena n po t čiji je koren $t = 0$ višestrukosti k. To je najmanja moguća višestrukost preseka krive i prave u tački O. Ako je tačka singularna, onda je svaka prava kroz tu tačku - tangenta. Medjutim, za pojedine prave višestrukost može biti i veća. Uočimo koeficijent $f_k(\alpha, \beta)$ uz t^k kao funkciju promenljivih α, β. To je netrivijalni ($f_k \neq 0$) homogeni polinom stepena k po tim promenljivim. On se razlaže u proizvod linearnih faktora $f_k(\alpha, \beta) = l_1^{m_1}(\alpha, \beta) \cdot \cdots \cdot l_p^{m_p}(\alpha, \beta), m_1 + \cdots + m_p = k$. Za poseban, konačan izbor tačaka $(\alpha_i : \beta_i) \in \mathbb{P}^1_K$ $(i = 1, \ldots, p)$ (beskonačno dalekih tačaka koje odgovaraju pravim $l_i(\alpha, \beta) = 0$) biće $f_k(\alpha, \beta) = 0$. Te su prave - prave tangentnog konusa krive $\mathcal{C}$ u tački $O(0,0)$, svaka ima odgovarajuću višestrukost m_i. *Tangentni konus* krive $\mathcal{C}$ u tački $O(0,0)$ je algebarska kriva reda k definisana jednačinom $f_k(x,y) = 0$.

Zadatak. Nadjite tangentne konuse krivih $xy = 1, xy = 0, y = x^3, y^2 = x^3$.

Krive trećeg reda

Posmatrajmo projektivno zatvorenje ireducibilne krive trećeg reda u projektivnoj ravni $\mathbb{P}^2_K$ u kojoj je $\mathbb{A}^2_K$ afina karta $Z \neq 0$. Dato je jednačinom

$$F(X,Y,Z) \equiv f_3(X,Y) + f_2(X,Y)\cdot Z + f_1(X,Y)\cdot Z^2 + f_0 \cdot Z^3 = 0.$$

Analiziraćemo prvo slučaj kada kriva ima singularnu tačku u $O(0,0)$. Višestrukost k singularne tačke može biti 2 ili 3. Ako je $k = 3$, kriva ima jednačinu $f_3(x,y) = 0$, homogeni polinom 3 stepena se razlaže u proizvod tri linearna faktora $f_3(x,y) = l_1(x,y)\cdot l_2(x,y)\cdot l_3(x,y)$ pa je kriva C reducibilna, unija tri prave koje se seku u jednoj tački. Zavisno od toga da li su sve te prave medjusobno različite imamo tri moguća slučaja, predstavljena jednačinama $xy(x-y) = 0$, $x^2y = 0$ i $x^3 = 0$.

Interesantniji je slučaj singularne tačke višestrukosti 2. Primetimo da može postojati samo jedna takva tačka. Ako bi postojale dve različite tačke, tada bi prava kroz te dve tačke sekla krivu trećeg reda sa višestrukošću $2+2 = 4 > 3$, što je nemoguće. Prenesimo koordinatni početak u singularnu tačku. Na osnovu svega rečenog, jednačina krive biće $f(x,y) \equiv f_3(x,y) + f_2(x,y) = 0$ sa tangentnim konusom $f_2(x,y) = 0$. Polinom $f_2(x,y)$ se rastavlja u proizvod dva linearna faktora i imamo dva moguća slučaja: faktori su različiti ili se poklapaju. U prvom slučaju odgovarajućim izborom koordinatnih osa možemo postići da je $f_2(x,y) = x^2 - y^2$, u drugom $f_2(x,y) = y^2$. Ova dva slučaja imaju predstavnike opisane jednačinama $y^2 = x^2(x-1)$ i $y^2 = x^3$. Prva se naziva α-kriva, a druga kasp-kriva ili polukubna parabola. Skicirajte njihove grafike i nadjite njihovo projektivno zatvorenje.

Vratimo se opštem slučaju. Neka je nesvodljiva kriva $\mathcal{C}$ u ravni $\mathbb{P}^2_K$ zadata jednačinom

$$F(X,Y,Z) \equiv f_3(X,Y) + f_2(X,Y)\cdot Z + f_1(X,Y)\cdot Z^2 + f_0 \cdot Z^3 = 0.$$

Pokušajmo da projektivne koordinatne prave $X = 0$, $Y = 0$, $Z = 0$ (tzv. projektivni koordinatni trougao) izaberemo na takav način da jednačina postane što je moguće jednostavnija. Osim afinih transformacija koristićemo homogenizaciju i dehomogenizaciju i projektivne (biracionalne) transformacije.

Za koordinatni početak O izaberimo regularnu tačku na krivoj $\mathcal{C}$, za osu $Z = 0$ tangentu p na krivu $\mathcal{C}$ u tački O. Na osnovu Bezuove teoreme, ona seče krivu $\mathcal{C}$ u trećoj tački A. Uzmimo za osu $X = 0$ tangentu q na krivu $\mathcal{C}$ u tački A. Kao treću osu $Y = 0$ izaberimo bilo koju pravu kroz O različitu od prave $Z = 0$. U takvom koordinatnom sistemu koordinate tačke O su $(1:0:0)$ a tačke $A(0:1:0)$. Uslovi da $O \in \mathcal{C}$ i $A \in \mathcal{C}$ daju $a_{30} = 0$ i $a_{03} = 0$. Uslov da je p tangenta u O daje $a_{21} = 0$, a uslov da je q tangenta u A daje $a_{02} = 0$ (proveriti!). U tom koordinatnom sistemu jednačina krive je

$$a_{20}X^2Z + a_{11}XYZ + a_{12}XY^2 + a_{10}XZ^2 + a_{01}YZ^2 + a_{00}Z^3 = 0.$$

Pri tome, koeficijent $a_{12} \neq 0$ jer bi u protivnom kriva bila reducibilna. Posle skraćivanja sa a_{12} i dehomogenizacije po Z, u afinoj karti $Z \neq 0$ sa koordinatama $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ jednačina poprima oblik

$$xy^2 + (ax+b)y = cx^2 + dx + e.$$

Pomnožimo je sa x

$$x^2y^2 + (ax + b)xy = cx^3 + dx^2 + ex$$

i dopunimo do potpunog kvadrata

$$(xy + \frac{1}{2}ax + \frac{1}{2}b)^2 = cx^3 + (d + \frac{1}{4}a^2)x^2 + (\frac{1}{2}a + e)x + \frac{1}{4}b^2.$$

Ovde se radi o projektivnoj (biracionalnoj) transformaciji

$$\begin{aligned} x_1 &= x \\ y_1 &= xy + \frac{1}{2}ax + \frac{1}{2}b. \end{aligned}$$

Inverzna transformacija je data formulama

$$\begin{aligned} x &= x_1 \\ y &= \frac{y_1 - \frac{1}{2}ax_1 - \frac{1}{2}b}{x_1} \end{aligned}$$

i veze izmedju (x, y) i (x_1, y_1) su opisane racionalnim funkcijama, odakle termin "biracionalna". Ovde se radi o jednoj specijalnoj biracionalnoj transformaciji koja nosi naziv "blow-up", σ-proces ili razduvavanje (ruski termin "razdutie", nisam mogao da smislim bolji termin, konkurs je otvoren i bolji predlozi su dobrodošli). Definitivno dobijamo jednačinu oblika

$$y^2 = P_3(x)$$

gde je $P_3(x)$ normirani polinom po x trećeg stepena, $P_3(x) = x^3 + px^2 + qx + r$. Ovaj oblik jednačine naziva se *Vajerštrasov oblik* jednačine krive trećeg reda. Dakle, svaka kriva trećeg reda se projektivnim transformacijama može svesti na Vajerštrasov oblik. U odnosu na broj različitih korena polinoma $P_3(x)$ imamo tri slučaja: prvi, sva tri korena se poklapaju; drugi, dva su jednaka i treći različit; treći, sva tri korena su različita. U prvom slučaju, linearna smena dovodi do jednačine $y^2 = x^3$ što je kasp-kriva. U drugom, linearna smena dovodi do jednačine $y^2 = x^2(x - \lambda)$ što je α-kriva. Najzad, treći slučaj predstavlja krivu trećeg reda bez singulariteta i elementarnim smenama se može svesti na oblik $y^2 = x(x-1)(x-\lambda)$ $(\lambda \neq 1)$. Ovakve krive nazivaju se i *eliptičke krive*. Sama jednačina se afinom transformacijom (translacijom duž x-ose tj. Čirnhauzenovom transformacijom) može svesti na oblik

$$y^2 = x^3 + px + q.$$

Opisani postupak svodjenja preuzet je iz knjige Silvermana i Tejta[1]. Postoji i jednostavniji način svodjenja na Vajerštrasov oblik, kako ga u svojoj knjizi

[1]Silverman J.H., Tate J.T.: Rational Points on Elliptic Curves. Undergraduate texts in mathematics, Springer, Berlin-Heidelberg-New York, 2015

opisuju Prasolov i Solovjov[2], način koji uopšte ne zahteva projektivne odnosno biracionalne, već isključivo afine transformacije, ali koristi neke osobine prevojnih tačaka.

Prevojne tačke i Hesijan krive

Neka je $f(x,y) = 0$ jednačina algebarske krive i $O(0,0)$ njena prevojna tačka. To znači da je tačka $O(0,0)$ regularna i da je njena višestrukost ≥ 3. Dakle, $f(\alpha t, \beta t) = f_n(\alpha,\beta)t^n + \cdots + f_2(\alpha,\beta)t^2 + f_1(\alpha,\beta)t$ pri čemu mora biti $f_1 \neq 0$, $f_1(\alpha,\beta) = f_2(\alpha,\beta) = 0$, gde je $x = \alpha t, y = \beta t$ jednačina tangente u $O(0,0)$. Ako definišemo Hesijan jednačine f kao polinom $Hf(x,y) = \det \begin{pmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial y^2} \end{pmatrix}$, tada je ova matrica - matrica kvadratne forme $f_2(x,y)$ i (α,β) je nula jednačine $Hf(x,y) = 0$. Može se pokazati i obrnuto, tj. prevojne tačke krive $f(x,y) = 0$ u afinoj karti $Z \neq 0$ su upravo rešenja sistema

$$f(x,y) = Hf(x,y) = 0.$$

Pri tome ne vidimo beskonačno daleka rešenja ovog sistema. Medjutim, slično kao kod tangenti, ovaj sistem ima i homogenu varijantu. Može se pokazati da svaka kubna kriva ima prevojnu tačku. Tačnije, Hesijan kubne krive je opet kubna kriva (primena rezultante) i po Bezuovoj teoremi ima $9 = 3 \cdot 3$ prevojnih tačaka (ako ih računamo sa višestrukostima).

Primer. Uočimo kubiku $y = x^3$. Homogenizovana jednačina je $X^3 - YZ^2 = 0$. Hesijan je $\begin{vmatrix} 6X & 0 & 0 \\ 0 & 0 & -2Z \\ 0 & -2Z & -2Y \end{vmatrix} = -24XZ^2$. Presek $F(X,Y,Z) = H(X,Y,Z) = 0$ dve kubne krive ima rešenja $(0:0:1)$ i $(0:1:0)$ višestrukosti 3 i 6 respektivno. U karti $Z \neq 0$ tj. ravni (x,y) nalazi se jedna trostruka tačka i to je prevojna tačka naše kubne parabole. U karti $Y \neq 0$ tj. ravni (x,z) nalazi se šestostruka tačka preseka krive i Hesijana, ali to je singularna tačka krive, a ne njena prevojna tačka (definicija prevojne tačke podrazumeva da se radi o regularnoj, a ne singularnoj tački).

Afino svodjenje na Vajerštrasov oblik

Svedimo sad jednačinu kubne krive u projektivnoj ravni $F(X,Y,Z) = 0$ na Vajerštrasov oblik. Translacijom koordinatnog sistema možemo smatrati da je ta prevojna tačka $(0:1:0)$. Izaberimo ose tako da tangenta u toj tački ima jednačinu $z = 0$ u odgovarajućoj afinoj karti $Y \neq 0$. Pošto je $(0,0)$ prevojna tačka i tangenta je x-osa, višestrukost tačke na krivoj jednaka je 3. To znači da je $f_3(x,y) = a_{30}x^3$ sa $a_{30} \neq 0$ (u suprotnom bi prava $z = 0$ bila komponenta

[2]Prasolov V. V., Solov'ev Yu. P.: Ellipticheskie funkcii i algebraicheskie uravneniya. Faktorial, Moskva, 1997.

krive). Homogena jednačina tangente u tački $(0:1:0)$ je

$$\frac{\partial F}{\partial X}(0:1:0)\cdot X+\frac{\partial F}{\partial Y}(0:1:0)\cdot Y+\frac{\partial F}{\partial Z}(0:1:0)\cdot Z=0.$$

Ali tačka $(0:1:0)$ je regularna, pa mora biti $\frac{\partial F}{\partial X}(0:1:0)=\frac{\partial F}{\partial Y}(0:1:0)=0, \frac{\partial F}{\partial Z}(0:1:0)\neq 0$. To znači da je $a_{02}\neq 0$. Skaliranjem možemo postići da je $a_{02}=1$. Posle dehomogenizacije jednačine $F(X,Y,Z)=0$ u karti $Z\neq 0$ (stavljanjem $Z=1$) dobijamo jednačinu

$$y^2-2(ax+b)y+P_3(x)=0$$

odakle dopunom do potpunog kvadrata (što je afina transformacija)

$$\begin{aligned} x_1 &= x \\ y_1 &= y-ax-b \end{aligned}$$

dobijamo Vajerštrasov oblik koji se daljom afinom transformacijom (translacijom i skaliranjem duž x-ose) može svesti na

$$y^2=x^3+px+q$$

Grupa na eliptičkoj krivoj

Neka je $\mathcal{C}$ eliptička kriva zadata Vajerštrasovom jednačinom oblika

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

gde polinom na desnoj strani ima tri različita korena $x^3+ax^2+bx+c=x(x-1)(x-\lambda)$ (potrebna translacija i skaliranje). Homogenizacijom ove jednačine dobijamo

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

Na beskonačno dalekoj pravoj $Z=0$ imamo $x^3=0$ odnosno $x=0$, što znači da je jedina tačka krive na beskonačno dalekoj pravoj $(0:1:0)$. Njena višestrukost na krivoj se vidi iz odgovarajuće jednačine $z=x^3+ax^2z+bxz^2+cz^3$ u afinoj karti $Y\neq 0$ i jednaka je 1. To je tačka O. Prava paralelna y-osi u afinoj karti (x,y) seče krivu u dve tačke, simetrične u odnosu na x-osu. Ovim je generisano preslikavanje $P\mapsto P'$ za tačke na krivoj koje se u afinim koordinatama vidi kao refleksija u odnosu na koordinatnu osu.

Definišimo operaciju nad tačkama na krivoj sa

$$P+Q:=(\text{treća presečna tačka prave kroz } P \text{ i } Q)'.$$

Ova se operacija može zapisati i ovako: $P+Q+R=O$ gde je O beskonačno daleka tačka krive $\mathcal{C}$. Pri tome je $P'=-P$, jer je $P+P'+O=O$ odnosno $P'=-P$.

Teorema. Ovim pravilom zadata je binarna operacija na skupu tačaka krive $\mathcal{C}$, koja pretvara krivu $\mathcal{C}$ u Abelovu grupu, tzv. grupu tačaka eliptičke krive $\mathcal{C}$.

Dokaz se sastoji u direktnoj proveri aksioma grupe koja sledi iz geometrijske realizacije krive i Bezuove teoreme. Neutralni element je beskonačno daleka tačka $O(0:1:0)$, a suprotni element za tačku P je tačka njoj simetrična u odnosu na x-osu. Komutativnost je očigledna. Jedina aksioma koja zahteva proveru je asocijativni zakon. U tom cilju potrebno nam je pomoćno tvrdjenje.

Lema. Ako kriva trećeg reda prolazi kroz osam tačaka preseka dve familije po tri prave, ona prolazi i kroz devetu tačku preseka.

Dokaz. Neka imamo dve familije po tri prave $\mathcal{P} = \{p_1, p_2, p_3\}$ i $\mathcal{Q} = \{q_1, q_2, q_3\}$ i neka su njihove jednačine $p_i(x, y) = 0, q_j(x, y) = 0$. One odredjuju tri (degenerisane) krive trećeg reda $P : p_1(x, y)p_2(x, y)p_3(x, y) = 0$ i $Q : q_1(x, y)q_2(x, y)q_3(x, y) = 0$ koje se na osnovu Bezuove teoreme seku u devet tačaka $A_{ij} = p_i \cap q_j$. Kubna kriva $\mathcal{D} : \alpha p_1p_2p_3 + \beta q_1q_2q_3 = 0$ prolazi kroz svih devet tačaka. Pretpostavimo da kubna kriva C sadrži sve tačke A_{ij} osim, eventualno, tačke A_{33}. Dokažimo da onda ona mora da sadrži i A_{33}. U tom cilju dokažimo da se jednačina krive C može predstaviti u obliku $\mathcal{D}$. Za koordinatni početak možemo izabrati tačku A_{11} a za koordinatne ose prave p_1 i q_1, tj. možemo smatrati da je $p_1(x, y) = y$ i $q_1(x, y) = x$. Neka je $P(x, y) = 0$ jednačina krive C u tom koordinatnom sistemu. Polinomi $P(0, y)$ i $yp_2(0, y)p_3(0, y)$ stepena najviše 3 jednaki su nuli u tri kolinearne tačke A_{11}, A_{21} i A_{31} koje leže na y-osi. Zato su oni proporcionalni, tj. $P(0, y) = \alpha yp_2(0, y)p_3(0, y)$. Isto tako, $P(x, 0) = \beta xq_2(x, 0)q_3(x, 0)$. Uočimo polinom $Q(x, y) = P(x, y) - \alpha yp_2(x, y)p_3(x, y) - \beta xq_2(x, y)q_3(x, y)$ i dokažimo da je on identički jednak 0. Očigledno, $Q(0, y) \equiv 0$. Odatle sledi da $x \mid Q$. Isto tako i $y \mid Q$, pa je $Q(x, y) = xy \cdot l(x, y)$ gde je stepen polinoma l najviše 1. Primetimo da je u tačkama A_{22}, A_{23}, A_{32} polinom $P(x, y) = p_2(x, y)p_3(x, y) = q_2(x, y)q_3(x, y) = 0$. Odatle sledi da je u tim tačkama i $Q(x, y) = 0$. Ali u tim tačkama je $xy \neq 0$, pa u njima mora biti $l(x, y) = 0$. Medjutim, ovo je jednačina prave, a te tačke nisu kolinearne, pa zato mora biti $l(x, y) \equiv 0$, $Q(x, y) \equiv 0$ i $P(x, y) = \alpha yp_2(x, y)p_3(x, y) + \beta xq_2(x, y)q_3(x, y)$. Zato i tačka A_{33} leži na krivoj $\mathcal{C}$.

Dokažimo da je operacija sabiranja tačaka na eliptičkoj krivoj asocijativna. Neka su P, Q, R tri tačke na eliptičkoj krivoj $\mathcal{C}$ i neka je $P+Q = S$ i $Q+R = T$. Treba dokazati da je $R+S = P+T$. Uočimo tri prave $p_1(QR)$, $p_2(OS)$, $p_3(PT)$ kao i tri prave $q_1(PQ)$, $q_2(OT)$, $q_3(RS)$. Osam presečnih tačaka ovih pravih su $p_1 \cap q_1 = Q$, $p_1 \cap q_2 = -T$, $p_1 \cap q_3 = R$, $p_2 \cap q_1 = -S$, $p_2 \cap q_2 = O$, $p_2 \cap q_3 = S$, $p_3 \cap q_1 = P$, $p_3 \cap q_2 = T$ i one sve leže na krivoj $\mathcal{C}$. Zato se i deveta presečna tačka $p_3 \cap q_3$ nalazi na krivoj $\mathcal{C}$. Ali to znači da je treća presečna tačka krive $\mathcal{C}$ i prave p_3 (tačka $-(P + T)$) ista kao i presečna tačka krive $\mathcal{C}$ i prave q_3 (tačka $-(R + S)$). Odatle sledi asocijativnost.