Galoisove reprezentacije pridružene eliptičkim krivuljama

Filip Najman

2. predavanje

10.11.2020.

Definicija

Neka je R integralna domena. Tada je $\mathrm{Frac}(R) = \{\frac{a}{b}, a, b \in R, b \neq 0\}/\sim$, *gdje je* $\sim$ *standardna relacija ekvivalencije,* ***polje razlomaka*** *od R.*

Definicija

Neka je R integralna domena. Tada je $\mathrm{Frac}(R) = \{\frac{a}{b}, a, b \in R, b \neq 0\}/\sim$, *gdje je* $\sim$ *standardna relacija ekvivalencije,* ***polje razlomaka*** *od R.*

Primjer

$\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, $\mathrm{Frac}(k[x]) = k(x)$.

Definicija

Afin prostor $\mathbb{A}^n/k$ *je mnogostrukost zadana praznim skupom jednadžbi, tj. svaka točka iz* k^n *se nalazi na* $\mathbb{A}^n$.

Definicija

Afin prostor $\mathbb{A}^n/k$ *je mnogostrukost zadana praznim skupom jednadžbi, tj. svaka točka iz* k^n *se nalazi na* $\mathbb{A}^n$*.*

Dakle $\mathbb{A}^n(k) = k^n$ kao skupovi.

Definicija

Afin prostor $\mathbb{A}^n/k$ *je mnogostrukost zadana praznim skupom jednadžbi, tj. svaka točka iz* k^n *se nalazi na* $\mathbb{A}^n$.

Dakle $\mathbb{A}^n(k) = k^n$ kao skupovi.

Definicija

Racionalna funkcija *na* $\mathbb{A}^n(k)$ *je* $f \in k(x_1, \ldots, x_n) =: k(\mathbb{A}^n)$.

Definicija

Afin prostor $\mathbb{A}^n/k$ *je mnogostrukost zadana praznim skupom jednadžbi, tj. svaka točka iz* k^n *se nalazi na* $\mathbb{A}^n$.

Dakle $\mathbb{A}^n(k) = k^n$ kao skupovi.

Definicija

Racionalna funkcija *na* $\mathbb{A}^n(k)$ *je* $f \in k(x_1, \ldots, x_n) =: k(\mathbb{A}^n)$.

Mi ćemo promatrati samo slučaj $n = 2$.

Definicija

Afin prostor $\mathbb{A}^n/k$ *je mnogostrukost zadana praznim skupom jednadžbi, tj. svaka točka iz* k^n *se nalazi na* $\mathbb{A}^n$.

Dakle $\mathbb{A}^n(k) = k^n$ kao skupovi.

Definicija

Racionalna funkcija *na* $\mathbb{A}^n(k)$ *je* $f \in k(x_1, \ldots, x_n) =: k(\mathbb{A}^n)$.

Mi ćemo promatrati samo slučaj $n = 2$.

Definicija

Neka je C/k *afina krivulja, te* $f = \frac{g}{h} \in k(\mathbb{A}^2)$, *gdje je* $h \neq 0$ *na* $C(k)$. *Restrikcija od* f *na* C

$$f : C - \{\text{konačan skup gdje je } h = 0\} \to \overline{k}$$

je ***racionalna funkcija na*** C. *Skup svih racionalnih funkcija na* C *čini polje, koje označavamo s* $k(C)$.

Činjenica

Neka je C_f afina krivulja definirana s $f \in k[x, y]$. Tada je

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x, y]}{(f)}\right).$$

Činjenica

Neka je C_f afina krivulja definirana s $f \in k[x,y]$. Tada je

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(f)}\right).$$

Primjer

Neka je $D : y = 0$ u afinoj ravnini.

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(y)}\right) \simeq \mathrm{Frac}(k[x]) = k(x).$$

Činjenica

Neka je C_f afina krivulja definirana s $f \in k[x,y]$. Tada je

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(f)}\right).$$

Primjer

Neka je $D : y = 0$ u afinoj ravnini.

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(y)}\right) \simeq \mathrm{Frac}(k[x]) = k(x).$$

Primjer

Neka je $C : y^2 = x^3 + 1$ u afinoj ravnini. Tada je

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(y^2 - x^3 - 1)}\right) \simeq k(x, \sqrt{x^3+1}).$$

Definicija

Neka su $X \subseteq \mathbb{A}^m$ *i* $Y \subseteq \mathbb{A}^n$ *afine mnogostrukosti definirane nad* k. *Morfizam* $f : X \to Y$ *je preslikavanje* $f(P) := (f_1(P), \ldots, f_n(P))$ *definirano s* $f_1, \ldots, f_n \in \overline{k}[X]$ *takvo da je* $f(P) \in Y$ *za svaki* $P \in X$.

Definicija

Neka su $X \subseteq \mathbb{A}^m$ i $Y \subseteq \mathbb{A}^n$ afine mnogostrukosti definirane nad k. Morfizam $f : X \to Y$ je preslikavanje $f(P) := (f_1(P), \ldots, f_n(P))$ definirano s $f_1, \ldots, f_n \in \overline{k}[X]$ takvo da je $f(P) \in Y$ za svaki $P \in X$.

Definition

Dvije mnogostrukosti X i Y su *izomorfne* ako postoji morfizam $f : X \to Y$ i $g : Y \to X$ takve da su $f \circ g$ i $g \circ f$ identiteta na X i Y. U tom slučaju kažemo da su f i g izomorfizmi.

Pretpostavimo u ovom predavanju da je $\operatorname{char} k \neq 2, 3$.

Definicija

Izogenija *između dvije eliptičke krivulje je morfizam* $\phi : E \to E'$ *s konačnom jezgrom koji preslikava* $\mathcal{O} \in E$ *u* $\mathcal{O}' \in E'$.

Pretpostavimo u ovom predavanju da je $\operatorname{char} k \neq 2, 3$.

Definicija

Izogenija *između dvije eliptičke krivulje je morfizam* $\phi : E \to E'$ *s konačnom jezgrom koji preslikava* $\mathcal{O} \in E$ *u* $\mathcal{O}' \in E'$.

Činjenica

Svaka izogenija je homomorfizam grupa.

Pretpostavimo u ovom predavanju da je $\operatorname{char} k \neq 2, 3$.

Definicija

Izogenija *između dvije eliptičke krivulje je morfizam $\phi : E \to E'$ s konačnom jezgrom koji preslikava $\mathcal{O} \in E$ u $\mathcal{O}' \in E'$.*

Činjenica

Svaka izogenija je homomorfizam grupa.

$[0] : E \to E$ je nul-izogenija. Definiraimo $\operatorname{st}[0] = 0$, tako da bi vrijedilo

$$\operatorname{st} \phi \circ \psi = \operatorname{st} \phi \operatorname{st} \cdot \psi$$

za sve izogenije $\phi : E \to E'$, $\psi : E' \to E$.

Primjer

Neka je $E : y^2 = x^3 + ax + b$. *Promotrimo množenje s* 2 *na* E, $[2] : E \to E$,

$$[2] : (x, y) \to \left(\frac{x^4 - 2ax^2 + a^2 - 8b}{4(x^3 + ax + b)}, \dots \right).$$

Preslikavanje [2] *je definirano racionalnim funkcijama, te je* $[2]\mathcal{O} = \mathcal{O}$, *tako da je* [2] *izogenija.*

Primjer

Neka je $E : y^2 = x^3 + ax + b$. *Promotrimo množenje s* 2 *na* E, $[2] : E \to E$,

$$[2] : (x, y) \to \left(\frac{x^4 - 2ax^2 + a^2 - 8b}{4(x^3 + ax + b)}, \dots \right).$$

Preslikavanje [2] *je definirano racionalnim funkcijama, te je* $[2]\mathcal{O} = \mathcal{O}$, *tako da je* [2] *izogenija.*

Primjer

Množenje s m *na eliptičkoj krivulji* $[m]$ *je za svaki* $m \geq 1$ *izogenija.*

Primjer

Neka je $E : y^2 = x^3 + ax + b$. *Promotrimo množenje s* 2 *na* E, $[2] : E \to E$,

$$[2] : (x, y) \to \left(\frac{x^4 - 2ax^2 + a^2 - 8b}{4(x^3 + ax + b)}, \dots \right).$$

Preslikavanje [2] *je definirano racionalnim funkcijama, te je* $[2]\mathcal{O} = \mathcal{O}$, *tako da je* [2] *izogenija.*

Primjer

Množenje s m *na eliptičkoj krivulji* $[m]$ *je za svaki* $m \geq 1$ *izogenija.*

Neka su E_1 i E_2 eliptičke krivulje. Tada je

$$\mathrm{Hom}(E_1, E_2) = \{\textit{izogenije} : E_1 \to E_2\}$$

grupa uz operaciju zbrajanja.

Nadalje, $\operatorname{End} E = \operatorname{Hom}(E, E)$ je prsten s jedinicom (s operacijama zbrajanja i kompozicije) koji sadrži $\mathbb{Z}$, pošto je množenje s m izogenija za svaki $m \in \mathbb{Z}$.

Nadalje, $\operatorname{End} E = \operatorname{Hom}(E, E)$ je prsten s jedinicom (s operacijama zbrajanja i kompozicije) koji sadrži $\mathbb{Z}$, pošto je množenje s m izogenija za svaki $m \in \mathbb{Z}$.
Zapravo, za eliptičke krivulje definirane nad poljima algebarskih brojeva, skoro uvijek će vrijediti $\operatorname{End} E = \mathbb{Z}$.

Nadalje, $\operatorname{End} E = \operatorname{Hom}(E, E)$ je prsten s jedinicom (s operacijama zbrajanja i kompozicije) koji sadrži $\mathbb{Z}$, pošto je množenje s m izogenija za svaki $m \in \mathbb{Z}$.
Zapravo, za eliptičke krivulje definirane nad poljima algebarskih brojeva, skoro uvijek će vrijediti $\operatorname{End} E = \mathbb{Z}$.

Napomena

Ako u subskriptu imamo polje, npr. $\operatorname{End}_k(E)$ *ili* $\operatorname{Hom}_k(E_1, E_2)$, *tada to označava skup morfizama tog tipa nad* k. *Ako ne piše ništa u subskriptu, onda se uvijek misli na preslikavanja definirana nad* $\overline{k}$.

Nadalje, $\operatorname{End} E = \operatorname{Hom}(E, E)$ je prsten s jedinicom (s operacijama zbrajanja i kompozicije) koji sadrži $\mathbb{Z}$, pošto je množenje s m izogenija za svaki $m \in \mathbb{Z}$.
Zapravo, za eliptičke krivulje definirane nad poljima algebarskih brojeva, skoro uvijek će vrijediti $\operatorname{End} E = \mathbb{Z}$.

Napomena

Ako u subskriptu imamo polje, npr. $\operatorname{End}_k(E)$ *ili* $\operatorname{Hom}_k(E_1, E_2)$, *tada to označava skup morfizama tog tipa nad* k. *Ako ne piše ništa u subskriptu, onda se uvijek misli na preslikavanja definirana nad* $\overline{k}$.

Primjer

Neka je $E : y^2 = x^3 - x$, *te* $[i] \in \operatorname{End} E$, $[i] : (x, y) = (-x, iy)$. *Primjetimo* $[i]([i][-1]) = [1]$, *te je* $[i]$ *automorfizam. Slijedi* $\operatorname{End} E \supset \mathbb{Z}[i]$. *Međutim,* $\operatorname{End}_{\mathbb{Q}} E = \mathbb{Z}$.

Neka su C i D glatke projektivne krivulje. Sjetimo se da je stupanj nekog nekonstantnog racionalnog preslikavanja krivulja $\phi : C \to D$ jednak maksimalnom broju točaka $\in C$ u praslici od $\phi(P)$ za neki $P \in D$. Ako je preslikavanje stupnja n, tada će $|\phi^{-1}(P)| = n$ za sve osim konačno mnogo P-ova. Ako je $|\phi^{-1}(P)| < n$ tada je ϕ **razgranato** u P, ako je $|\phi^{-1}(P)| = n$ onda je **nerazgranato** u P.

Neka su C i D glatke projektivne krivulje. Sjetimo se da je stupanj nekog nekonstantnog racionalnog preslikavanja krivulja $\phi : C \to D$ jednak maksimalnom broju točaka $\in C$ u praslici od $\phi(P)$ za neki $P \in D$. Ako je preslikavanje stupnja n, tada će $|\phi^{-1}(P)| = n$ za sve osim konačno mnogo P-ova. Ako je $|\phi^{-1}(P)| < n$ tada je ϕ **razgranato** u P, ako je $|\phi^{-1}(P)| = n$ onda je **nerazgranato** u P. Ako je $\phi : E_1 \to E_2$ ne-nul izogenija, tada je $\operatorname{Ker}\phi = \phi^{-1}(\mathcal{O})$ konačna podgrupa (od $E(\overline{k})$).

Neka su C i D glatke projektivne krivulje. Sjetimo se da je stupanj nekog nekonstantnog racionalnog preslikavanja krivulja $\phi : C \to D$ jednak maksimalnom broju točaka $\in C$ u praslici od $\phi(P)$ za neki $P \in D$. Ako je preslikavanje stupnja n, tada će $|\phi^{-1}(P)| = n$ za sve osim konačno mnogo P-ova. Ako je $|\phi^{-1}(P)| < n$ tada je ϕ **razgranato** u P, ako je $|\phi^{-1}(P)| = n$ onda je **nerazgranato** u P. Ako je $\phi : E_1 \to E_2$ ne-nul izogenija, tada je $\operatorname{Ker}\phi = \phi^{-1}(\mathcal{O})$ konačna podgrupa (od $E(\overline{k})$).

Primjer

Neka je $E : y^2 = (x - a_1)(x - a_2)(x - a_3), a_i \in \mathbb{Q}$, $T_i = (a_i, 0)$. *Tada je*

$$\operatorname{Ker}[2] = \{\mathcal{O}, T_1, T_2, T_3\} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Neka je E eliptička krivulja, $\mathcal{O} \neq P \in E$. Definiramo

$$\tau_P : E \to E,$$

$$\tau_P(Q) = P + Q$$

tj. τ_p je translacija s P. Preslikavanje τ_p je morfizam (ali nije homomorfizam grupa).

Teorem

Neka su E_1, E_2 eliptičke krivulje nad poljem algebarskih brojeva k, te $\phi : E_1 \to E_2$ izogenija stupnja $n \neq 0$.

1. *ϕ je nerazgranato preslikavanje, tj. $|\phi^{-1}(P)| = n$ za svaki $P \in D$.*
2. *Ako je $\psi : E_1 \to E_3$ izogenija i $\operatorname{Ker}\psi \supset \operatorname{Ker}\phi$, tada postoji jedinstvena izogenija $\chi : E_2 \to E_3$ takva da je $\psi = \chi \circ \phi$.*

Teorem

Neka su E_1, E_2 eliptičke krivulje nad poljem algebarskih brojeva k, te $\phi : E_1 \to E_2$ izogenija stupnja $n \neq 0$.

1. *ϕ je nerazgranato preslikavanje, tj. $|\phi^{-1}(P)| = n$ za svaki $P \in D$.*
2. *Ako je $\psi : E_1 \to E_3$ izogenija i $\operatorname{Ker}\psi \supset \operatorname{Ker}\phi$, tada postoji jedinstvena izogenija $\chi : E_2 \to E_3$ takva da je $\psi = \chi \circ \phi$.*

Činjenica

Ako je Φ konačna podgrupa od $E(\overline{k})$, tada postoji jedinstvena eliptička krivulja E' i izogenija

$$\phi : E \to E'$$

takva da je $\ker\phi = \Phi$.

Propozicija

Grupa automorfizama eliptičke krivulje (nad $\overline{k}$)
$\mathrm{Aut}\, E = \{$ *izomorfizmi* $: E \to E$ *definirani nad* $\overline{k}\}$ *je je*

$$\mathbb{Z}/2\mathbb{Z} \text{ za } y^2 = x^3 + ax + b, a, b \neq 0$$

$$\mathbb{Z}/4\mathbb{Z} \text{ za } y^2 = x^3 + ax,$$

$$\mathbb{Z}/6\mathbb{Z} \text{ za } y^2 = x^3 + b.$$

Propozicija

Grupa automorfizama eliptičke krivulje (nad $\overline{k}$)
$\operatorname{Aut} E = \{$ *izomorfizmi* $: E \to E$ *definirani nad* $\overline{k}\}$ *je je*

$$\mathbb{Z}/2\mathbb{Z} \text{ za } y^2 = x^3 + ax + b, a, b \neq 0$$

$$\mathbb{Z}/4\mathbb{Z} \text{ za } y^2 = x^3 + ax,$$

$$\mathbb{Z}/6\mathbb{Z} \text{ za } y^2 = x^3 + b.$$

Dokaz.

$\operatorname{Aut} E = \{u \in \overline{k}^* : u^4 a = a,\ u^6 b = b\}$, pa slijedi da je

$$\operatorname{Aut} E = \langle -1 \rangle, \text{ ako } a, b \neq 0,$$

$$\operatorname{Aut} E = \langle i \rangle, \text{ ako } b = 0,$$

$$\operatorname{Aut} E = \langle \zeta_6 \rangle, \text{ ako } a = 0,$$

gdje je ζ_6 primitivni šesti korijen iz jedinice (npr. $\frac{1-\sqrt{-3}}{2}$). □

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 $f_p = 2$.