Galoisove reprezentacije pridružene eliptičkim krivuljama

Filip Najman

1. predavanje

2.11.2020.

Osnovne informacije o kolegiju

- napredni kolegij na Doktorskom studiju PMF-MO.

Osnovne informacije o kolegiju

- napredni kolegij na Doktorskom studiju PMF-MO.

Termin održavanja: utorkom 10-12

Osnovne informacije o kolegiju

- napredni kolegij na Doktorskom studiju PMF-MO.

Termin održavanja: utorkom 10-12

Korisne reference:

- Skripta A. Dujella: Eliptičke krivulje u kriptografiji
- Moja skripte: Eliptičke krivulje nad poljima algebarskih brojeva
- J.–P. Serre : Abelian ℓ-adic representations attached to elliptic curves
- J. Silverman: Arithmetic of elliptic curves
- J. Silverman: Advanced topics in the artihmatic of elliptic curves
- L. Washington: Elliptic cuvres
- S. Siksek: Explicit methods for modular curves, web skripta

Sadržaj kolegija

Osnovni rezultati o eliptički krivuljama Zbrajanje točaka na eliptičkoj krivulji. Mordell-Weilova grupa eliptičke krivulje nad poljem racionalnih brojeva. Eliptičke krivulje nad $\mathbb{C}$. Tor

Sadržaj kolegija

Osnovni rezultati o eliptički krivuljama Zbrajanje točaka na eliptičkoj krivulji. Mordell-Weilova grupa eliptičke krivulje nad poljem racionalnih brojeva. Eliptičke krivulje nad $\mathbb{C}$. Tor

Reprezentacije pridružene eliptičkim krivuljama Općenito o reprezentacijama (konačnih) grupa. Mod ℓ reprezentacije pridružene eliptičkim krivuljama. ℓ-adske reprezentacije. Adeličke reprezentacije.

Sadržaj kolegija

Osnovni rezultati o eliptički krivuljama Zbrajanje točaka na eliptičkoj krivulji. Mordell-Weilova grupa eliptičke krivulje nad poljem racionalnih brojeva. Eliptičke krivulje nad $\mathbb{C}$. Tor

Reprezentacije pridružene eliptičkim krivuljama Općenito o reprezentacijama (konačnih) grupa. Mod ℓ reprezentacije pridružene eliptičkim krivuljama. ℓ-adske reprezentacije. Adeličke reprezentacije.

Modularne krivulje Defincije, rezultati i veze s Galoisovim reprezentacijama.

Sadržaj kolegija

Osnovni rezultati o eliptički krivuljama Zbrajanje točaka na eliptičkoj krivulji. Mordell-Weilova grupa eliptičke krivulje nad poljem racionalnih brojeva. Eliptičke krivulje nad $\mathbb{C}$. Tor

Reprezentacije pridružene eliptičkim krivuljama Općenito o reprezentacijama (konačnih) grupa. Mod ℓ reprezentacije pridružene eliptičkim krivuljama. ℓ-adske reprezentacije. Adeličke reprezentacije.

Modularne krivulje Defincije, rezultati i veze s Galoisovim reprezentacijama.

Moguće slike Galoisovih reprezentacija pridruženih eliptičkim krivuljama Serreov teorem o otvorenoj slici. Poznati rezultati i otvoreni problemi.

Sadržaj kolegija

Osnovni rezultati o eliptički krivuljama Zbrajanje točaka na eliptičkoj krivulji. Mordell-Weilova grupa eliptičke krivulje nad poljem racionalnih brojeva. Eliptičke krivulje nad $\mathbb{C}$. Tor

Reprezentacije pridružene eliptičkim krivuljama Općenito o reprezentacijama (konačnih) grupa. Mod ℓ reprezentacije pridružene eliptičkim krivuljama. ℓ-adske reprezentacije. Adeličke reprezentacije.

Modularne krivulje Defincije, rezultati i veze s Galoisovim reprezentacijama.

Moguće slike Galoisovih reprezentacija pridruženih eliptičkim krivuljama Serreov teorem o otvorenoj slici. Poznati rezultati i otvoreni problemi.

Ostali vezani rezultati Ovisno o tome koliko ćemo imati vremena.

Očekivano predznanje

Uz osnove algebre, očekuje se poznavanje algebarske teorije brojeva: Galoisova teorija, jedinstvrna faktorizacija ideala u prstenima cijelih PAB, cijepanje prostih, ciklotomska polja, itd.

Način polaganja ispita

Zadaće Bit će 5-6 zadaća, otprilike svaka 2 do 3 puta.

Način polaganja ispita

Zadaće Bit će 5-6 zadaća, otprilike svaka 2 do 3 puta.

Seminar: Trebate održati jedan seminar (vjerojatno će pokrivati neki članak o vezanoj tematici).

Definicija

Neka je K polje. Projektivni n-dimenzionalni prostor $\mathbb{P}^n(K)$ nad K je skup svih klasa ekvivalencija točaka u $K^{n+1}\setminus\{(0,\ldots,0)\}$ gdje je ekvialencija dana s

$$(a_0,\ldots,a_n)\sim(\lambda a_0,\ldots,\lambda a_n)$$

za sve $\lambda\in K^*$.

Definicija

Neka je K polje. Projektivni n-dimenzionalni prostor $\mathbb{P}^n(K)$ nad K je skup svih klasa ekvivalencija točaka u $K^{n+1}\setminus\{(0,\ldots,0)\}$ gdje je ekvialencija dana s

$$(a_0,\ldots,a_n)\sim(\lambda a_0,\ldots,\lambda a_n)$$

za sve $\lambda\in K^*$.

Oznaka za klasu od $(a_0,\ldots,a_n)$ je $(a_0:a_1:\ldots:a_n)$.

Primjer

$(1:2)=(2:4)$, $(1:1:0)=(5:5:0)$.

Projektivni pravac i ravnina

Definicija

Prostor $\mathbb{P}^1(K)$ se naziva projektivni pravac, a $\mathbb{P}^2(K)$ se naziva projektivna ravnina nad K.

Projektivni pravac i ravnina

Definicija

Prostor $\mathbb{P}^1(K)$ se naziva projektivni pravac, a $\mathbb{P}^2(K)$ se naziva projektivna ravnina nad K.

Projektivni pravac nad K se sastoji od točaka oblika $(x : 1)$ (koje su u bijekciji s K) i od točke $(1 : 0)$, koja se naziva **točka u beskonačnosti**.

Projektivni pravac i ravnina

Definicija

Prostor $\mathbb{P}^1(K)$ se naziva projektivni pravac, a $\mathbb{P}^2(K)$ se naziva projektivna ravnina nad K.

Projektivni pravac nad K se sastoji od točaka oblika $(x : 1)$ (koje su u bijekciji s K) i od točke $(1 : 0)$, koja se naziva **točka u beskonačnosti**.

Projektivni ravnina nad K se sastoji od točaka oblika $(x : y : 1)$ (koje su u bijekciji s K^2) i od **projektivnog pravca u beskonačnosti**, tj. točaka oblika $(x : y : 0)$.

Projektivne krivulje

Definicija

Projektivna krivulja X *u (projektivnoj) ravnini nad* K *je skup točaka* $X(K)$ *u* $\mathbb{P}^2(K)$ *koji zadovoljavaju jednu* ***homogenu*** *polinomijalnu jednadžbu.*

Projektivne krivulje

Definicija

Projektivna krivulja *X u (projektivnoj) ravnini nad K je skup točaka $X(K)$ u $\mathbb{P}^2(K)$ koji zadovoljavaju jednu* ***homogenu*** *polinomijalnu jednadžbu.*

Definicija

Afina jednadžba od neke projektivne krivulje u ravnini nad K zadane s $f(x, y, z) = 0$ je krivulja u K^2 zadana s $f(x, y, 1) = 0$.

Primjer

$x^2 + y^2 = z^2$ je jednadžba jedne projektivne kružnice, a $y = 3x + 2z$ od jednog projektivnog pravca. Njihove afine jednadžbe su $x^2 + y^2 = 1$ i $y = 3x + 2$.

Točke u beskonačnosti

Točke na projektivnoj krivulji koje su oblika $(x_0 : y_0 : 0)$ se zovu **točke u beskonačnosti**. To su upravo one točke *koje se ne vide* u afinoj jednadžbi.

Točke u beskonačnosti

Točke na projektivnoj krivulji koje su oblika $(x_0 : y_0 : 0)$ se zovu **točke u beskonačnosti**. To su upravo one točke *koje se ne vide* u afinoj jednadžbi.

Primjer

Kružnica $x^2 + y^2 = z^2$ nema točaka u beskonačnosti (nad $\mathbb{Q}$).
Pravac $x = 2y + 3z$ ima točku $(2 : 1 : 0)$.

Definicija eliptičke krivulje

Definicija

Eliptička krivulja nad $\mathbb{K}$ je nesingularna projektivna kubna krivulja nad $\mathbb{K}$ s barem jednom ($\mathbb{K}$-racionalnom) točkom.

Definicija eliptičke krivulje

Definicija

Eliptička krivulja nad $\mathbb{K}$ je nesingularna projektivna kubna krivulja nad $\mathbb{K}$ s barem jednom ($\mathbb{K}$-racionalnom) točkom.

Ona ima afinu jednadžbu oblika

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

gdje su koeficijenti $a, b, c, \ldots, j \in \mathbb{K}$, a nesingularnost znači da je u svakoj točki na krivulji, promatranoj u projektivnoj ravnini $\mathbb{P}^2(\overline{\mathbb{K}})$ nad algebarskim zatvorenjem od $\mathbb{K}$, barem jedna parcijalna derivacija funkcije F različita od 0.

Weierstrassova forma

Svaka takva jednadžba može se biracionalnim transformacijama (racionalnim transformacijama čiji je inverz također racionalna transformacija) svesti na oblik

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

koji nazivamo **Weierstrassova forma**.

Weierstrassova forma

Svaka takva jednadžba može se biracionalnim transformacijama (racionalnim transformacijama čiji je inverz također racionalna transformacija) svesti na oblik

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

koji nazivamo **Weierstrassova forma**.

Definicija

Karakteristika nekog prstena s 1 je najmani $n \in \mathbb{N}$ *takav da je* $n \cdot 1 = 0$, *ako takav postoji, u suprotnom je karakteristika jednaka* 0.

Weierstrassova forma

Svaka takva jednadžba može se biracionalnim transformacijama (racionalnim transformacijama čiji je inverz također racionalna transformacija) svesti na oblik

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

koji nazivamo **Weierstrassova forma**.

Definicija

Karakteristika nekog prstena s 1 je najmani $n \in \mathbb{N}$ takav da je $n \cdot 1 = 0$, ako takav postoji, u suprotnom je karakteristika jednaka 0.

Ako je karakteristika polja $\mathbb{K}$ različita od 2 i 3 (pa smijemo nadopunjavati na potpun kvadrat i potpun kub, dijeleći s 2 i 3 ako je potrebno), onda se ova jednadžba može transformirati u oblik

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

koji nazivamo **kratka Weierstrassova forma**.

Točka u beskonačnosti

Oprez: ovo je samo afina jednadžba!

Točka u beskonačnosti

Oprez: ovo je samo afina jednadžba!

Projektivna jednadžba krivulje je $y^2z = x^3 + axz^2 + bz^3$.

Točka u beskonačnosti

Oprez: ovo je samo afina jednadžba!

Projektivna jednadžba krivulje je $y^2z = x^3 + axz^2 + bz^3$.

Ona ima jednu očitu točku u beskonačnosti $\mathcal{O} = (0 : 1 : 0)$.

Nesingularnost

Uvjet nesingularnosti za našu krivulju

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

je da $f(x) = x^3 + ax + b$ nema višestrukih nultočaka (u algebarskom zatvorenju $\overline{\mathbb{K}}$).

Nesingularnost

Uvjet nesingularnosti za našu krivulju

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

je da $f(x) = x^3 + ax + b$ nema višestrukih nultočaka (u algebarskom zatvorenju $\overline{\mathbb{K}}$).

To je ekvivalentno uvjetu da je *diskriminanta* $D = -4a^3 - 27b^2$ od polinoma $f(x)$ različita od 0.

Skup K-racionalnih točaka

Skup K-racionalnih točaka eliptičkr krivulje nad poljem $\mathbb{K}$ (karakteristike različite od 2 i 3) podrazumijevati skup svih točaka $(x, y) \in \mathbb{K} \times \mathbb{K}$ koji zadovoljavaju jednadžbu

$$E: \quad y^2 = x^3 + ax + b,$$

gdje su $a, b \in \mathbb{K}$ i $4a^3 + 27b^2 \neq 0$, zajedno s točkom u beskonačnosti $\mathcal{O}$.

Skup K-racionalnih točaka

Skup K-racionalnih točaka eliptičkr krivulje nad poljem $\mathbb{K}$ (karakteristike različite od 2 i 3) podrazumijevati skup svih točaka $(x, y) \in \mathbb{K} \times \mathbb{K}$ koji zadovoljavaju jednadžbu

$$E: \quad y^2 = x^3 + ax + b,$$

gdje su $a, b \in \mathbb{K}$ i $4a^3 + 27b^2 \neq 0$, zajedno s točkom u beskonačnosti $\mathcal{O}$.

Taj skup ćemo označavati s $E(\mathbb{K})$.

Grupa točaka

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na njima može, na prirodan način, uvesti operacija uz koju one postaju Abelove grupe.

Grupa točaka

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na njima može, na prirodan način, uvesti operacija uz koju one postaju Abelove grupe.

Da bismo to objasnili, neka je $\mathbb{K} = \mathbb{R}$ polje realnih brojeva.

Grupa točaka

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na njima može, na prirodan način, uvesti operacija uz koju one postaju Abelove grupe.

Da bismo to objasnili, neka je $\mathbb{K} = \mathbb{R}$ polje realnih brojeva.

Definiramo operaciju zbrajanja na $E(\mathbb{R})$.

Grupa točaka

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na njima može, na prirodan način, uvesti operacija uz koju one postaju Abelove grupe.

Da bismo to objasnili, neka je $\mathbb{K} = \mathbb{R}$ polje realnih brojeva.

Definiramo operaciju zbrajanja na $E(\mathbb{R})$.

Definiramo da je $\mathcal{O}$ neutralni element.

Grupa točaka

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na njima može, na prirodan način, uvesti operacija uz koju one postaju Abelove grupe.

Da bismo to objasnili, neka je $\mathbb{K} = \mathbb{R}$ polje realnih brojeva.

Definiramo operaciju zbrajanja na $E(\mathbb{R})$.

Definiramo da je $\mathcal{O}$ neutralni element.

Operacija (zbrajanja) na skupu $E(\mathbb{R})$ se uvodi po pravilu $P + Q + R = \mathcal{O}$ akko su P, Q, R kolinearni.

Grupa točaka

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na njima može, na prirodan način, uvesti operacija uz koju one postaju Abelove grupe.

Da bismo to objasnili, neka je $\mathbb{K} = \mathbb{R}$ polje realnih brojeva.

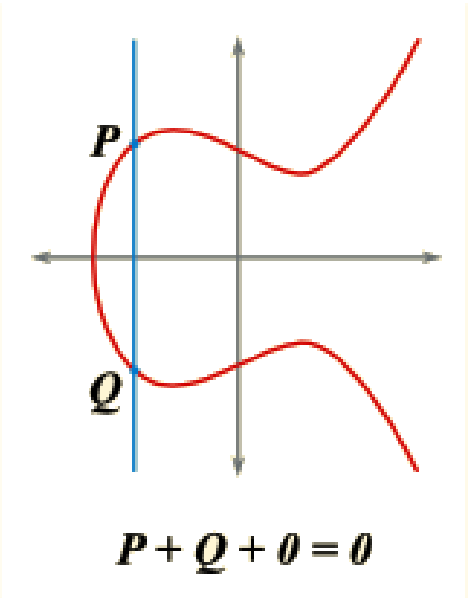
Definiramo operaciju zbrajanja na $E(\mathbb{R})$.

Definiramo da je $\mathcal{O}$ neutralni element.

Operacija (zbrajanja) na skupu $E(\mathbb{R})$ se uvodi po pravilu $P + Q + R = \mathcal{O}$ akko su P, Q, R kolinearni.

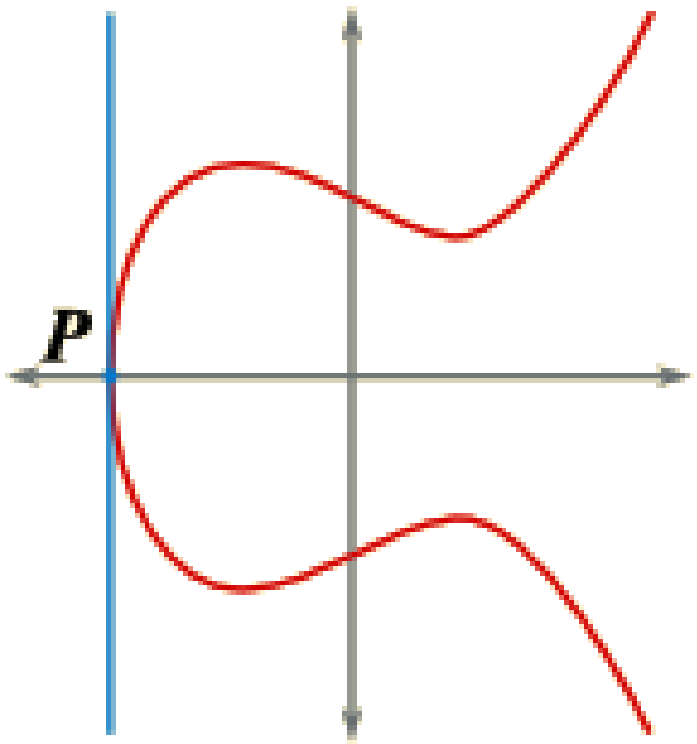
Tako dobivene formule onda mogu poslužiti za definiciju zbrajanja točaka na eliptičkoj krivulji nad proizvoljnim poljem (uz malu modifikaciju ako je karakteristika polja 2 ili 3).

Skicirat ćemo sve što radimo nad $\mathbb{R}$, tj. za $E(\mathbb{R})$, iako sve što radimo vrijedi i nad općenitim poljem k.



Dakle $P + Q + \mathcal{O} = \mathcal{O}$, tj. $P = -Q$.

Ako je $y(P) = 0$, tada će okomiti pravac biti tangenta na E u P ,



pa je $P + P + \mathcal{O} = \mathcal{O}$, tj. $2P = \mathcal{O}$, tj. P će biti točka reda 2 u našoj grupi.

Uzmimo sada da su $P, Q \in E(k)$ dvije točke s različitim x-koordinatama, te neka pravac p kroz njih siječe svaku od točaka s multiplicitetom 1 (dakle nije ni tangenta ni infleksijska točka). Tada po Bezoutovom teoremu slijedi da pravac kroz P i Q, nad $\overline{k}$, siječe E u nekoj trećoj točki $R \in E(\overline{k})$. Međutim $x(R)$ je rješenje sustava jednadžbi

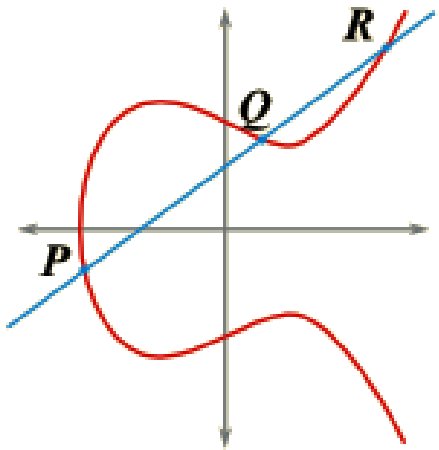
$$y^2 = x^3 + ax + b$$

$$p : y = cx + d,$$

gdje su c i d k-racionalni. Dakle, pošto

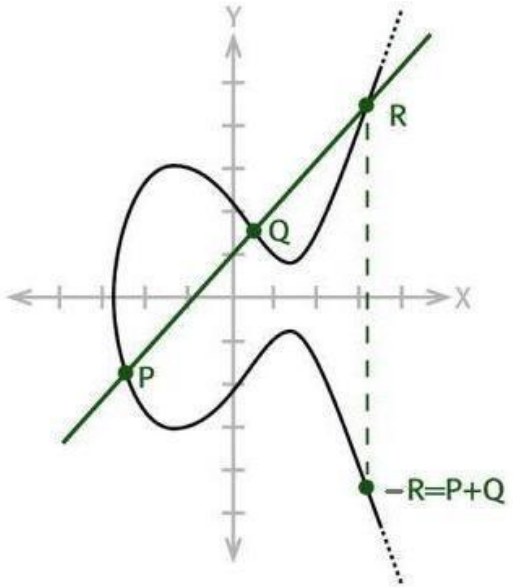
$$(cx + d)^2 = x^3 + ax + b$$

ima 2 rješenja ($x(P)$ i $x(Q)$), tada i treća nultočka mora biti definirana nad k. Također mora biti različita od $x(P)$ i $x(Q)$ pošto smo pretpostavili da se p i E sijeku u točkama multipliciteta 1. Iz jednadžbe za p slijedi da je $y(R)$ također k-racionalan, pa je $R \in E(K)$.

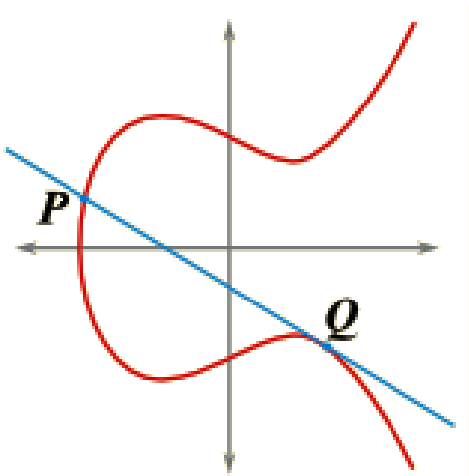


$P+Q+R=0$

Pošto je $P+Q+R=0$ slijedi da je $R=-(P+Q)$ pa je $P+Q$ prema ranije dokazanom točka $-R$, tj. točka koju dobijemo zrcaljenjem s obzirom na x-os. Ovaj postupak nam zapravo daje pravilo zbrajanja točaka: povuci pravac kroz točke krivulje, nađi treću točku na pravcu (koja može biti jedna od već odabranih), te zrcali s obziron na x-os.



Pogledajmo za kraj što dobijemo ako pravac p prolazi kroz različite točke P i Q, te taj pravac siječe neku točku s multiplicitetom 2 (ne može više zbog Bezoutovog teorema).



tj. vrijedi $P + Q = -Q$.
Ako je točka P točka infleksije, tj. tangenta siječe eliptičku krivulju s multiplicitetom 3, tada je $P + P + P = 0$, odnosno P je točka reda 3.

Neka je $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Tada je
1) $-\mathcal{O} = \mathcal{O}$;

Neka je $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Tada je

1) $-\mathcal{O} = \mathcal{O}$;

2) $-P = (x_1, -y_1)$;

Neka je $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Tada je

1) $-\mathcal{O} = \mathcal{O}$;

2) $-P = (x_1, -y_1)$;

3) $\mathcal{O} + P = P$;

Neka je $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Tada je

1) $-\mathcal{O} = \mathcal{O}$;
2) $-P = (x_1, -y_1)$;
3) $\mathcal{O} + P = P$;
4) ako je $Q = -P$, onda je $P + Q = \mathcal{O}$;

Neka je $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Tada je

1) $-\mathcal{O} = \mathcal{O}$;
2) $-P = (x_1, -y_1)$;
3) $\mathcal{O} + P = P$;
4) ako je $Q = -P$, onda je $P + Q = \mathcal{O}$;
5) ako je $Q \neq -P$, onda je $P + Q = (x_3, y_3)$, gdje je

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = -y_1 + \lambda(x_1 - x_3),$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1, \\ \frac{3x_1^2 + a}{2y_1}, & \text{ako je } x_2 = x_1. \end{cases}$$

Broj λ je koeficijent smjera pravca kroz P i Q, odnosno tangente u točki P u slučaju $P = Q$.

Grupa točaka

Pokazuje se da je $(E(\mathbb{K}), +)$ Abelova grupa.

Grupa točaka

Pokazuje se da je $(E(\mathbb{K}), +)$ Abelova grupa.

Sva svojstva Abelove grupe su evidentna, osim asocijativnosti čiji je dokaz nešto kompliciraniji.

Grupa točaka

Pokazuje se da je $(E(\mathbb{K}), +)$ Abelova grupa.

Sva svojstva Abelove grupe su evidentna, osim asocijativnosti čiji je dokaz nešto kompliciraniji.

Za primjene u kriptografiji, najvažniji je slučaj kada je $\mathbb{K}$ konačno polje $\mathbb{F}_q$.

Grupa točaka

Pokazuje se da je $(E(\mathbb{K}), +)$ Abelova grupa.

Sva svojstva Abelove grupe su evidentna, osim asocijativnosti čiji je dokaz nešto kompliciraniji.

Za primjene u kriptografiji, najvažniji je slučaj kada je $\mathbb{K}$ konačno polje $\mathbb{F}_q$.

Posebno su važni slučajevi $q = p$ (prost broj) i $q = 2^k$.

Grupa točaka

Pokazuje se da je $(E(\mathbb{K}), +)$ Abelova grupa.

Sva svojstva Abelove grupe su evidentna, osim asocijativnosti čiji je dokaz nešto kompliciraniji.

Za primjene u kriptografiji, najvažniji je slučaj kada je $\mathbb{K}$ konačno polje $\mathbb{F}_q$.

Posebno su važni slučajevi $q = p$ (prost broj) i $q = 2^k$.

S druge strane, u teoriji brojeva najvažniju ulogu imaju eliptičke krivulje nad poljem racionalnih brojeva $\mathbb{Q}$ i općenitije nad poljima algebarskih brojeva.

Eliptički integrali

Veza između eliptičkih krivulja i elipse dolazi preko problema računanja opsega elipse.

Eliptički integrali

Veza između eliptičkih krivulja i elipse dolazi preko problema računanja opsega elipse.

Neka je elipsa zadana jednadžbom $q^2x^2 + p^2y^2 = p^2q^2$.

Eliptički integrali

Veza između eliptičkih krivulja i elipse dolazi preko problema računanja opsega elipse.

Neka je elipsa zadana jednadžbom $q^2x^2 + p^2y^2 = p^2q^2$.

Tada je njezin opseg jednak vrijednosti integrala

$$4p \int_0^1 \frac{1 - (p^2 - q^2)t^2}{\sqrt{(1 - t^2)(1 - (p^2 - q^2)t^2)}}\, dt.$$

Eliptički integrali

Veza između eliptičkih krivulja i elipse dolazi preko problema računanja opsega elipse.

Neka je elipsa zadana jednadžbom $q^2x^2 + p^2y^2 = p^2q^2$.

Tada je njezin opseg jednak vrijednosti integrala

$$4p \int_0^1 \frac{1 - (p^2 - q^2)t^2}{\sqrt{(1 - t^2)(1 - (p^2 - q^2)t^2)}}\, dt.$$

Pomoću racionalne supstitucije, ovaj se integral može svesti na sličan integral u kojem se pod korijenom nalazi kubna funkcija.

Eliptički integrali

Veza između eliptičkih krivulja i elipse dolazi preko problema računanja opsega elipse.

Neka je elipsa zadana jednadžbom $q^2x^2 + p^2y^2 = p^2q^2$.

Tada je njezin opseg jednak vrijednosti integrala

$$4p \int_0^1 \frac{1 - (p^2 - q^2)t^2}{\sqrt{(1 - t^2)(1 - (p^2 - q^2)t^2)}}\, dt.$$

Pomoću racionalne supstitucije, ovaj se integral može svesti na sličan integral u kojem se pod korijenom nalazi kubna funkcija.

Općenito se integrali u kojima je javljaju drugi korijeni polinoma trećeg ili četvrtog stupnja nazivaju *eliptički integrali*.

Eliptički integrali

Veza između eliptičkih krivulja i elipse dolazi preko problema računanja opsega elipse.

Neka je elipsa zadana jednadžbom $q^2x^2 + p^2y^2 = p^2q^2$.

Tada je njezin opseg jednak vrijednosti integrala

$$4p \int_0^1 \frac{1 - (p^2 - q^2)t^2}{\sqrt{(1 - t^2)(1 - (p^2 - q^2)t^2)}}\, dt.$$

Pomoću racionalne supstitucije, ovaj se integral može svesti na sličan integral u kojem se pod korijenom nalazi kubna funkcija.

Općenito se integrali u kojima je javljaju drugi korijeni polinoma trećeg ili četvrtog stupnja nazivaju *eliptički integrali*.

Oni se ne mogu izraziti pomoću elementarnih funkcija.

Eliptički integrali

Međutim, moguće ih je izraziti pomoću *Weierstrassove* $\wp$*-funkcije*.

Međutim, moguće ih je izraziti pomoću *Weierstrassove $\wp$-funkcije*.

Ova funkcija zadovoljava diferencijalnu jednadžbu oblika

$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

Međutim, moguće ih je izraziti pomoću *Weierstrassove $\wp$-funkcije*.

Ova funkcija zadovoljava diferencijalnu jednadžbu oblika

$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

Ovdje je njena uloga analogna ulozi funkcije sinus (ili kosinus) u računanju integrala kod kojih se ispod korijena javljaju kvadratne funkcije.

Eliptički integrali

Međutim, moguće ih je izraziti pomoću *Weierstrassove $\wp$-funkcije*.

Ova funkcija zadovoljava diferencijalnu jednadžbu oblika

$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

Ovdje je njena uloga analogna ulozi funkcije sinus (ili kosinus) u računanju integrala kod kojih se ispod korijena javljaju kvadratne funkcije.

Naime, funkcija $y = \sin x$ zadovoljava diferencijalnu jednadžbu $y^2 + (y')^2 = 1$.

Eliptički integrali

Međutim, moguće ih je izraziti pomoću *Weierstrassove $\wp$-funkcije*.

Ova funkcija zadovoljava diferencijalnu jednadžbu oblika

$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

Ovdje je njena uloga analogna ulozi funkcije sinus (ili kosinus) u računanju integrala kod kojih se ispod korijena javljaju kvadratne funkcije.

Naime, funkcija $y = \sin x$ zadovoljava diferencijalnu jednadžbu $y^2 + (y')^2 = 1$.

Slično kao što jediničnu kružnicu možemo parametrizirati pomoću $(\cos t, \sin t)$, tako se kompleksne točke na eliptičkoj krivulji $y^2 = x^3 + ax + b$ mogu parametrizirati pomoću $(\wp(t), \frac{1}{2}\wp'(t))$.

Međutim, moguće ih je izraziti pomoću *Weierstrassove $\wp$-funkcije*.

Ova funkcija zadovoljava diferencijalnu jednadžbu oblika

$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

Ovdje je njena uloga analogna ulozi funkcije sinus (ili kosinus) u računanju integrala kod kojih se ispod korijena javljaju kvadratne funkcije.

Naime, funkcija $y = \sin x$ zadovoljava diferencijalnu jednadžbu $y^2 + (y')^2 = 1$.

Slično kao što jediničnu kružnicu možemo parametrizirati pomoću $(\cos t, \sin t)$, tako se kompleksne točke na eliptičkoj krivulji $y^2 = x^3 + ax + b$ mogu parametrizirati pomoću $(\wp(t), \frac{1}{2}\wp'(t))$.

Štoviše, pokazuje se da ako je $P = (\wp(t), \frac{1}{2}\wp'(t))$ i $Q = (\wp(u), \frac{1}{2}\wp'(u))$, onda je $P + Q = (\wp(t+u), \frac{1}{2}\wp'(t+u))$.

Dakle, zbrajanje točaka na $E(\mathbb{C})$ odgovara zbrajanju kompleksnih brojeva.

Dakle, zbrajanje točaka na $E(\mathbb{C})$ odgovara zbrajanju kompleksnih brojeva.

Poznavanje te činjenice daje elegantni dokaz asocijativnosti zbrajanja točaka na eliptičkoj krivulji.

Eliptičke krivulje nad $\mathbb{C}$

Što je eliptička krivulja nad $\mathbb{C}$?

Eliptičke krivulje nad $\mathbb{C}$

Što je eliptička krivulja nad $\mathbb{C}$?

Za odgovor nam može pomoći funkcija $\wp$.

Eliptičke krivulje nad $\mathbb{C}$

Što je eliptička krivulja nad $\mathbb{C}$?

Za odgovor nam može pomoći funkcija $\wp$.

Jedno od njzienih svojstava je da je dvostruko periodična, tj. postoje kompleksni brojevi ω_1 i ω_2 (takvi da $\omega_1/\omega_2 \notin \mathbb{R}$) sa svojstvom $\wp(z + m\omega_1 + n\omega_2) = \wp(z)$ za sve cijele brojeve m, n.

Eliptičke krivulje nad $\mathbb{C}$

Što je eliptička krivulja nad $\mathbb{C}$?

Za odgovor nam može pomoći funkcija $\wp$.

Jedno od njzienih svojstava je da je dvostruko periodična, tj. postoje kompleksni brojevi ω_1 i ω_2 (takvi da $\omega_1/\omega_2 \notin \mathbb{R}$) sa svojstvom $\wp(z + m\omega_1 + n\omega_2) = \wp(z)$ za sve cijele brojeve m, n.

Označimo s L "rešetku" svih točaka oblika $m\omega_1 + n\omega_2$, $m, n \in \mathbb{Z}$.

Eliptičke krivulje nad $\mathbb{C}$

Što je eliptička krivulja nad $\mathbb{C}$?

Za odgovor nam može pomoći funkcija $\wp$.

Jedno od njzienih svojstava je da je dvostruko periodična, tj. postoje kompleksni brojevi ω_1 i ω_2 (takvi da $\omega_1/\omega_2 \notin \mathbb{R}$) sa svojstvom $\wp(z + m\omega_1 + n\omega_2) = \wp(z)$ za sve cijele brojeve m, n.

Označimo s L "rešetku" svih točaka oblika $m\omega_1 + n\omega_2$, $m, n \in \mathbb{Z}$.

Funkcija $\wp$ je analitička u svim točkama kompleksne ravnine, osim u točkama iz rešetke L u kojima ima pol drugog reda (tj. $\wp$ je meromorfna funkcija).

Eliptičke krivulje nad $\mathbb{C}$

Što je eliptička krivulja nad $\mathbb{C}$?

Za odgovor nam može pomoći funkcija $\wp$.

Jedno od njzienih svojstava je da je dvostruko periodična, tj. postoje kompleksni brojevi ω_1 i ω_2 (takvi da $\omega_1/\omega_2 \notin \mathbb{R}$) sa svojstvom $\wp(z + m\omega_1 + n\omega_2) = \wp(z)$ za sve cijele brojeve m, n.

Označimo s L "rešetku" svih točaka oblika $m\omega_1 + n\omega_2$, $m, n \in \mathbb{Z}$.

Funkcija $\wp$ je analitička u svim točkama kompleksne ravnine, osim u točkama iz rešetke L u kojima ima pol drugog reda (tj. $\wp$ je meromorfna funkcija).

Naime, vrijedi da je

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in L,\, w \neq 0} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Eliptičke krivulje nad $\mathbb{C}$

Što je eliptička krivulja nad $\mathbb{C}$?

Za odgovor nam može pomoći funkcija $\wp$.

Jedno od njzienih svojstava je da je dvostruko periodična, tj. postoje kompleksni brojevi ω_1 i ω_2 (takvi da $\omega_1/\omega_2 \notin \mathbb{R}$) sa svojstvom $\wp(z + m\omega_1 + n\omega_2) = \wp(z)$ za sve cijele brojeve m, n.

Označimo s L "rešetku" svih točaka oblika $m\omega_1 + n\omega_2$, $m, n \in \mathbb{Z}$.

Funkcija $\wp$ je analitička u svim točkama kompleksne ravnine, osim u točkama iz rešetke L u kojima ima pol drugog reda (tj. $\wp$ je meromorfna funkcija).

Naime, vrijedi da je

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in L,\, w \neq 0} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Općenito se meromorfne, dvostruko periodične funkcije nazivaju *eliptičke funkcije*.

Eliptičke krivulje nad $\mathbb{C}$

Parametrizacija točaka na eliptičkoj krivulji pomoću funkcije $\wp$ predstavlja zapravo izomorfizam grupa $E(\mathbb{C})$ i $\mathbb{C}/L$.

Eliptičke krivulje nad $\mathbb{C}$

Parametrizacija točaka na eliptičkoj krivulji pomoću funkcije $\wp$ predstavlja zapravo izomorfizam grupa $E(\mathbb{C})$ i $\mathbb{C}/L$.

Funkcija $\wp$ je u potpunosti određena svojim vrijednostima u "fundamentalnom paralelogramu" koji se sastoji od svih kompleksnih brojeva oblika $\alpha\omega_1 + \beta\omega_2$, $0 \leq \alpha, \beta < 1$.

Eliptičke krivulje nad $\mathbb{C}$

Parametrizacija točaka na eliptičkoj krivulji pomoću funkcije $\wp$ predstavlja zapravo izomorfizam grupa $E(\mathbb{C})$ i $\mathbb{C}/L$.

Funkcija $\wp$ je u potpunosti određena svojim vrijednostima u "fundamentalnom paralelogramu" koji se sastoji od svih kompleksnih brojeva oblika $\alpha\omega_1 + \beta\omega_2$, $0 \leq \alpha, \beta < 1$.

Dvostruka peridoičnost of $\wp$ nam može pomoći da eliptičku krivulju nad $\mathbb{C}$ vizualiziramo kao torus.

Genus

Torus možemo zamisliti i kao sferu s “rupom”.

Genus

Torus možemo zamisliti i kao sferu s “rupom”.

Pokazuje se da se svaka algebarska krivulja može prikazati u trodimenzionalnom prostoru kao sfera s konačno mnogo rupa.

Genus

Torus možemo zamisliti i kao sferu s "rupom".

Pokazuje se da se svaka algebarska krivulja može prikazati u trodimenzionalnom prostoru kao sfera s konačno mnogo rupa.

Taj broj rupa se naziva *genus* ili *rod* krivulje.

Genus

Torus možemo zamisliti i kao sferu s "rupom".

Pokazuje se da se svaka algebarska krivulja može prikazati u trodimenzionalnom prostoru kao sfera s konačno mnogo rupa.

Taj broj rupa se naziva *genus* ili *rod* krivulje.

Alternativna (šira) definicija eliptičke krivulje nad K je da je to glatka algebarska krivulja genusa jednakog 1 s zadanom K-racionalnom točkom.

Genus

Torus možemo zamisliti i kao sferu s "rupom".

Pokazuje se da se svaka algebarska krivulja može prikazati u trodimenzionalnom prostoru kao sfera s konačno mnogo rupa.

Taj broj rupa se naziva *genus* ili *rod* krivulje.

Alternativna (šira) definicija eliptičke krivulje nad K je da je to glatka algebarska krivulja genusa jednakog 1 s zadanom K-racionalnom točkom.

Ova definicija uključuje ne samo nesingularne kubne krivulje, već i sve one krivulje koje su im biracionalnog ekvivalentne.

Definicija

Biracionalne transformacija krivulje C_1 u C_2 je prelikavanje

$$(x, y) \mapsto (f(x, y), g(x, y)),$$

gdje su f i g racionalne funkcije, te je inverz, koji je definiran u svim osim konačno mnogo točaka, također racionlna funckija.

Biracionalne transformacije čuvaju genus krivulje, ali ne čuvaju njezin stupanj.
Ako krivulja ima stupanj n, onda je njezin genus $\leq (n-1)(n-2)/2$, s time da ako je krivulja nesingularna, onda joj je genus upravo jednak $(n-1)(n-2)/2$.

Biracionalne transformacije čuvaju genus krivulje, ali ne čuvaju njezin stupanj.
Ako krivulja ima stupanj n, onda je njezin genus $\leq (n-1)(n-2)/2$, s time da ako je krivulja nesingularna, onda joj je genus upravo jednak $(n-1)(n-2)/2$.

Poznato je da tzv. hipereliptičke krivulje čija je jednadžba $y^2 = f(x)$, gdje je $f(x)$ polinom stupnja $n \geq 3$ bez višestrukih korijena, imaju genus $\lfloor (n-1)/2 \rfloor$.

Biracionalne transformacije čuvaju genus krivulje, ali ne čuvaju njezin stupanj.
Ako krivulja ima stupanj n, onda je njezin genus $\leq (n-1)(n-2)/2$, s time da ako je krivulja nesingularna, onda joj je genus upravo jednak $(n-1)(n-2)/2$.

Poznato je da tzv. hipereliptičke krivulje čija je jednadžba $y^2 = f(x)$, gdje je $f(x)$ polinom stupnja $n \geq 3$ bez višestrukih korijena, imaju genus $\lfloor (n-1)/2 \rfloor$.

To posebno znači da, pored slučaja kada je $n = 3$, i u slučaju kad je $n = 4$ (i krivulja ima barem jednu racionalnu točku) također imamo eliptičku krivulju.

Primjer

Neka je C krivulja zadana jednadžbom

$$y^2 = x^4 + 3x^2 + 2x.$$

Primjer

Neka je C krivulja zadana jednadžbom

$$y^2 = x^4 + 3x^2 + 2x.$$

Ona ima očitu racionalnu točku $(0, 0)$.

Primjer

Neka je C krivulja zadana jednadžbom

$$y^2 = x^4 + 3x^2 + 2x.$$

Ona ima očitu racionalnu točku $(0, 0)$.

Supstitucijama $x = \frac{2}{v}$, $y = \frac{2t}{v^2}$ dobivamo

$$\frac{4t^2}{v^4} = \frac{2^4}{v^4} + 3\frac{2^2}{v^2} + 2\frac{2}{v},$$

tj. krivulju $t^2 = v^3 + 3v^2 + 4$, te konačno supstitucijom $v + 1 = s$ dobivamo eliptičku krivulju E u kratkoj Weiestrassovoj formi

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

Primjer

Neka je C krivulja zadana jednadžbom

$$y^2 = x^4 + 3x^2 + 2x.$$

Ona ima očitu racionalnu točku $(0, 0)$.

Supstitucijama $x = \frac{2}{v}$, $y = \frac{2t}{v^2}$ dobivamo

$$\frac{4t^2}{v^4} = \frac{2^4}{v^4} + 3\frac{2^2}{v^2} + 2\frac{2}{v},$$

tj. krivulju $t^2 = v^3 + 3v^2 + 4$, te konačno supstitucijom $v + 1 = s$ dobivamo eliptičku krivulju E u kratkoj Weiestrassovoj formi

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

Dakle, transformacija koja prevodi C u E je $x = \frac{2}{s-1}$, $y = \frac{2t}{(s-1)^2}$.

Inverzna transformacija je $s = \frac{x+2}{x}$, $t = \frac{2y}{x^2}$. Stoga je ovo biracionalna transformacija.

Genus

Genus krivulje igra važnu ulogu kod klasifikacije diofantskih jednadžbi. Naime, o njemu ovisi broj cjelobrojnih, odnosno racionalnih rješenja jednadžbe, te struktura skupa tih rješenja.

Genus

Genus krivulje igra važnu ulogu kod klasifikacije diofantskih jednadžbi. Naime, o njemu ovisi broj cjelobrojnih, odnosno racionalnih rješenja jednadžbe, te struktura skupa tih rješenja.

Krivulje genusa 0 su upravo one koje posjeduju parametrizaciju pomoću racionalnih funkcija.

Genus

Genus krivulje igra važnu ulogu kod klasifikacije diofantskih jednadžbi. Naime, o njemu ovisi broj cjelobrojnih, odnosno racionalnih rješenja jednadžbe, te struktura skupa tih rješenja.

Krivulje genusa 0 su upravo one koje posjeduju parametrizaciju pomoću racionalnih funkcija.

Svaka krivulja drugog stupnja (konika) ima genus 0. Npr. krivulja $x^2 + y^2 = 1$ ima racionalnu parametrizaciju

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

Genus

Genus krivulje igra važnu ulogu kod klasifikacije diofantskih jednadžbi. Naime, o njemu ovisi broj cjelobrojnih, odnosno racionalnih rješenja jednadžbe, te struktura skupa tih rješenja.

Krivulje genusa 0 su upravo one koje posjeduju parametrizaciju pomoću racionalnih funkcija.

Svaka krivulja drugog stupnja (konika) ima genus 0. Npr. krivulja $x^2 + y^2 = 1$ ima racionalnu parametrizaciju

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

Kubne singularne krivulje također imaju genus 0. Npr. krivulja $y^2 = x^3$ ima singularnu točku $(0,0)$ (šiljak - *cusp*).

Genus

Genus krivulje igra važnu ulogu kod klasifikacije diofantskih jednadžbi. Naime, o njemu ovisi broj cjelobrojnih, odnosno racionalnih rješenja jednadžbe, te struktura skupa tih rješenja.

Krivulje genusa 0 su upravo one koje posjeduju parametrizaciju pomoću racionalnih funkcija.

Svaka krivulja drugog stupnja (konika) ima genus 0. Npr. krivulja $x^2 + y^2 = 1$ ima racionalnu parametrizaciju

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

Kubne singularne krivulje također imaju genus 0. Npr. krivulja $y^2 = x^3$ ima singularnu točku $(0,0)$ (šiljak - *cusp*).

Stoga ova kubna krivulja nije eliptička. Njezina racionalna parametrizacija je $x = t^2$, $y = t^3$.

Još jedna parametrizacija

Kao drugi primjer navedimo krivulju $y^2 = x^3 + 2x^2$. Ona također ima singularnu točku $(0, 0)$ (čvor - *node*) i ima racionalnu parametrizaciju $x = t^2 - 2$, $y = t^3 - 2t$.

Očito je da ove dvije kubne krivulje imaju beskonačno mnogo cjelobrojnih točaka.

Očito je da ove dvije kubne krivulje imaju beskonačno mnogo cjelobrojnih točaka.

Pellova jednadžba $x^2 - dy^2 = 1$ (d prirodan broj koji nije potpun kvadrat) je primjer krivulje drugog stupnja koja ima beskonačno mnogo cjelobrojnih točaka.

Očito je da ove dvije kubne krivulje imaju beskonačno mnogo cjelobrojnih točaka.

Pellova jednadžba $x^2 - dy^2 = 1$ (d prirodan broj koji nije potpun kvadrat) je primjer krivulje drugog stupnja koja ima beskonačno mnogo cjelobrojnih točaka.

Krivulja genusa 1 može imati samo konačno mnogo cjelobrojnih točaka (Siegelov teorem).

Očito je da ove dvije kubne krivulje imaju beskonačno mnogo cjelobrojnih točaka.

Pellova jednadžba $x^2 - dy^2 = 1$ (d prirodan broj koji nije potpun kvadrat) je primjer krivulje drugog stupnja koja ima beskonačno mnogo cjelobrojnih točaka.

Krivulja genusa 1 može imati samo konačno mnogo cjelobrojnih točaka (Siegelov teorem).

Racionalnih točaka može biti beskonačno mnogo, ali su "konačno generirane" (sve se mogu dobiti iz konačno točaka primjenom grupovne operacije na eliptičkoj krivulji).

Očito je da ove dvije kubne krivulje imaju beskonačno mnogo cjelobrojnih točaka.

Pellova jednadžba $x^2 - dy^2 = 1$ (d prirodan broj koji nije potpun kvadrat) je primjer krivulje drugog stupnja koja ima beskonačno mnogo cjelobrojnih točaka.

Krivulja genusa 1 može imati samo konačno mnogo cjelobrojnih točaka (Siegelov teorem).

Racionalnih točaka može biti beskonačno mnogo, ali su "konačno generirane" (sve se mogu dobiti iz konačno točaka primjenom grupovne operacije na eliptičkoj krivulji).

Theorem (Mordell-Weil)

Neka je K polje algebarskih brojeva. Tada je $E(K)$ konačno generirana Abelova grupa.

Očito je da ove dvije kubne krivulje imaju beskonačno mnogo cjelobrojnih točaka.

Pellova jednadžba $x^2 - dy^2 = 1$ (d prirodan broj koji nije potpun kvadrat) je primjer krivulje drugog stupnja koja ima beskonačno mnogo cjelobrojnih točaka.

Krivulja genusa 1 može imati samo konačno mnogo cjelobrojnih točaka (Siegelov teorem).

Racionalnih točaka može biti beskonačno mnogo, ali su "konačno generirane" (sve se mogu dobiti iz konačno točaka primjenom grupovne operacije na eliptičkoj krivulji).

Theorem (Mordell-Weil)

Neka je K polje algebarskih brojeva. Tada je $E(K)$ konačno generirana Abelova grupa.

Krivulja genusa većeg od 1 može imati samo konačno mnogo racionalnih točaka. Ova tvrdnja je poznata Mordellova slutnja koju je 1983. godine dokazao Faltings.

Neka je

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

eliptička krivulja u kratkoj Weierstrtassovoj formi. Tada je **diskriminata eliptičke krivulje**

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

Neka je

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

eliptička krivulja u kratkoj Weierstrtassovoj formi. Tada je **diskriminata eliptičke krivulje**

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

Napomena: za polinom $f(x) := a_n \prod_i^n (x - \alpha_i)$, **diskriminata** polinoma je $\Delta(f) = a_n^{2n-2} \prod_{i<j}^n (\alpha_i - \alpha_j)^2$.

Neka je

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

eliptička krivulja u kratkoj Weierstrtassovoj formi. Tada je **diskriminata eliptičke krivulje**

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

Napomena: za polinom $f(x) := a_n \prod_i^n (x - \alpha_i)$, **diskriminata** polinoma je $\Delta(f) = a_n^{2n-2} \prod_{i<j}^n (\alpha_i - \alpha_j)^2$.

Lako se vidi da za kubni polinom vrijedi $f(u) = 0$ i $\Delta(f) = 0 \iff$ f ima (barem) dvostruku nultočku u u.

Neka je

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

eliptička krivulja u kratkoj Weierstrtassovoj formi. Tada je **diskriminata eliptičke krivulje**

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

Napomena: za polinom $f(x) := a_n \prod_i^n (x - \alpha_i)$, **diskriminata** polinoma je $\Delta(f) = a_n^{2n-2} \prod_{i<j}^n (\alpha_i - \alpha_j)^2$.

Lako se vidi da za kubni polinom vrijedi $f(u) = 0$ i $\Delta(f) = 0 \iff$ f ima (barem) dvostruku nultočku u u.

Primjetimo da je $\Delta(E) = 16\times$ diskriminanta od $x^3 + ax + b$, te tvrdimo da je $\Delta \neq 0$ ekvivalentno tome da je E nesingularna.

Neka je

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

eliptička krivulja u kratkoj Weierstrtassovoj formi. Tada je **diskriminata eliptičke krivulje**

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

Napomena: za polinom $f(x) := a_n \prod_i^n (x - \alpha_i)$, **diskriminata** polinoma je $\Delta(f) = a_n^{2n-2} \prod_{i<j}^n (\alpha_i - \alpha_j)^2$.

Lako se vidi da za kubni polinom vrijedi $f(u) = 0$ i $\Delta(f) = 0 \iff$ f ima (barem) dvostruku nultočku u u.

Primjetimo da je $\Delta(E) = 16\times$ diskriminanta od $x^3 + ax + b$, te tvrdimo da je $\Delta \neq 0$ ekvivalentno tome da je E nesingularna.

Da bi to dokazali prvo primjetimo da ako zapišemo E u projektivnim kordinatama kao $y^2z = x^3 + axz^2 + bz^3$, te $F = y^2z - x^3 - axz^2 - bz^3$ tada lako vidimo da u $O = (0 : 1 : 0)$ vrijedi $\frac{dF}{dz}(P) = 1$, dakle krivulja je nesingularna u O.

Neka je

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

eliptička krivulja u kratkoj Weierstrtassovoj formi. Tada je **diskriminata eliptičke krivulje**

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

Napomena: za polinom $f(x) := a_n \prod_i^n (x - \alpha_i)$, **diskriminata** polinoma je $\Delta(f) = a_n^{2n-2} \prod_{i<j}^n (\alpha_i - \alpha_j)^2$.

Lako se vidi da za kubni polinom vrijedi $f(u) = 0$ i $\Delta(f) = 0 \iff$ f ima (barem) dvostruku nultočku u u.

Primjetimo da je $\Delta(E) = 16\times$ diskriminanta od $x^3 + ax + b$, te tvrdimo da je $\Delta \neq 0$ ekvivalentno tome da je E nesingularna.

Da bi to dokazali prvo primjetimo da ako zapišemo E u projektivnim kordinatama kao $y^2z = x^3 + axz^2 + bz^3$, te $F = y^2z - x^3 - axz^2 - bz^3$ tada lako vidimo da u $O = (0 : 1 : 0)$ vrijedi $\frac{dF}{dz}(P) = 1$, dakle krivulja je nesingularna u O.

Dakle od sada nadalje možemo uzeti $z = 1$.

Općenito se diskriminanta polinoma f stupnja n s vodećim koeficijentom a_n i korijenima $x_1, \ldots, x_n$ (iz $\overline{\mathbb{K}}$) definira kao

$$\Delta(f) = a_n^{2n-2} \prod_{i<j}^{n} (x_i - x_j)^2$$

Općenito se diskriminanta polinoma f stupnja n s vodećim koeficijentom a_n i korijenima $x_1, \ldots, x_n$ (iz $\overline{\mathbb{K}}$) definira kao

$$\Delta(f) = a_n^{2n-2} \prod_{i<j}^{n} (x_i - x_j)^2$$

i jednaka je 0 ako i samo ako f ima višestrukih korijena.

Općenito se diskriminanta polinoma f stupnja n s vodećim koeficijentom a_n i korijenima $x_1, \ldots, x_n$ (iz $\overline{\mathbb{K}}$) definira kao

$$\Delta(f) = a_n^{2n-2} \prod_{i<j} (x_i - x_j)^2$$

i jednaka je 0 ako i samo ako f ima višestrukih korijena.

Ako je eliptička krivulja dana jednadžbom $y^2 = x^3 + ax + b$, onda je $\Delta(E) = -16(4a^3 + 27b^2)$.

Općenito se diskriminanta polinoma f stupnja n s vodećim koeficijentom a_n i korijenima $x_1, \ldots, x_n$ (iz $\overline{\mathbb{K}}$) definira kao

$$\Delta(f) = a_n^{2n-2} \prod_{i<j} (x_i - x_j)^2$$

i jednaka je 0 ako i samo ako f ima višestrukih korijena.

Ako je eliptička krivulja dana jednadžbom $y^2 = x^3 + ax + b$, onda je $\Delta(E) = -16(4a^3 + 27b^2)$.

Za krivulje definirane nad $\mathbb{R}$, predznak diskriminante nam govori koliko komponenti ima graf krivulje: ako je $\Delta < 0$, onda imamo jednu komponentu, a ako je $\Delta > 0$, onda imamo dvije komponente.

j-invarijanta i izomorfizmi

Ako je eliptička krivulja dana jednadžbom $E : y^2 = x^3 + ax + b$, onda je j-invarijanta $j(E)$ od E

$$j(E) := 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

j-invarijanta i izomorfizmi

Ako je eliptička krivulja dana jednadžbom $E : y^2 = x^3 + ax + b$, onda je j-invarijanta $j(E)$ od E

$$j(E) := 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Naziv j-invarijanta dolazi od toga što izomorfne krivulje imaju iste j-invarijante.

j-invarijanta i izomorfizmi

Ako je eliptička krivulja dana jednadžbom $E : y^2 = x^3 + ax + b$, onda je j-invarijanta $j(E)$ od E

$$j(E) := 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Naziv j-invarijanta dolazi od toga što izomorfne krivulje imaju iste j-invarijante.

U slučaju kratkih Weierstrassovih formi jedine dopustive supstitucije u izomorfizmu eliptičkih krivulja između E i $E' : (y')^2 = (x')^3 + a'x' + b'$ su

$$x = u^2 x', \quad y = u^3 y', \quad u \in \mathbb{Q}^*.$$

j-invarijanta i izomorfizmi

Ako je eliptička krivulja dana jednadžbom $E : y^2 = x^3 + ax + b$, onda je j-invarijanta $j(E)$ od E

$$j(E) := 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Naziv j-invarijanta dolazi od toga što izomorfne krivulje imaju iste j-invarijante.

U slučaju kratkih Weierstrassovih formi jedine dopustive supstitucije u izomorfizmu eliptičkih krivulja između E i $E' : (y')^2 = (x')^3 + a'x' + b'$ su

$$x = u^2 x', \quad y = u^3 y', \quad u \in \mathbb{Q}^*.$$

Vrijedi i svojevrstan obrat ovog svojstva j-invarijanti. Naime, dvije eliptičke krivulje su izomorfne nad algebarskim proširenjem $\overline{\mathbb{Q}}$ ako i samo ako imaju istu j-invarijantu.

j-invarijanta i izomorfizmi

Ako promatramo krivulje nad algebarski zatvorenim poljem, onda nam j-invarijanta govori jesu li krivulje izomorfne.

j-invarijanta i izomorfizmi

Ako promatramo krivulje nad algebarski zatvorenim poljem, onda nam j-invarijanta govori jesu li krivulje izomorfne.

No, ako polje nije algebarski zatvoreno, primjerice ako promatramo krivulje nad $\mathbb{Q}$, onda dvije krivulje mogu imati jednake j-invarijante, ali da se ne mogu transformirati jedna u drugu pomoću racionalnih funkcija s koeficijentima iz $\mathbb{Q}$.

j-invarijanta i izomorfizmi

Ako promatramo krivulje nad algebarski zatvorenim poljem, onda nam j-invarijanta govori jesu li krivulje izomorfne.

No, ako polje nije algebarski zatvoreno, primjerice ako promatramo krivulje nad $\mathbb{Q}$, onda dvije krivulje mogu imati jednake j-invarijante, ali da se ne mogu transformirati jedna u drugu pomoću racionalnih funkcija s koeficijentima iz $\mathbb{Q}$.

Na primjer, krivulje $y^2 = x^3 - 4x$ i $y^2 = x^3 - 25x$ obje imaju $j = 1728$. Prva od njih ima konačno mnogo racionalnih točaka, dok ih druga ima beskonačno mnogo (točka $(-4, 6)$ je beskonačnog reda).

j-invarijanta i izomorfizmi

Ako promatramo krivulje nad algebarski zatvorenim poljem, onda nam j-invarijanta govori jesu li krivulje izomorfne.

No, ako polje nije algebarski zatvoreno, primjerice ako promatramo krivulje nad $\mathbb{Q}$, onda dvije krivulje mogu imati jednake j-invarijante, ali da se ne mogu transformirati jedna u drugu pomoću racionalnih funkcija s koeficijentima iz $\mathbb{Q}$.

Na primjer, krivulje $y^2 = x^3 - 4x$ i $y^2 = x^3 - 25x$ obje imaju $j = 1728$. Prva od njih ima konačno mnogo racionalnih točaka, dok ih druga ima beskonačno mnogo (točka $(-4, 6)$ je beskonačnog reda).

Dakle, ove krivulje nisu izomorfne nad $\mathbb{Q}$, ali jesu nad $\mathbb{Q}(\sqrt{10})$ (supstitucije su $(x, y) \mapsto (u^2x, u^3y)$, $u = \frac{\sqrt{10}}{2}$).

j-invarijanta

Neka je $E : y^2 = x^3 + ax + b, \quad E' : y^2 = x^3 + a'x + b'$. Tada $E \simeq E'$ izomorfni akko postoji $u \in k^*$ takav da $a' = u^4 a,\ b' = u^6 b$.

j-invarijanta

Neka je $E : y^2 = x^3 + ax + b, \quad E' : y^2 = x^3 + a'x + b'$. Tada $E \simeq E'$ izomorfni akko postoji $u \in k^*$ takav da $a' = u^4 a,\ b' = u^6 b$.

Propozicija

Neka je k polje karakteristike $\neq 2, 3$.

1. *Eliptičke krivulje E i E' su izomorfne nad $\overline{k}$ ako i samo ako je $j(E) = j(E')$.*
2. *Za svaki $j \in k$, postoji eliptička krivulja E/k takva da je $j(E) = j$.*

j-invarijanta

Neka je $E : y^2 = x^3 + ax + b, \quad E' : y^2 = x^3 + a'x + b'$. Tada $E \simeq E'$ izomorfni akko postoji $u \in k^*$ takav da $a' = u^4 a,\ b' = u^6 b$.

Propozicija

Neka je k polje karakteristike $\neq 2, 3$.

1. *Eliptičke krivulje E i E' su izomorfne nad $\overline{k}$ ako i samo ako je $j(E) = j(E')$.*
2. *Za svaki $j \in k$, postoji eliptička krivulja E/k takva da je $j(E) = j$.*

Korolar

Postoji bijekcija između $\{$eliptičke krivulje $/k$ do na $\overline{k}$-izomorfizam$\}$ i k.

Reduckija modulo p eliptičke krivulje

"Redukcija modulo p" (homomorfizam $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$) je jedan od osnovnih alata u teoriji brojeva.

Reduckija modulo p eliptičke krivulje

"Redukcija modulo p" (homomorfizam $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$) je jedan od osnovnih alata u teoriji brojeva.

Prednosti projektivnog prostora je da se cijeli prostor $\mathbb{P}^n(\mathbb{Q})$ može reducirati u $\mathbb{P}^n(\mathbb{F}_p)$.

Reduckija modulo p eliptičke krivulje

"Redukcija modulo p" (homomorfizam $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$) je jedan od osnovnih alata u teoriji brojeva.

Prednosti projektivnog prostora je da se cijeli prostor $\mathbb{P}^n(\mathbb{Q})$ može reducirati u $\mathbb{P}^n(\mathbb{F}_p)$.

Ideja - eliptičke krivulje reduciramo mod p tako da reduciramo mod p njezine koeficijente.

Reduckija modulo p eliptičke krivulje

"Redukcija modulo p" (homomorfizam $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$) je jedan od osnovnih alata u teoriji brojeva.

Prednosti projektivnog prostora je da se cijeli prostor $\mathbb{P}^n(\mathbb{Q})$ može reducirati u $\mathbb{P}^n(\mathbb{F}_p)$.

Ideja - eliptičke krivulje reduciramo mod p tako da reduciramo mod p njezine koeficijente.

Neka je E definirana nad $\mathbb{Q}$. Da bi reducirali eliptičke krivulje modulo p, treba dovesti eliptičku krivulju u pogodan oblik za to.

Reduckija modulo p eliptičke krivulje

"Redukcija modulo p" (homomorfizam $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$) je jedan od osnovnih alata u teoriji brojeva.

Prednosti projektivnog prostora je da se cijeli prostor $\mathbb{P}^n(\mathbb{Q})$ može reducirati u $\mathbb{P}^n(\mathbb{F}_p)$.

Ideja - eliptičke krivulje reduciramo mod p tako da reduciramo mod p njezine koeficijente.

Neka je E definirana nad $\mathbb{Q}$. Da bi reducirali eliptičke krivulje modulo p, treba dovesti eliptičku krivulju u pogodan oblik za to.

Prvo primjetimo da je svaka eliptička krivulja nad $\mathbb{Q}$ izomorfna nekoj eliptičkoj krivulji nad $\mathbb{Q}$ oblika

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}.$$

Reduckija modulo p eliptičke krivulje

"Redukcija modulo p" (homomorfizam $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$) je jedan od osnovnih alata u teoriji brojeva.

Prednosti projektivnog prostora je da se cijeli prostor $\mathbb{P}^n(\mathbb{Q})$ može reducirati u $\mathbb{P}^n(\mathbb{F}_p)$.

Ideja - eliptičke krivulje reduciramo mod p tako da reduciramo mod p njezine koeficijente.

Neka je E definirana nad $\mathbb{Q}$. Da bi reducirali eliptičke krivulje modulo p, treba dovesti eliptičku krivulju u pogodan oblik za to.

Prvo primjetimo da je svaka eliptička krivulja nad $\mathbb{Q}$ izomorfna nekoj eliptičkoj krivulji nad $\mathbb{Q}$ oblika

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}.$$

To se lako vidi jer ako krenemo od $Y^2 = X^3 + a'X + b'$, tada možemo uzeti da je u najmanji zajednički više kratnik od nazivnika od a' i b', te uz $a = u^4 a'$, $b = u^6 b'$ imamo da je naša početna jednadžba izomorfna nekoj sa cjelobrojnim koeficijentima.

Međutim, postoji puno izomorfnih eliptičkih krivulja s cjelobrojnim koeficijentima, te njihove redukcije nisu nikako iste.

Međutim, postoji puno izomorfnih eliptičkih krivulja s cjelobrojnim koeficijentima, te njihove redukcije nisu nikako iste. Npr.

$$E_1 : y^2 = x^3 + x + 1, \quad \text{i}$$

$$E_2 : y^2 = x^2 + 81x + 729$$

su izomorfne nad $\mathbb{Q}$, međutim njihove redukcije mod 3 su

$$\overline{E}_1 : y^2 = x^3 + x + 1$$

$$\overline{E}_2 : y^2 = x^3,$$

gdje prva jednadžba opisuje eliptičku krivulju, a druga ne (singularna je).

Međutim, postoji puno izomorfnih eliptičkih krivulja s cjelobrojnim koeficijentima, te njihove redukcije nisu nikako iste. Npr.

$$E_1 : y^2 = x^3 + x + 1, \quad \text{i}$$

$$E_2 : y^2 = x^2 + 81x + 729$$

su izomorfne nad $\mathbb{Q}$, međutim njihove redukcije mod 3 su

$$\overline{E}_1 : y^2 = x^3 + x + 1$$

$$\overline{E}_2 : y^2 = x^3,$$

gdje prva jednadžba opisuje eliptičku krivulju, a druga ne (singularna je). Primjetimo

$$\Delta(E_1) = 2^4 \cdot 31, \quad \Delta(E_2) = 2^4 \cdot 3^{12} \cdot 31.$$

Dakle, $\Delta(E_1) \equiv 1 \pmod 3$, a $\Delta(E_2) \equiv 0 \pmod 3$, pa $\overline{E}_2$ nije eliptička krivulja nad $\mathbb{F}_3$.

Međutim, postoji puno izomorfnih eliptičkih krivulja s cjelobrojnim koeficijentima, te njihove redukcije nisu nikako iste. Npr.

$$E_1 : y^2 = x^3 + x + 1, \quad \text{i}$$

$$E_2 : y^2 = x^2 + 81x + 729$$

su izomorfne nad $\mathbb{Q}$, međutim njihove redukcije mod 3 su

$$\overline{E}_1 : y^2 = x^3 + x + 1$$

$$\overline{E}_2 : y^2 = x^3,$$

gdje prva jednadžba opisuje eliptičku krivulju, a druga ne (singularna je). Primjetimo

$$\Delta(E_1) = 2^4 \cdot 31, \quad \Delta(E_2) = 2^4 \cdot 3^{12} \cdot 31.$$

Dakle, $\Delta(E_1) \equiv 1 \pmod 3$, a $\Delta(E_2) \equiv 0 \pmod 3$, pa $\overline{E}_2$ nije eliptička krivulja nad $\mathbb{F}_3$.
Dakle, da bi smisleno reducirali eliptičku krivulju, treba izabrati *minimalni* model u klasi izomorfizma eliptičke krivulje nad $\mathbb{Q}$.

Dakle, da bi smisleno reducirali eliptičku krivulju, treba izabrati *minimalni* model u klasi izomorfizma eliptičke krivulje nad $\mathbb{Q}$.

Dakle, da bi smisleno reducirali eliptičku krivulju, treba izabrati *minimalni* model u klasi izomorfizma eliptičke krivulje nad $\mathbb{Q}$.

Definicija

Kažemo da je model od $E/\mathbb{Q}$

$$E : y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_4x + a_6,$$

***minimalan**, ako su* $a_i \in \mathbb{Z}$ *i ako je* $|\Delta(E)|$ *minimalan u klasi izomorfizma od* E.

Dakle, da bi smisleno reducirali eliptičku krivulju, treba izabrati *minimalni* model u klasi izomorfizma eliptičke krivulje nad $\mathbb{Q}$.

Definicija

Kažemo da je model od $E/\mathbb{Q}$

$$E : y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_4x + a_6,$$

***minimalan**, ako su* $a_i \in \mathbb{Z}$ *i ako je* $|\Delta(E)|$ *minimalan u klasi izomorfizma od* E.

Definicija

Neka je $n \in \mathbb{Z}$, *te zapišimo* $n = p^k \cdot m$, *gdje* $(p, m) = 1$, $k \geq 0$. *Tada je* p-***adska valuacija*** *od* n, $\nu_p(n) = k$. *Tj.* p-*adska valuacija od* n *je najveća potencija od* p *koja dijeli* n.

Propozicija

Neka je

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

Ako je $0 \leq \nu_p(\Delta(E)) < 12$, *za sve proste brojeve* p, *tada je* E *minimalan model.*

Propozicija

Neka je

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

Ako je $0 \leq \nu_p(\Delta(E)) < 12$, *za sve proste brojeve* p, *tada je* E *minimalan model.*

Za sve $p \geq 5$, vrijedi i obrat, tj. ako je E minimalni model od E tada je $\nu_p(\Delta(E)) < 12$.

Do kraja predavanja pretpostavljamo da je $E/\mathbb{Q}$ zadana u minimalnom modelu.

Do kraja predavanja pretpostavljamo da je $E/\mathbb{Q}$ zadana u minimalnom modelu.

Definicija

Neka je $E/\mathbb{Q}$ zadana sa (minimalnim modelom)

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

Tada, definiramo $\overline{E}/\mathbb{F}_p$ kao

$$\overline{E} : y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6,$$

gdje su $\overline{a}_i$ slike od a_i od homomorfizma $\mathbb{Z} \to \mathbb{F}_p$ redukcija mod p.

Do kraja predavanja pretpostavljamo da je $E/\mathbb{Q}$ zadana u minimalnom modelu.

Definicija

Neka je $E/\mathbb{Q}$ zadana sa (minimalnim modelom)

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

Tada, definiramo $\overline{E}/\mathbb{F}_p$ kao

$$\overline{E} : y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6,$$

gdje su $\overline{a}_i$ slike od a_i od homomorfizma $\mathbb{Z} \to \mathbb{F}_p$ redukcija mod p.

Primjetimo da je $\overline{E}$ eliptička krivulja $\iff \Delta(\overline{E}) \neq 0$ (u $\mathbb{F}_p$) $\iff p \nmid \Delta(E)$.

Dobra redukcija

Definicija

Ako $p \nmid \Delta(E)$, tj. da je redukcija mod p od E eliptička krivulja, tada kažemo da E ima ***dobru redukciju u*** *p. Ako E nema dobru redukciju u p, tada ima* ***lošu redukciju*** *u p.*

Loša redukcija

Ima više vrsta loše redukcije.

Definicija

Neka je eliptička krivulja zadana modelom $E : y^2 = f(x)$, *gdje je* f *polinom stupnja 3, te neka je* $\overline{E} : y^2 = \overline{f}(x)$, *gdje je* $\overline{f} \in \mathbb{F}_p[x]$ *polinom* f *modulo* p *(sve koeficijente reduciramo modulo* p*).*

Loša redukcija

Ima više vrsta loše redukcije.

Definicija

Neka je eliptička krivulja zadana modelom $E : y^2 = f(x)$, *gdje je* f *polinom stupnja 3, te neka je* $\overline{E} : y^2 = \overline{f}(x)$, *gdje je* $\overline{f} \in \mathbb{F}_p[x]$ *polinom* f *modulo* p *(sve koeficijente reduciramo modulo* p*).*

Tada E *ima lošu redukciju ako i samo ako* $\overline{f}$ *ima višestruki korijen.*

Loša redukcija

Ima više vrsta loše redukcije.

Definicija

Neka je eliptička krivulja zadana modelom $E : y^2 = f(x)$, gdje je f polinom stupnja 3, te neka je $\overline{E} : y^2 = \overline{f}(x)$, gdje je $\overline{f} \in \mathbb{F}_p[x]$ polinom f modulo p (sve koeficijente reduciramo modulo p).

Tada E ima lošu redukciju ako i samo ako $\overline{f}$ ima višestruki korijen.

Ako $\overline{f}$ ima dvostruki korijen, tada E ima ***multiplikativnu redukciju*** *u p. Dakle $\overline{E}$ ima model $y^2 = x^2(x + a)$. Ako je a kvadratni ostatak modulo p, tad kažemo da E ima* ***podijeljenu multiplikativnu redukciju****, a inače kažemo da ima* ***nepodijeljenu multiplikativnu redukciju****.*
Ako $\overline{f}$ ima trostruki korijen, tada kažemo da E ima ***aditivnu redukciju*** *modulo p.*

Pošto diskriminanta minimalnog modela ima samo konačno mnogo prostih faktora, slijedi da svaka eliptička krivulja ima lošu redukciju u samo konačno mnogo p-ova.

Pošto diskriminanta minimalnog modela ima samo konačno mnogo prostih faktora, slijedi da svaka eliptička krivulja ima lošu redukciju u samo konačno mnogo p-ova.

Primjer

Neka je $E : y^2 = x^3 - x^2 - 86x + 240$. Vrijedi $\Delta(E) = -2^6 3^4 5^2 13^2$, dakle E ima lošu redukciju u $2, 3, 5, 13$.

Pošto diskriminanta minimalnog modela ima samo konačno mnogo prostih faktora, slijedi da svaka eliptička krivulja ima lošu redukciju u samo konačno mnogo p-ova.

Primjer

Neka je $E : y^2 = x^3 - x^2 - 86x + 240$. Vrijedi $\Delta(E) = -2^6 3^4 5^2 13^2$, dakle E ima lošu redukciju u $2, 3, 5, 13$.

Redukcija mod 3 je

$$y^2 = x^3 - x^2 + x = x(x+1)^2.$$

Promjenom varijabli $x \to x - 1$ dobivamo

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

te pošto 2 nije kvadratni ostatak modulo 3, E ima nepodijeljenu multiplikativnu redukciju mod 3.

Propozicija

Neka je E eliptička krivulja s dobrom redukcijom u p. Tada je redukcija mod p,

$$E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$$

$$P = (x : y : z) \in \mathbb{P}^2(\mathbb{Z}) \to (\overline{x} : \overline{y} : \overline{z}) \in \mathbb{P}^2(\mathbb{F}_p)$$

homomorfizam grupa.

U prethodnoj propoziciji uzimamo točku $P = (x : y : z)$ takvu da su $x, y, z \in \mathbb{Z}$, da je barem jedan $\neq 0$, te da nisu svi djeljivi s p.

U prethodnoj propoziciji uzimamo točku $P = (x : y : z)$ takvu da su $x, y, z \in \mathbb{Z}$, da je barem jedan $\neq 0$, te da nisu svi djeljivi s p.

Zbog jednostavnosti ćemo za grupu točaka redukciju mod p neke $E/\mathbb{Q}$ pisati $E(\mathbb{F}_p)$ umjesto $\overline{E}(\mathbb{F}_p)$.

U prethodnoj propoziciji uzimamo točku $P = (x : y : z)$ takvu da su $x, y, z \in \mathbb{Z}$, da je barem jedan $\neq 0$, te da nisu svi djeljivi s p.

Zbog jednostavnosti ćemo za grupu točaka redukciju mod p neke $E/\mathbb{Q}$ pisati $E(\mathbb{F}_p)$ umjesto $\overline{E}(\mathbb{F}_p)$.

Primjetimo da redukcija modulo p preslikava $\mathcal{O} \in E(\mathbb{Q})$ u $\mathcal{O} \in E(\mathbb{F}_p)$.

U prethodnoj propoziciji uzimamo točku $P = (x : y : z)$ takvu da su $x, y, z \in \mathbb{Z}$, da je barem jedan $\neq 0$, te da nisu svi djeljivi s p.

Zbog jednostavnosti ćemo za grupu točaka redukciju mod p neke $E/\mathbb{Q}$ pisati $E(\mathbb{F}_p)$ umjesto $\overline{E}(\mathbb{F}_p)$.

Primjetimo da redukcija modulo p preslikava $\mathcal{O} \in E(\mathbb{Q})$ u $\mathcal{O} \in E(\mathbb{F}_p)$.

Grupovni zakon nad $\mathbb{F}_p$ je potpuno jednak kao nad $\mathbb{Q}$ - koristimo iste formule, samo sve reduciramo mod p. Pošto nad $\mathbb{F}_2$ i $\mathbb{F}_3$ nekad treba koristiti dugu Weierstrassovu formu, grupovni zakon ima drukčije jednadžbe.

Konduktor

Za krivulju definiranu nad $\mathbb{Q}$ se definira veličina povezana s diskriminantom koja se naziva *konduktor*:

$$N = \prod_p p^{f_p}.$$

Ako je $p \neq 2, 3$, onda se f_p može lako odrediti iz minimalnog Weierstrassovog modela za E:

- $f_p = 0$ ako $p \nmid \Delta$;
- $f_p = 1$ ako $p | \Delta$ i $p \nmid c_4$;
- $f_p \geq 2$ ako $p | \Delta$ i $p | c_4$; ako je $p \neq 2, 3$, onda je $f_p = 2$.