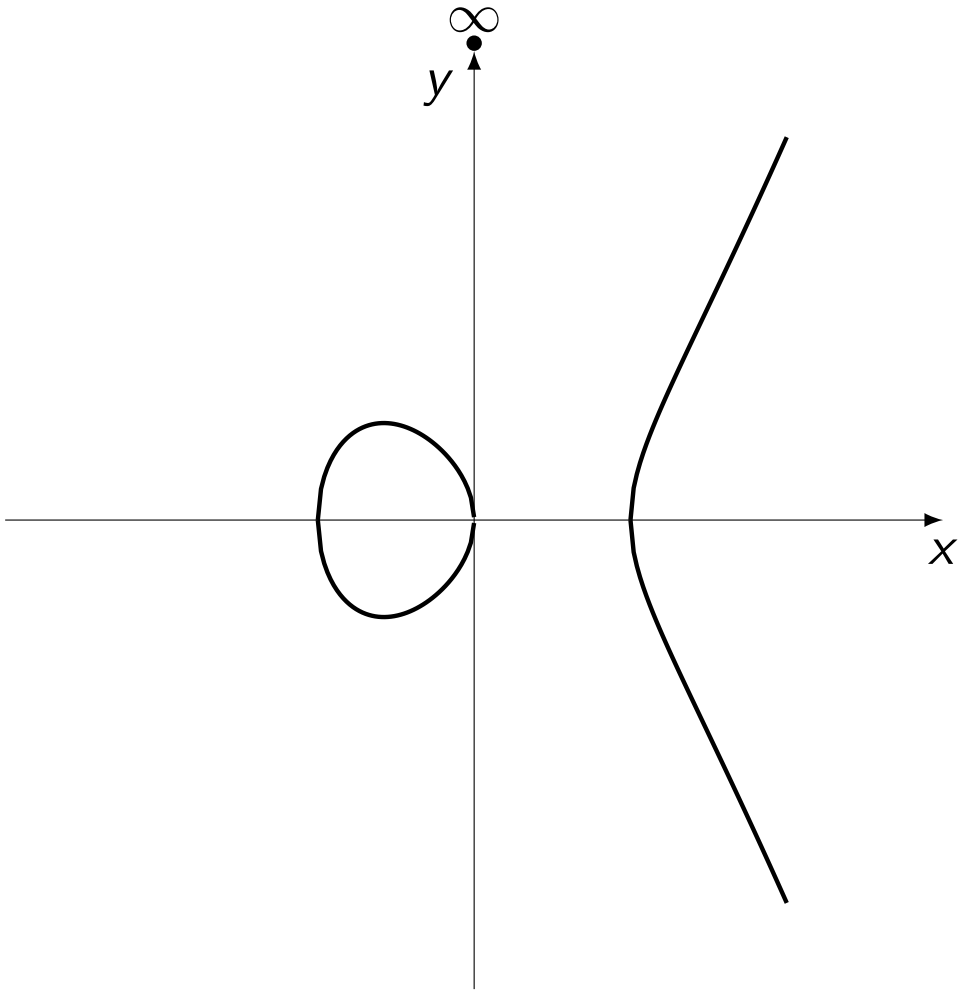
On the Construction of Elliptic Curves with a Prescribed Number of Points

Eugenio Paracucchi

Università di Pisa

28/01/2022

Equazione di Weierstrass

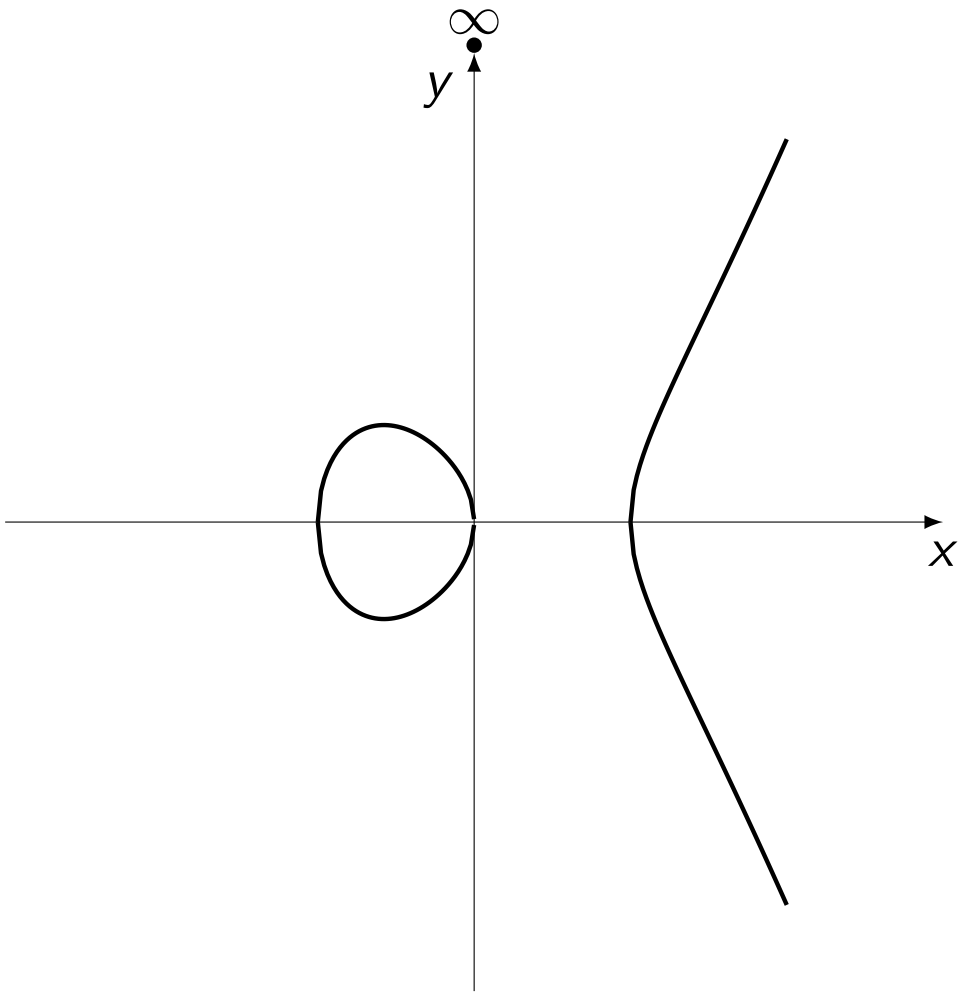


Sia K un campo di caratteristica diversa da 2 e da 3. Una curva ellittica su K è una varietà proiettiva in $\mathbb{P}^2_K$ definita da un'equazione

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3,$$

con $A, B \in K$ e $4A^3 + 27B^2 \neq 0$.

Equazione di Weierstrass



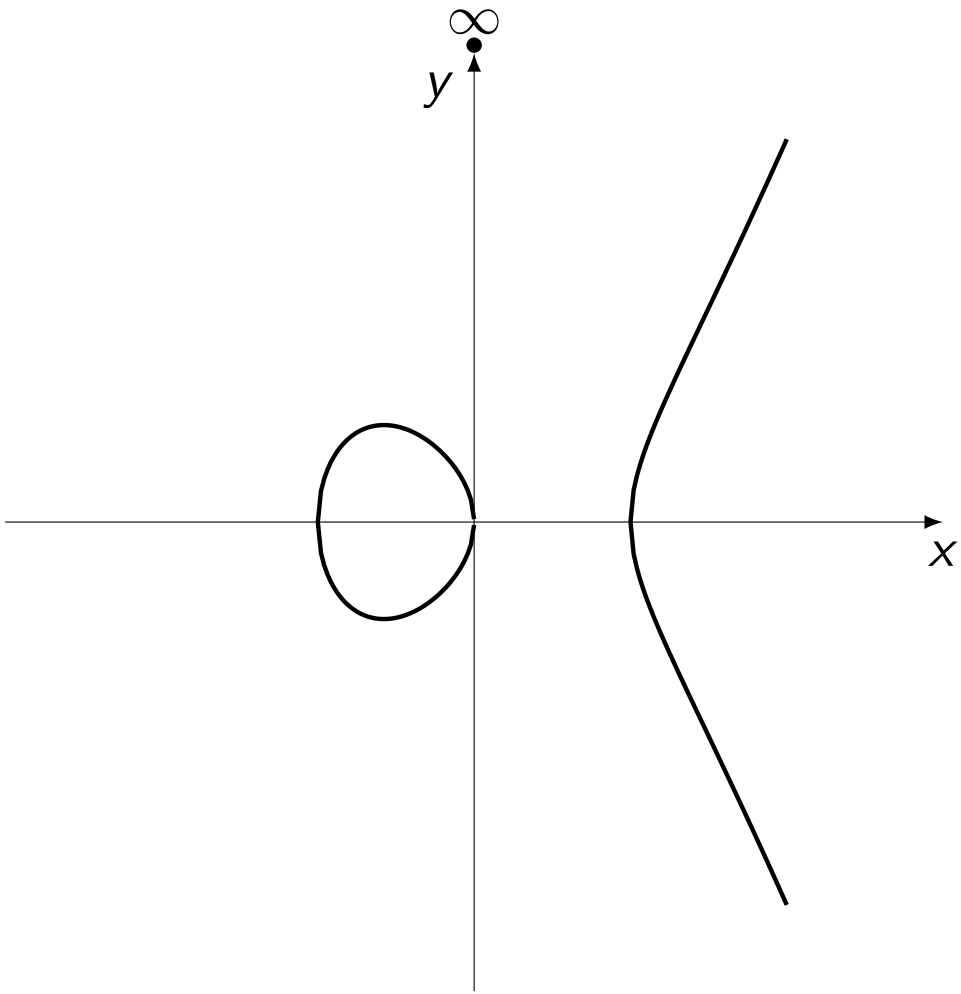
Sia K un campo di caratteristica diversa da 2 e da 3. Una curva ellittica su K è una varietà proiettiva in $\mathbb{P}^2_K$ definita da un'equazione

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3,$$

con $A, B \in K$ e $4A^3 + 27B^2 \neq 0$.

- $\infty = [0 : 1 : 0]$ è detto punto all'infinito.

Equazione di Weierstrass



Sia K un campo di caratteristica diversa da 2 e da 3. Una curva ellittica su K è una varietà proiettiva in $\mathbb{P}^2_K$ definita da un'equazione

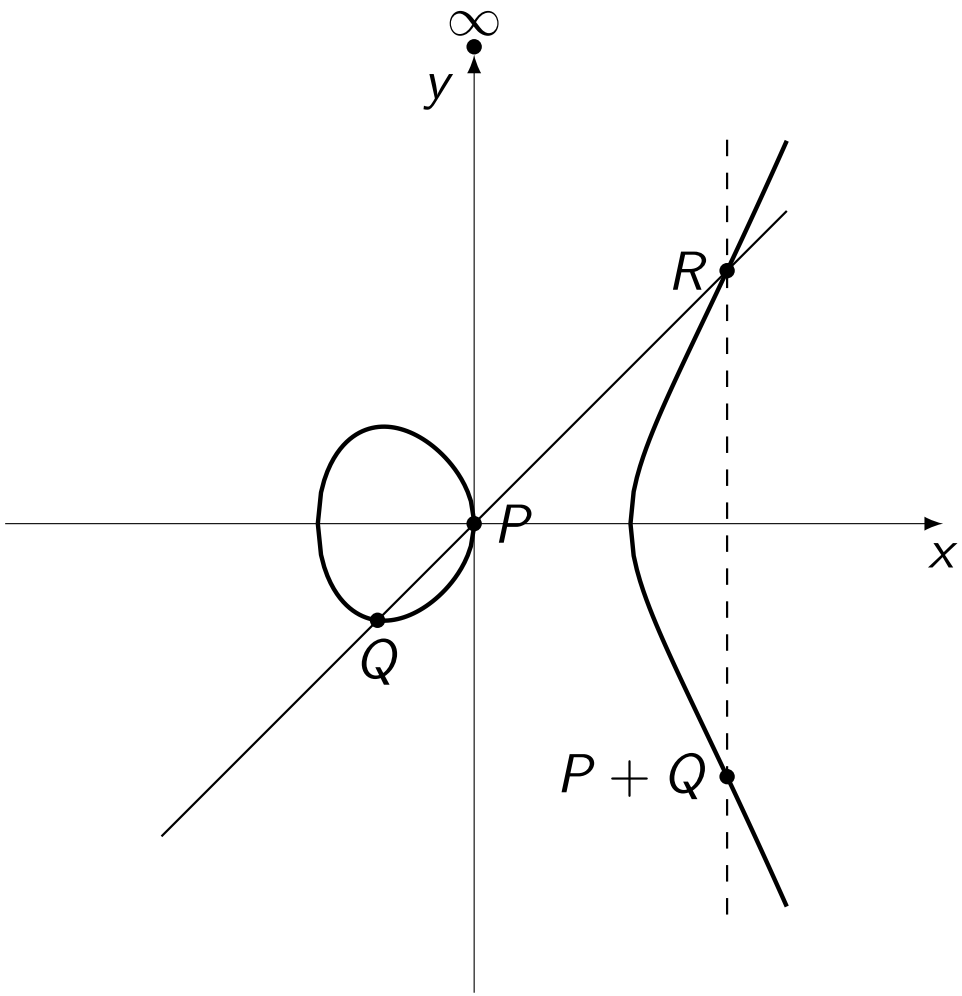
$$E : Y^2Z = X^3 + AXZ^2 + BZ^3,$$

con $A, B \in K$ e $4A^3 + 27B^2 \neq 0$.

- $\infty = [0 : 1 : 0]$ è detto punto all'infinito.
- Nelle coordinate affini $x = X/Z$, $y = Y/Z$

$$E : y^2 = x^3 + Ax + B.$$

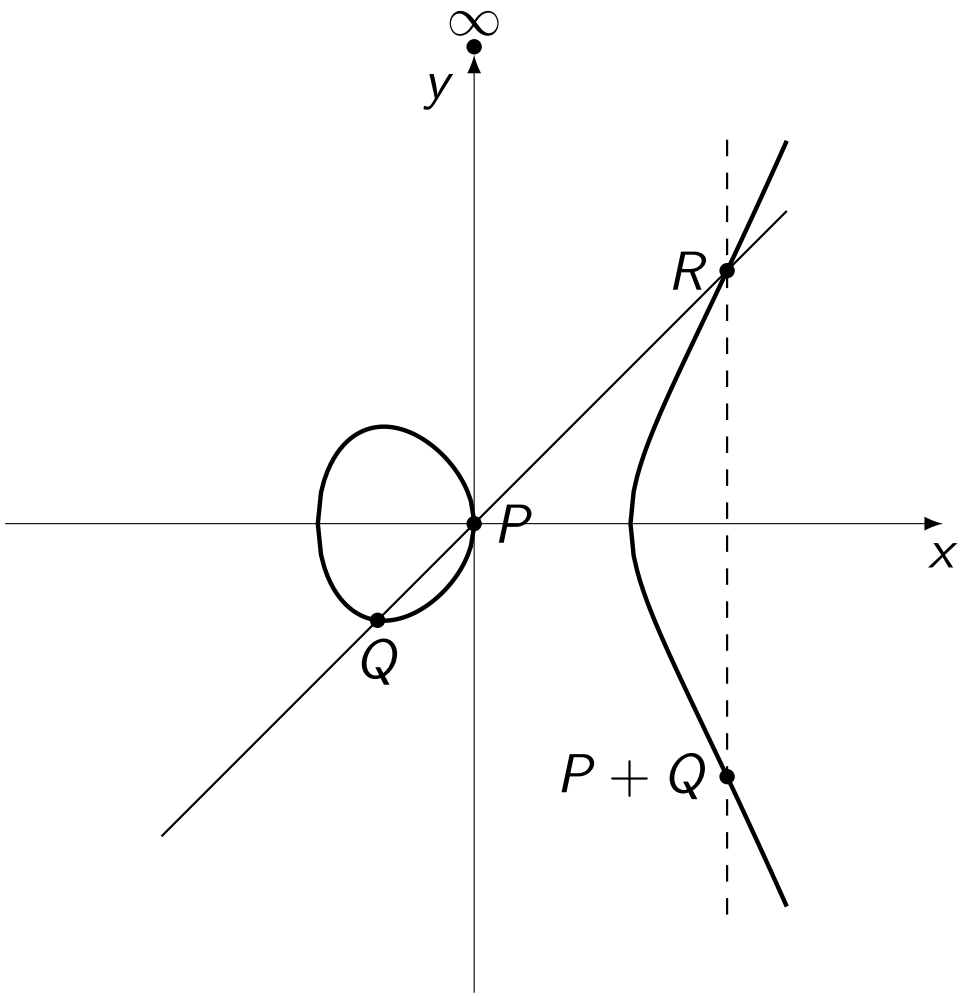
Legge di gruppo



Indichiamo con $E(K)$ l'insieme dei punti K-razionali, cioè l'insieme

$$\{(x,y) \in \mathbb{A}^2_K \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Legge di gruppo

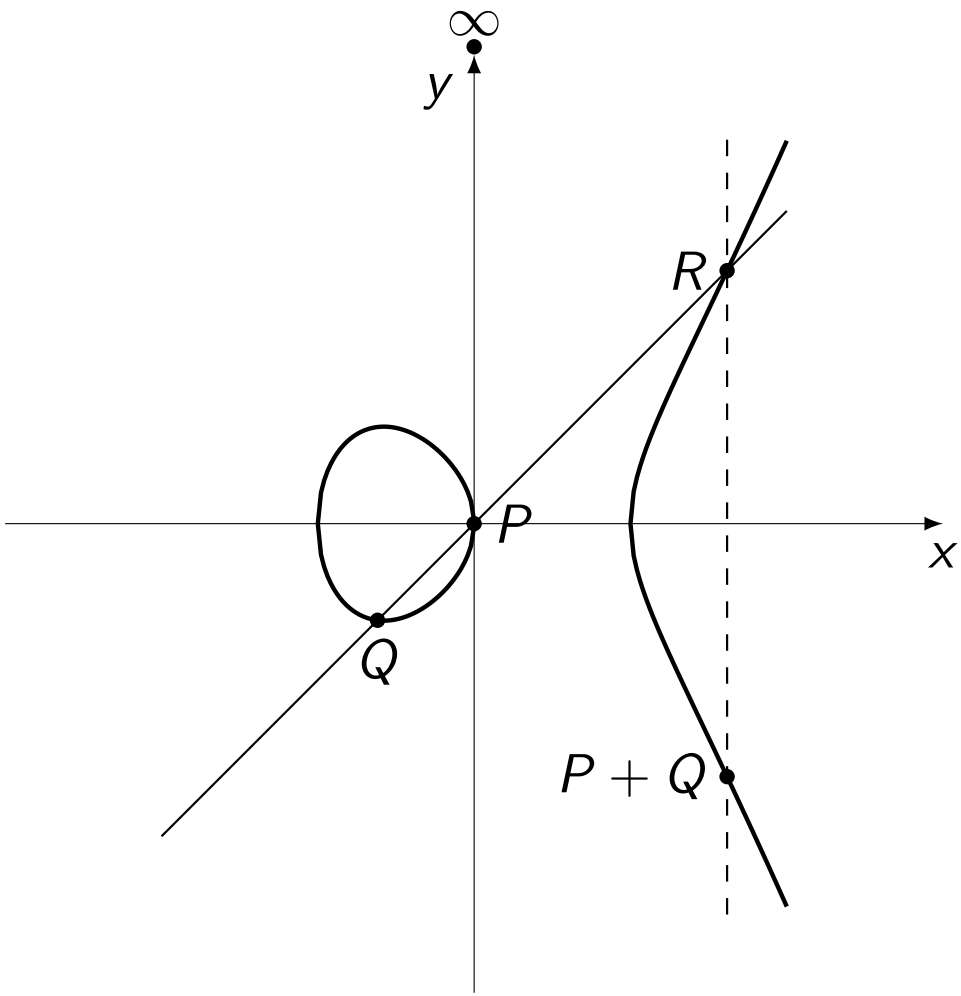


Indichiamo con $E(K)$ l'insieme dei punti K-razionali, cioè l'insieme

$$\{(x,y) \in \mathbb{A}^2_K \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Possiamo definire su $E(K)$ una somma, $+$, imponendo che tre punti allineati sommino a zero.

Legge di gruppo



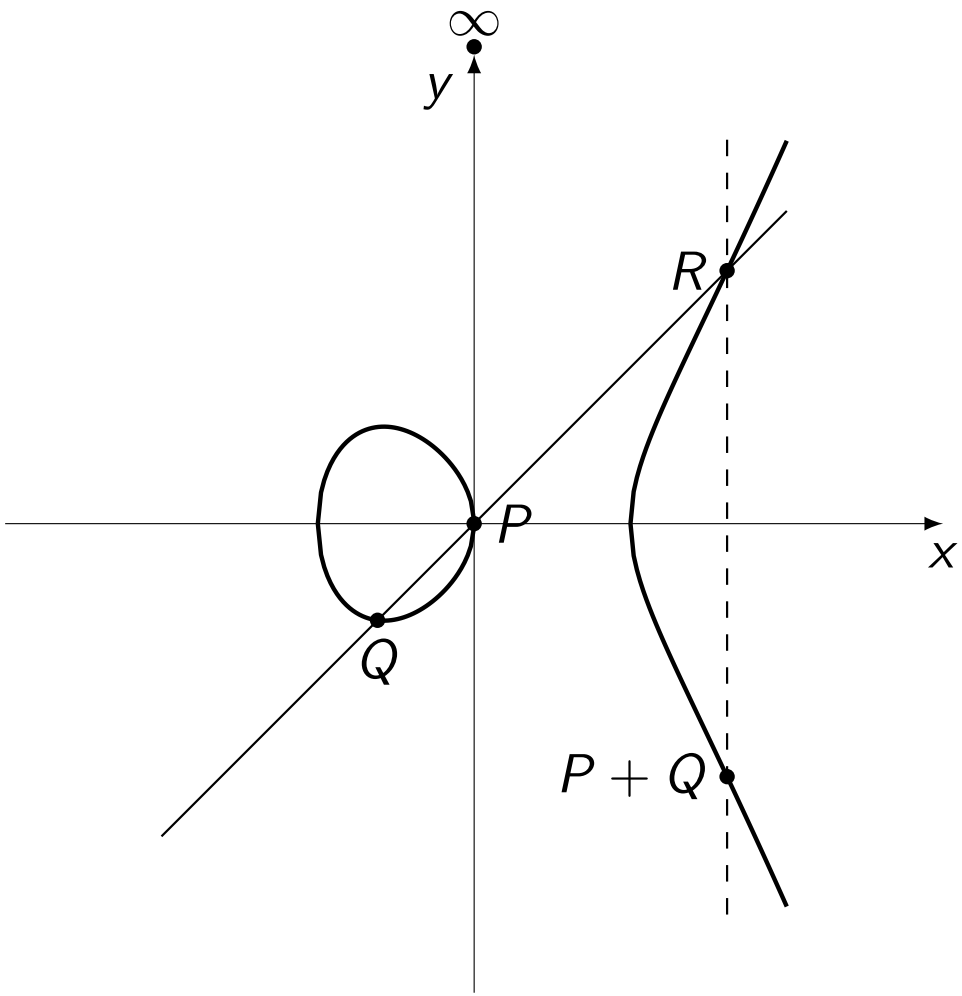
Indichiamo con $E(K)$ l'insieme dei punti K-razionali, cioè l'insieme

$$\{(x,y) \in \mathbb{A}^2_K \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Possiamo definire su $E(K)$ una somma, $+$, imponendo che tre punti allineati sommino a zero.

- ∞ è l'elemento neutro;

Legge di gruppo



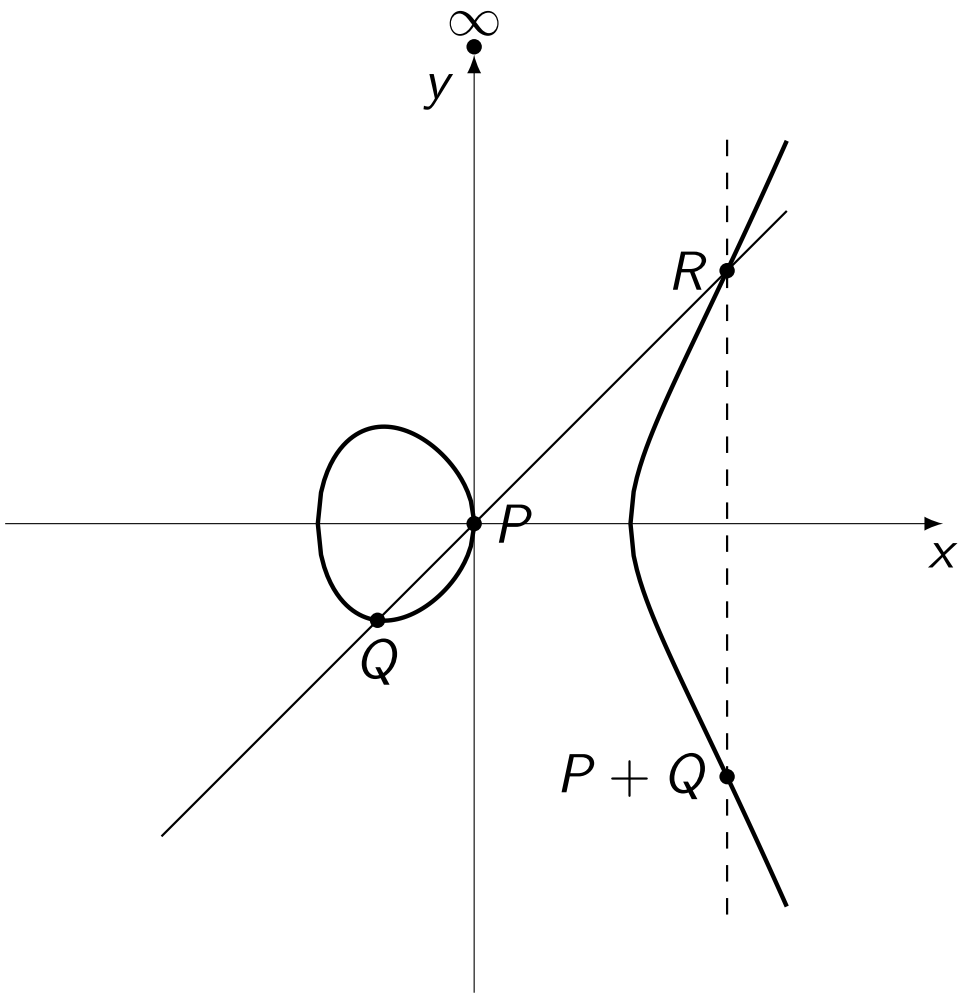
Indichiamo con $E(K)$ l'insieme dei punti K-razionali, cioè l'insieme

$$\{(x,y) \in \mathbb{A}^2_K \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Possiamo definire su $E(K)$ una somma, $+$, imponendo che tre punti allineati sommino a zero.

- ∞ è l'elemento neutro;
- l'operazione è commutativa;

Legge di gruppo



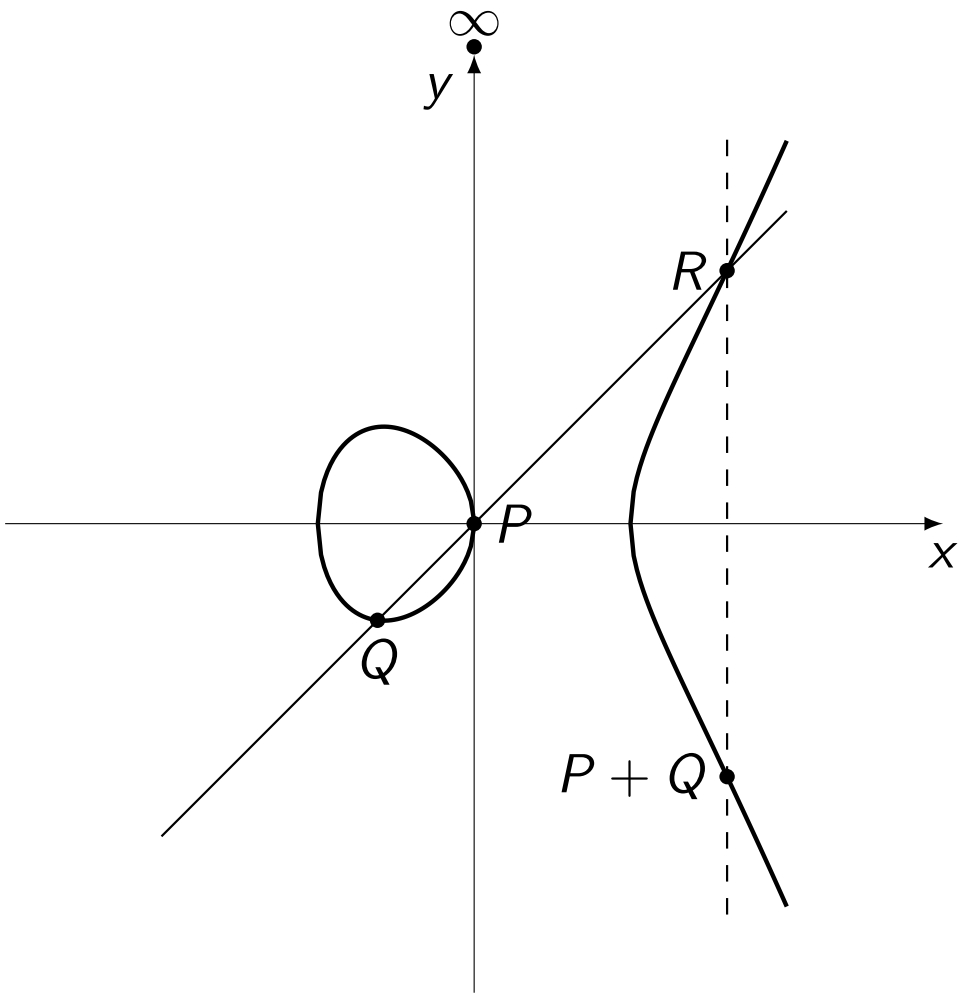
Indichiamo con $E(K)$ l'insieme dei punti K-razionali, cioè l'insieme

$$\{(x,y) \in \mathbb{A}^2_K \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Possiamo definire su $E(K)$ una somma, $+$, imponendo che tre punti allineati sommino a zero.

- ∞ è l'elemento neutro;
- l'operazione è commutativa;
- l'opposto di un punto si ottiene cambiando segno alla coordinata y.

Legge di gruppo



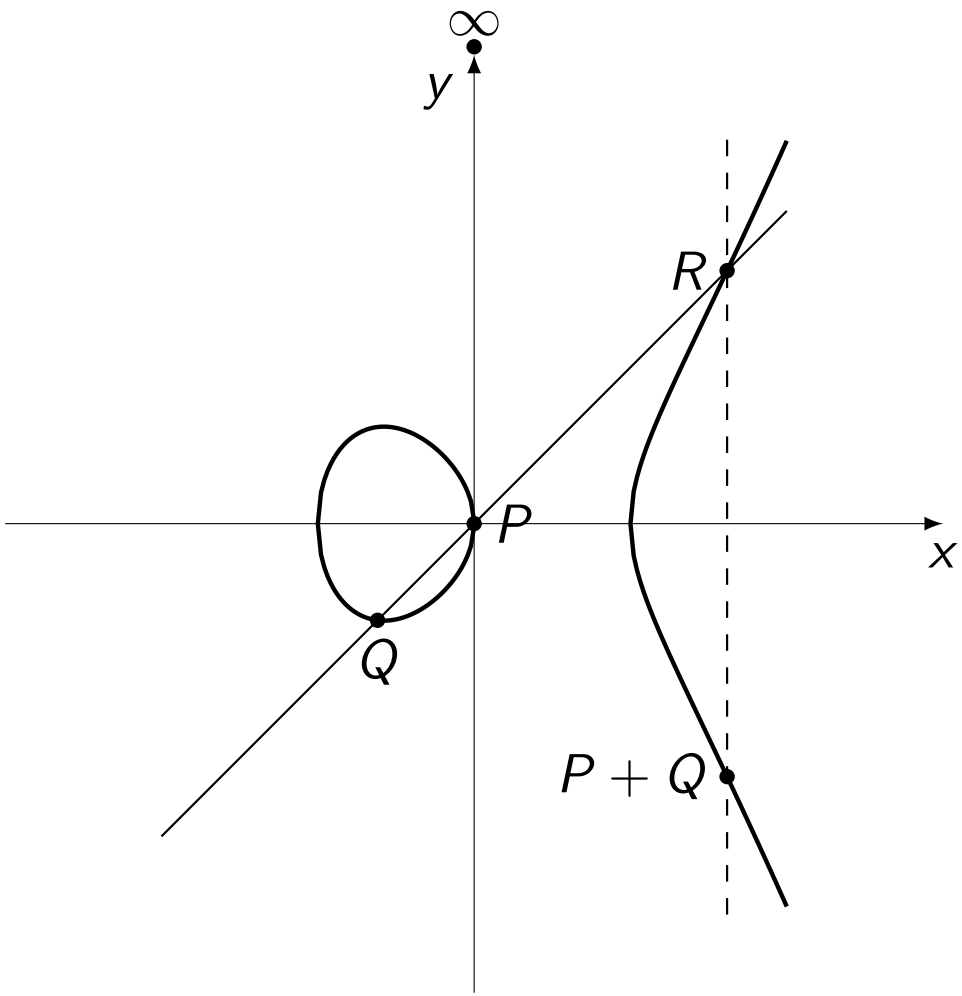
Indichiamo con $E(K)$ l'insieme dei punti K-razionali, cioè l'insieme

$$\{(x,y) \in \mathbb{A}^2_K \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Possiamo definire su $E(K)$ una somma, $+$, imponendo che tre punti allineati sommino a zero.

- ∞ è l'elemento neutro;
- l'operazione è commutativa;
- l'opposto di un punto si ottiene cambiando segno alla coordinata y.
- La somma di due punti è data da formule algebriche.

Legge di gruppo



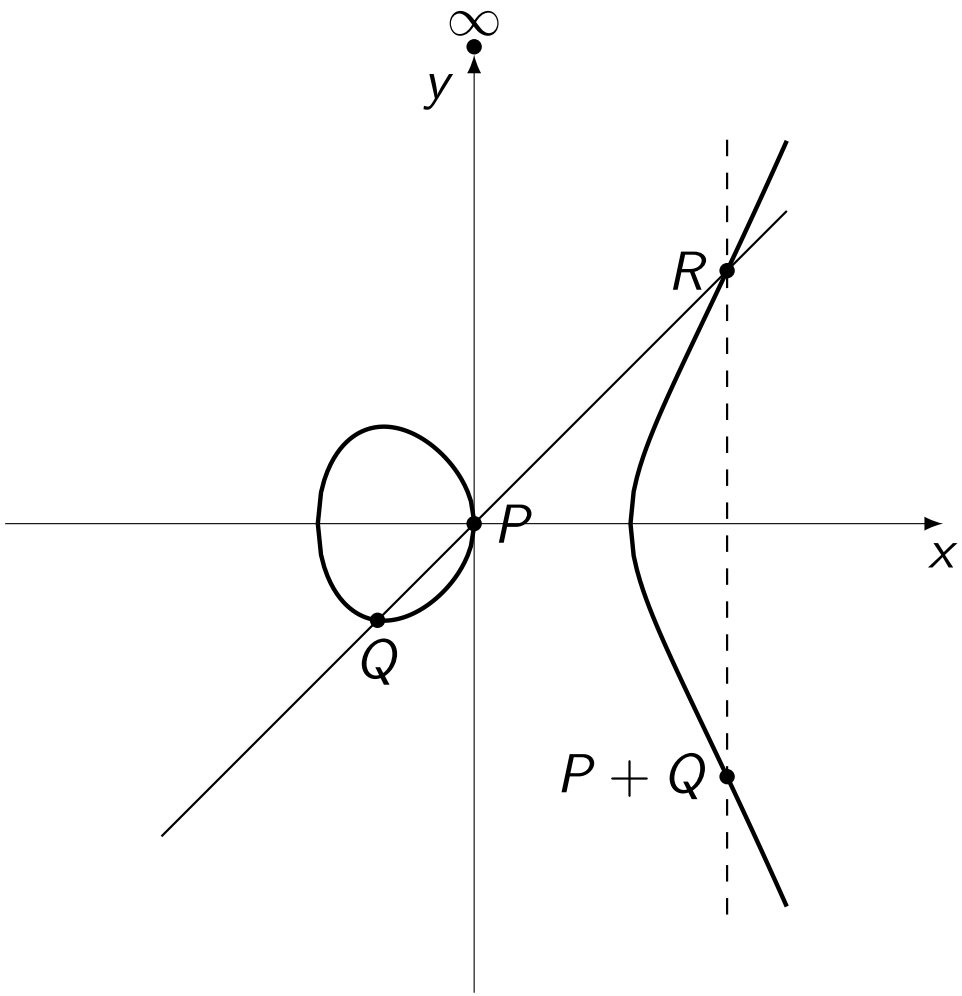
Indichiamo con $E(K)$ l'insieme dei punti K-razionali, cioè l'insieme

$$\{(x,y) \in \mathbb{A}^2_K \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Possiamo definire su $E(K)$ una somma, $+$, imponendo che tre punti allineati sommino a zero.

- ∞ è l'elemento neutro;
- l'operazione è commutativa;
- l'opposto di un punto si ottiene cambiando segno alla coordinata y.
- La somma di due punti è data da formule algebriche.

Legge di gruppo



Indichiamo con $E(K)$ l'insieme dei punti K-razionali, cioè l'insieme

$$\{(x,y) \in \mathbb{A}^2_K \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Possiamo definire su $E(K)$ una somma, $+$, imponendo che tre punti allineati sommino a zero.

- ∞ è l'elemento neutro;
- l'operazione è commutativa;
- l'opposto di un punto si ottiene cambiando segno alla coordinata y.
- La somma di due punti è data da formule algebriche.

Teorema

$(E(K), +)$ è un gruppo abeliano.

Isomorfismi

Quando due equazioni di Weierstrass definiscono curve ellittiche isomorfe ?

Isomorfismi

Quando due equazioni di Weierstrass definiscono curve ellittiche isomorfe ?

Invariante j

Sia $E : y^2 = x^3 + Ax + B$ una curva ellittica su K. Il suo invariante j è la quantità

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2},$$

ed è ben definito perché $4A^3 + 27B^2 \neq 0$.

Isomorfismi

Quando due equazioni di Weierstrass definiscono curve ellittiche isomorfe ?

Invariante j

Sia $E : y^2 = x^3 + Ax + B$ una curva ellittica su K. Il suo invariante j è la quantità

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2},$$

ed è ben definito perché $4A^3 + 27B^2 \neq 0$.

Fatto fondamentale

$E \cong_{\overline{K}} E' \iff j(E) = j(E')$. Inoltre un isomorfismo è dato da

$$(x, y) \mapsto (u^2x, u^3y)$$

con $u \in \overline{K}^{\times}$.

Sui campi finiti

Se $K = \mathbb{F}_q$ è un campo finito allora $E(\mathbb{F}_q)$ è un gruppo abeliano finito.

Sui campi finiti

Se $K = \mathbb{F}_q$ è un campo finito allora $E(\mathbb{F}_q)$ è un gruppo abeliano finito.

Hasse-Weil

Sia $E/\mathbb{F}_q$ una curva ellittica, allora vale la stima

$$q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}.$$

Sui campi finiti

Se $K = \mathbb{F}_q$ è un campo finito allora $E(\mathbb{F}_q)$ è un gruppo abeliano finito.

Hasse-Weil

Sia $E/\mathbb{F}_q$ una curva ellittica, allora vale la stima

$$q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}.$$

Questi oggetti "discreti" vengono ampiamente usati in crittografia.

Sui campi finiti

Se $K = \mathbb{F}_q$ è un campo finito allora $E(\mathbb{F}_q)$ è un gruppo abeliano finito.

Hasse-Weil

Sia $E/\mathbb{F}_q$ una curva ellittica, allora vale la stima

$$q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}.$$

Questi oggetti "discreti" vengono ampiamente usati in crittografia.

Nella pratica

- Scambio di chiavi in stile Diffie-Hellman $\rightarrow$ vorrei che $|E(\mathbb{F}_q)|$ fosse primo.
- Certificati di primalità $\rightarrow$ vorrei avere controllo su $|E(\mathbb{F}_q)|$.

Metodo CM

Il metodo CM produce delle coppie (p, E) con p primo ed $E/\mathbb{F}_p$ curva ellittica avente cardinalità $|E(\mathbb{F}_p)| = N$ data.

Metodo CM

Il metodo CM produce delle coppie (p, E) con p primo ed $E/\mathbb{F}_p$ curva ellittica avente cardinalità $|E(\mathbb{F}_p)| = N$ data.

Idea

Ridurre un'opportuna curva ellittica E definita su un campo di numeri F modulo un opportuno ideale primo $\mathfrak{p}$ di $\mathcal{O}_F$.

Metodo CM

Il metodo CM produce delle coppie (p, E) con p primo ed $E/\mathbb{F}_p$ curva ellittica avente cardinalità $|E(\mathbb{F}_p)| = N$ data.

Idea

Ridurre un'opportuna curva ellittica E definita su un campo di numeri F modulo un opportuno ideale primo $\mathfrak{p}$ di $\mathcal{O}_F$.

$$E : y^2 = x^3 + Ax + B \text{ su } F \rightsquigarrow \quad E_{\mathfrak{p}} : y^2 = x^3 + \overline{A}x + \overline{B} \text{ su } \mathcal{O}_F / \mathfrak{p} \cong \mathbb{F}_p$$

Metodo CM

Il metodo CM produce delle coppie (p, E) con p primo ed $E/\mathbb{F}_p$ curva ellittica avente cardinalità $|E(\mathbb{F}_p)| = N$ data.

Idea

Ridurre un'opportuna curva ellittica E definita su un campo di numeri F modulo un opportuno ideale primo $\mathfrak{p}$ di $\mathcal{O}_F$.

$$E : y^2 = x^3 + Ax + B \text{ su } F \rightsquigarrow \ E_{\mathfrak{p}} : y^2 = x^3 + \overline{A}x + \overline{B} \text{ su } \mathcal{O}_F / \mathfrak{p} \cong \mathbb{F}_p$$

Ingredienti

1. Curve ellittiche CM (Complex Multiplication).

Metodo CM

Il metodo CM produce delle coppie (p, E) con p primo ed $E/\mathbb{F}_p$ curva ellittica avente cardinalità $|E(\mathbb{F}_p)| = N$ data.

Idea

Ridurre un'opportuna curva ellittica E definita su un campo di numeri F modulo un opportuno ideale primo $\mathfrak{p}$ di $\mathcal{O}_F$.

$$E : y^2 = x^3 + Ax + B \text{ su } F \rightsquigarrow \ E_{\mathfrak{p}} : y^2 = x^3 + \overline{A}x + \overline{B} \text{ su } \mathcal{O}_F / \mathfrak{p} \cong \mathbb{F}_p$$

Ingredienti

1. Curve ellittiche CM (Complex Multiplication).
2. Buona riduzione.

Metodo CM

Il metodo CM produce delle coppie (p, E) con p primo ed $E/\mathbb{F}_p$ curva ellittica avente cardinalità $|E(\mathbb{F}_p)| = N$ data.

Idea

Ridurre un'opportuna curva ellittica E definita su un campo di numeri F modulo un opportuno ideale primo $\mathfrak{p}$ di $\mathcal{O}_F$.

$$E : y^2 = x^3 + Ax + B \text{ su } F \rightsquigarrow \ E_{\mathfrak{p}} : y^2 = x^3 + \overline{A}x + \overline{B} \text{ su } \mathcal{O}_F / \mathfrak{p} \cong \mathbb{F}_p$$

Ingredienti

1. Curve ellittiche CM (Complex Multiplication).
2. Buona riduzione.
3. Polinomi di classe.

Endomorfismi

Sia E/K una curva ellittica, un endomorfismo è una mappa algebrica $\varphi : E \longrightarrow E$ tale che $\varphi(\infty) = \infty$. Indichiamo con $\mathrm{End}(E)$ l'insieme degli endomorfismi di E.

Endomorfismi

Sia E/K una curva ellittica, un endomorfismo è una mappa algebrica $\varphi : E \longrightarrow E$ tale che $\varphi(\infty) = \infty$. Indichiamo con $\mathrm{End}(E)$ l'insieme degli endomorfismi di E.

Esempio

Per ogni intero positivo n

$$\begin{array}{rccc} [n]: & E & \longrightarrow & E \\ & P & \mapsto & \underbrace{P + \cdots + P}_{n \text{ volte}}. \end{array}$$

Per $n < 0$ si pone $[n]P := [-n](-P)$ e per $n = 0$, $[0]P := \infty$. Abbiamo dunque un'inclusione

$$\mathbb{Z} \hookrightarrow \mathrm{End}(E).$$

Endomorfismi

Sia E/K una curva ellittica, un endomorfismo è una mappa algebrica $\varphi : E \longrightarrow E$ tale che $\varphi(\infty) = \infty$. Indichiamo con $\mathrm{End}(E)$ l'insieme degli endomorfismi di E.

Esempio

Per ogni intero positivo n

$$\begin{array}{rccc} [n]: & E & \longrightarrow & E \\ & P & \mapsto & \underbrace{P + \cdots + P}_{n \text{ volte}}. \end{array}$$

Per $n < 0$ si pone $[n]P := [-n](-P)$ e per $n = 0$, $[0]P := \infty$. Abbiamo dunque un'inclusione

$$\mathbb{Z} \hookrightarrow \mathrm{End}(E).$$

Fatto importante

$(\mathrm{End}(E), +, \circ, [1], [0])$ è un anello.

Endomorfismi

Teorema

Sia E/K una curva ellittica. Allora $\mathrm{End}(E)$ è isomorfo a uno dei seguenti:

1. l'anello dei numeri interi $\mathbb{Z}$;
2. un ordine $\mathcal{O}$ in un campo immaginario quadratico K (i.e. un sottoanello che è uno $\mathbb{Z}$-modulo finitamente generato tale che $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = K$);
3. un ordine R in un'algebra di quaternioni H (i.e. un sottoanello che è uno $\mathbb{Z}$-modulo finitamente generato tale che $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = H$).

Endomorfismi

Teorema

Sia E/K una curva ellittica. Allora $\mathrm{End}(E)$ è isomorfo a uno dei seguenti:

1. l'anello dei numeri interi $\mathbb{Z}$;
2. un ordine $\mathcal{O}$ in un campo immaginario quadratico K (i.e. un sottoanello che è uno $\mathbb{Z}$-modulo finitamente generato tale che $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = K$);
3. un ordine R in un'algebra di quaternioni H (i.e. un sottoanello che è uno $\mathbb{Z}$-modulo finitamente generato tale che $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = H$).

Definizione

Se $\mathbb{Z} \subsetneq \mathrm{End}(E)$ diremo che E ha moltiplicazione complessa, brevemente CM.

Endomorfismi

Teorema

Sia E/K una curva ellittica. Allora $\mathrm{End}(E)$ è isomorfo a uno dei seguenti:

1. l'anello dei numeri interi $\mathbb{Z}$;
2. un ordine $\mathcal{O}$ in un campo immaginario quadratico K (i.e. un sottoanello che è uno $\mathbb{Z}$-modulo finitamente generato tale che $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = K$);
3. un ordine R in un'algebra di quaternioni H (i.e. un sottoanello che è uno $\mathbb{Z}$-modulo finitamente generato tale che $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = H$).

Definizione

Se $\mathbb{Z} \subsetneq \mathrm{End}(E)$ diremo che E ha moltiplicazione complessa, brevemente CM.

- Se $\mathrm{Char}\, K = 0$ allora $\mathrm{End}(E)$ è commutativo (quindi 3. non è possibile), e "tipicamente" $\mathrm{End}(E) = \mathbb{Z}$.
- Se $\mathrm{Char}\, K \neq 0$ allora $\mathbb{Z} \subsetneq \mathrm{End}(E)$ (quindi 1. non è possibile).

Due esempi

- $E : y^2 = x^3 + x$ su $\mathbb{C}$, la mappa

$$\begin{array}{rccc} [i] : & E & \longrightarrow & E \\ & (x, y) & \mapsto & (-x, iy) \\ & \infty & \mapsto & \infty \end{array}$$

è un endomorfismo e $[i]^2 = -id$. Quindi $\mathbb{Z} \subsetneq \mathrm{End}(E)$ e in effetti $\mathrm{End}(E) = \mathbb{Z}[i]$ è un ordine in $\mathbb{Q}(i)$.

- La stessa curva vista su $\mathbb{F}_p$ con $p \equiv 3 \pmod 4$ ha un comportamento diverso. La mappa

$$\begin{array}{rccc} F_p : & E & \longrightarrow & E \\ & (x, y) & \mapsto & (x^p, y^p) \\ & \infty & \mapsto & \infty \end{array}$$

è un endomorfismo e $[i] \circ F_p \neq F_p \circ [i]$ (intendiamo che $i \in \mathbb{F}_{p^2}$). Quindi $\mathrm{End}(E)$ è non commutativo (e quindi un ordine in un algebra di quaternioni).

Curve ellittiche CM

$E/\mathbb{C}$ curva ellittica CM, allora $\mathrm{End}(E) = \mathcal{O}$ è un ordine in un campo quadratico immaginario.

Curve ellittiche CM

$E/\mathbb{C}$ curva ellittica CM, allora $\mathrm{End}(E) = \mathcal{O}$ è un ordine in un campo quadratico immaginario. Ci interessano a meno di isomorfismo:

$$\mathcal{ELL}(\mathcal{O}) = \frac{\{E/\mathbb{C} \mid \mathrm{End}(E) = \mathcal{O}\}}{\text{isomorfismo}} = \{j(E) \mid \mathrm{End}(E) = \mathcal{O}\}$$

Curve ellittiche CM

$E/\mathbb{C}$ curva ellittica CM, allora $\mathrm{End}(E) = \mathcal{O}$ è un ordine in un campo quadratico immaginario. Ci interessano a meno di isomorfismo:

$$\mathcal{ELL}(\mathcal{O}) = \frac{\{E/\mathbb{C} \mid \mathrm{End}(E) = \mathcal{O}\}}{\text{isomorfismo}} = \{j(E) \mid \mathrm{End}(E) = \mathcal{O}\}$$

Fatti fondamentali

- $\mathcal{ELL}(\mathcal{O})$ è un insieme finito.

Curve ellittiche CM

$E/\mathbb{C}$ curva ellittica CM, allora $\mathrm{End}(E) = \mathcal{O}$ è un ordine in un campo quadratico immaginario. Ci interessano a meno di isomorfismo:

$$\mathcal{ELL}(\mathcal{O}) = \frac{\{E/\mathbb{C} \mid \mathrm{End}(E) = \mathcal{O}\}}{\text{isomorfismo}} = \{j(E) \mid \mathrm{End}(E) = \mathcal{O}\}$$

Fatti fondamentali

- $\mathcal{ELL}(\mathcal{O})$ è un insieme finito.
- $j(E)$ è un intero algebrico.

Costruzioni CM: setting

Sia $E/\mathbb{C}$ una curva ellittica CM.

Costruzioni CM: setting

Sia $E/\mathbb{C}$ una curva ellittica CM.

- $\mathrm{End}(E) = \mathcal{O}_D$ ordine di discriminante $D < -4$ in $K = \mathbb{Q}(\sqrt{D})$

Costruzioni CM: setting

Sia $E/\mathbb{C}$ una curva ellittica CM.

- $\mathrm{End}(E) = \mathcal{O}_D$ ordine di discriminante $D < -4$ in $K = \mathbb{Q}(\sqrt{D})$
- E è definita su F, il ring class field di $\mathcal{O}_D$, che è generata su K da $j(E)$:

$$F = K(j(E)).$$

Costruzioni CM: setting

Sia $E/\mathbb{C}$ una curva ellittica CM.

- $\mathrm{End}(E) = \mathcal{O}_D$ ordine di discriminante $D < -4$ in $K = \mathbb{Q}(\sqrt{D})$
- E è definita su F, il ring class field di $\mathcal{O}_D$, che è generata su K da $j(E)$:

$$F = K(j(E)).$$

Costruzioni CM: setting

Sia $E/\mathbb{C}$ una curva ellittica CM.

- $\mathrm{End}(E) = \mathcal{O}_D$ ordine di discriminante $D < -4$ in $K = \mathbb{Q}(\sqrt{D})$
- E è definita su F, il ring class field di $\mathcal{O}_D$, che è generata su K da $j(E)$:

$$F = K(j(E)).$$

Sia $p \in \mathbb{Z}$ un primo tale che

$$p\,\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}}$$

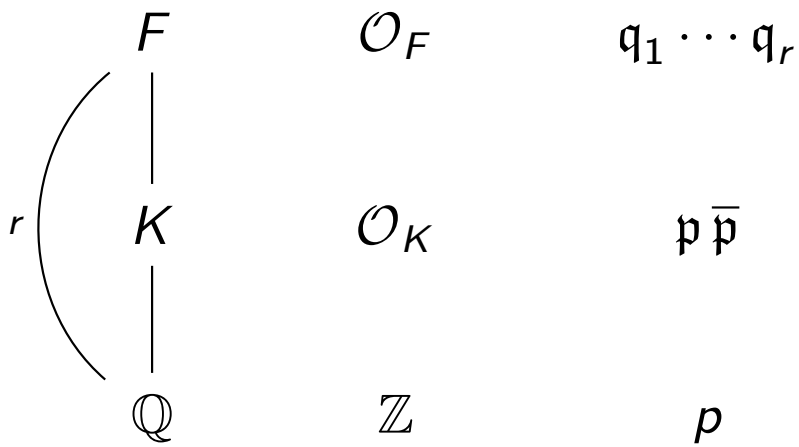
con $\mathfrak{p} = (\pi)$ primo, $\pi \in \mathcal{O}_D$.

Costruzioni CM

Conseguenza

p si spezza completamente in $\mathcal{O}_F$.

Graficamente



Costruzioni CM

Fissiamo un primo $\mathfrak{q} \mid p$ di $\mathcal{O}_F$.

Claim

Esiste L/F finita tale che E/L ha buona riduzione in ogni primo sopra $\mathfrak{q}$. Inoltre possiamo scegliere L in modo tale che $\mathfrak{q}$ sia totalmente ramificato.

Costruzioni CM

Fissiamo un primo $\mathfrak{q} \mid p$ di $\mathcal{O}_F$.

Claim

Esiste L/F finita tale che E/L ha buona riduzione in ogni primo sopra $\mathfrak{q}$. Inoltre possiamo scegliere L in modo tale che $\mathfrak{q}$ sia totalmente ramificato.
Infatti $j(E)$ è intero algebrico e quindi E/F ha buona riduzione potenziale in $\mathfrak{q}$.

Costruzioni CM

Fissiamo un primo $\mathfrak{q} \mid p$ di $\mathcal{O}_F$.

Claim

Esiste L/F finita tale che E/L ha buona riduzione in ogni primo sopra $\mathfrak{q}$. Inoltre possiamo scegliere L in modo tale che $\mathfrak{q}$ sia totalmente ramificato.
Infatti $j(E)$ è intero algebrico e quindi E/F ha buona riduzione potenziale in $\mathfrak{q}$.

Sia $\mathfrak{P} \mid \mathfrak{q}$ un primo di $\mathcal{O}_L$ (l'unico), allora esiste un modello $E : y^2 = x^3 + Ax + B$ con $A, B \in \mathcal{O}_L$ tale che la curva ridotta

$$E_{\mathfrak{P}} : y^2 = x^3 + \overline{A}x + \overline{B}$$

definita su $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_L / \mathfrak{P}$ sia una curva ellittica.

Costruzioni CM

Fissiamo un primo $\mathfrak{q} \mid p$ di $\mathcal{O}_F$.

Claim

Esiste L/F finita tale che E/L ha buona riduzione in ogni primo sopra $\mathfrak{q}$. Inoltre possiamo scegliere L in modo tale che $\mathfrak{q}$ sia totalmente ramificato.
Infatti $j(E)$ è intero algebrico e quindi E/F ha buona riduzione potenziale in $\mathfrak{q}$.

Sia $\mathfrak{P} \mid \mathfrak{q}$ un primo di $\mathcal{O}_L$ (l'unico), allora esiste un modello $E : y^2 = x^3 + Ax + B$ con $A, B \in \mathcal{O}_L$ tale che la curva ridotta

$$E_{\mathfrak{P}} : y^2 = x^3 + \overline{A}x + \overline{B}$$

definita su $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_L / \mathfrak{P}$ sia una curva ellittica.

- $\mathbb{F}_{\mathfrak{P}} \cong \mathbb{F}_p$

Costruzioni CM

Fissiamo un primo $\mathfrak{q} \mid p$ di $\mathcal{O}_F$.

Claim

Esiste L/F finita tale che E/L ha buona riduzione in ogni primo sopra $\mathfrak{q}$. Inoltre possiamo scegliere L in modo tale che $\mathfrak{q}$ sia totalmente ramificato.
Infatti $j(E)$ è intero algebrico e quindi E/F ha buona riduzione potenziale in $\mathfrak{q}$.

Sia $\mathfrak{P} \mid \mathfrak{q}$ un primo di $\mathcal{O}_L$ (l'unico), allora esiste un modello $E : y^2 = x^3 + Ax + B$ con $A, B \in \mathcal{O}_L$ tale che la curva ridotta

$$E_{\mathfrak{P}} : y^2 = x^3 + \overline{A}x + \overline{B}$$

definita su $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_L / \mathfrak{P}$ sia una curva ellittica.

- $\mathbb{F}_{\mathfrak{P}} \cong \mathbb{F}_p$
- $j(E_{\mathfrak{P}}) \equiv j(E) \pmod{\mathfrak{q}}$

Costruzioni CM

Fissiamo un primo $\mathfrak{q} \mid p$ di $\mathcal{O}_F$.

Claim

Esiste L/F finita tale che E/L ha buona riduzione in ogni primo sopra $\mathfrak{q}$. Inoltre possiamo scegliere L in modo tale che $\mathfrak{q}$ sia totalmente ramificato.
Infatti $j(E)$ è intero algebrico e quindi E/F ha buona riduzione potenziale in $\mathfrak{q}$.

Sia $\mathfrak{P} \mid \mathfrak{q}$ un primo di $\mathcal{O}_L$ (l'unico), allora esiste un modello $E : y^2 = x^3 + Ax + B$ con $A, B \in \mathcal{O}_L$ tale che la curva ridotta

$$E_{\mathfrak{P}} : y^2 = x^3 + \overline{A}x + \overline{B}$$

definita su $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_L / \mathfrak{P}$ sia una curva ellittica.

- $\mathbb{F}_{\mathfrak{P}} \cong \mathbb{F}_p$
- $j(E_{\mathfrak{P}}) \equiv j(E) \pmod{\mathfrak{q}}$

Costruzioni CM

Fissiamo un primo $\mathfrak{q} \mid p$ di $\mathcal{O}_F$.

Claim

Esiste L/F finita tale che E/L ha buona riduzione in ogni primo sopra $\mathfrak{q}$. Inoltre possiamo scegliere L in modo tale che $\mathfrak{q}$ sia totalmente ramificato.
Infatti $j(E)$ è intero algebrico e quindi E/F ha buona riduzione potenziale in $\mathfrak{q}$.

Sia $\mathfrak{P} \mid \mathfrak{q}$ un primo di $\mathcal{O}_L$ (l'unico), allora esiste un modello $E : y^2 = x^3 + Ax + B$ con $A, B \in \mathcal{O}_L$ tale che la curva ridotta

$$E_{\mathfrak{P}} : y^2 = x^3 + \overline{A}x + \overline{B}$$

definita su $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_L / \mathfrak{P}$ sia una curva ellittica.

- $\mathbb{F}_{\mathfrak{P}} \cong \mathbb{F}_p$
- $j(E_{\mathfrak{P}}) \equiv j(E) \pmod{\mathfrak{q}}$

Miracolo

$$|E_{\mathfrak{P}}(\mathbb{F}_p)| = p + 1 \pm \mathrm{Tr}_{K/\mathbb{Q}}(\pi)$$

Conseguenza

Scegliendo D e p in maniera opportuna otteniamo curve ellittiche su $\mathbb{F}_p$ di cardinalità assegnata.

Conseguenza

Scegliendo D e p in maniera opportuna otteniamo curve ellittiche su $\mathbb{F}_p$ di cardinalità assegnata.

Domande

1. Quali sono i primi p tali per cui esiste $\pi \in \mathcal{O}_D$ di norma p ?

Conseguenza

Scegliendo D e p in maniera opportuna otteniamo curve ellittiche su $\mathbb{F}_p$ di cardinalità assegnata.

Domande

1. Quali sono i primi p tali per cui esiste $\pi \in \mathcal{O}_D$ di norma p ?
2. Come calcolo $j(E_{\mathfrak{P}})$?

Conseguenza

Scegliendo D e p in maniera opportuna otteniamo curve ellittiche su $\mathbb{F}_p$ di cardinalità assegnata.

Domande

1. Quali sono i primi p tali per cui esiste $\pi \in \mathcal{O}_D$ di norma p ?
2. Come calcolo $j(E_{\mathfrak{P}})$?
3. Dato N intero positivo, qual è il modo giusto di scegliere D e p tali che $|E_{\mathfrak{P}}(\mathbb{F}_p)| = N$?

Primi di norma p

Sia $p > 3$ un primo che non divide il discriminante D. Allora esiste $\pi \in \mathcal{O}_D$ di norma p se e soltanto se la seguente equazione

$$4p = t^2 - v^2 D$$

ha soluzioni intere (t, v). In tal caso si ha che $\mathrm{Tr}_{K/\mathbb{Q}}(\pi) = \pm t$.

Primi di norma p

Sia $p > 3$ un primo che non divide il discriminante D. Allora esiste $\pi \in \mathcal{O}_D$ di norma p se e soltanto se la seguente equazione

$$4p = t^2 - v^2 D$$

ha soluzioni intere (t, v). In tal caso si ha che $\mathrm{Tr}_{K/\mathbb{Q}}(\pi) = \pm t$.

Operativamente

Dato p, risolviamo l'equazione $4p = t^2 - v^2 D$ con l'algoritmo di Cornacchia.

Il polinomio di Hilbert

Definizione

Sia $D < 0$ un discriminante. Il polinomio di Hilbert è

$$H_D(x) = \prod_{j(E) \in \mathcal{ELL}(\mathcal{O}_D)} (x - j(E)).$$

Il polinomio di Hilbert

Definizione

Sia $D < 0$ un discriminante. Il polinomio di Hilbert è

$$H_D(x) = \prod_{j(E) \in \mathcal{ELL}(\mathcal{O}_D)} (x - j(E)).$$

Fatto fondamentale

$H_D(x)$ ha coefficienti interi.

Il polinomio di Hilbert

Definizione

Sia $D < 0$ un discriminante. Il polinomio di Hilbert è

$$H_D(x) = \prod_{j(E) \in \mathcal{ELL}(\mathcal{O}_D)} (x - j(E)).$$

Fatto fondamentale

$H_D(x)$ ha coefficienti interi.

Quindi se p, $\mathfrak{q}$ e $\mathfrak{P}$ sono come prima allora $j(E_{\mathfrak{P}}) \equiv j(E) \pmod{\mathfrak{q}}$ è soluzione di $H_D(x) \pmod{p}$.

Il polinomio di Hilbert

Definizione

Sia $D < 0$ un discriminante. Il polinomio di Hilbert è

$$H_D(x) = \prod_{j(E) \in \mathcal{ELL}(\mathcal{O}_D)} (x - j(E)).$$

Fatto fondamentale

$H_D(x)$ ha coefficienti interi.

Quindi se p, $\mathfrak{q}$ e $\mathfrak{P}$ sono come prima allora $j(E_{\mathfrak{P}}) \equiv j(E) \pmod{\mathfrak{q}}$ è soluzione di $H_D(x) \pmod{p}$.

Operativamente

Calcolo $H_D(x) \in \mathbb{Z}[x]$ e successivamente una radice $j_0 \in \mathbb{F}_p$ di $H_D(x) \pmod{p}$.

Metodo CM: ricetta

1. Dato N intero positivo, iniziando da $D < -4$, si cerca un discriminante D e una soluzione intera (s, v) all'equazione quadratica

$$4N = s^2 - v^2 D$$

tale che $p = N - 1 + t$ sia primo, posto $t = s + 2$. Allora

$$4p = t^2 - v^2 D$$

Metodo CM: ricetta

1. Dato N intero positivo, iniziando da $D < -4$, si cerca un discriminante D e una soluzione intera (s, v) all'equazione quadratica

$$4N = s^2 - v^2 D$$

tale che $p = N - 1 + t$ sia primo, posto $t = s + 2$. Allora

$$4p = t^2 - v^2 D$$

2. Si calcola $H_D(x) \in \mathbb{Z}[x]$ e una soluzione j_0 di $H_D(x) \pmod p$. Per quanto detto j_0 è l'invariante j di $E_{\mathfrak{P}}/\mathbb{F}_p$ tale che (a meno di un twist quadratico)

$$|E_{\mathfrak{P}}(\mathbb{F}_p)| = p + 1 - t = N$$

Polinomio di Hilbert: continuazione

Esempio

Se $D = -71$ allora

$$\begin{aligned} H_{-71}(x) = x^7 &+ 313645809715x^6 - 3091990138604570x^5 + \\ &+ 9839403881004781204930 2x^4 - 8235342634397307799680913 89x^3 + \\ &+ 513880036645397678032372632 9446x^2 + \\ &- 425319473946139603274605151187659x + \\ &+ 737707086760731113357714241006081263 \end{aligned}$$

e all'aumentare di $|D|$ va ancora peggio...

Polinomio di Hilbert: continuazione

Esempio

Se $D = -71$ allora

$$\begin{aligned} H_{-71}(x) = x^7 &+ 313645809715x^6 - 3091990138604570x^5 + \\ &+ 9839403881004781204930 2x^4 - 8235342634397307799680913 89x^3 + \\ &+ 513880036645397678032372632 9446x^2 + \\ &- 425319473946139603274605151187659x + \\ &+ 737707086760731113357714241006081263 \end{aligned}$$

e all'aumentare di $|D|$ va ancora peggio... Alternative?

$$\begin{aligned} G_{-71}(x) = x^7 &+ 6745x^6 - 327467x^5 + 51857115x^4 - 2319299751x^3 \\ &+ 41264582513x^2 - 307873876442x + 903568991567 \end{aligned}$$

La funzione j

Fatto fondamentale

Esiste una corrispondenza biunivoca tra

$$\frac{\left\{\text{Reticoli in } \mathbb{C}\right\}}{\text{omotetia}} \longleftrightarrow \frac{\left\{\text{Curve ellittiche su } \mathbb{C}\right\}}{\text{isomorfismo}}$$

data da $\Lambda \mapsto E_\Lambda = \mathbb{C}/\Lambda$.

La funzione j

Fatto fondamentale

Esiste una corrispondenza biunivoca tra

$$\frac{\left\{\text{Reticoli in } \mathbb{C}\right\}}{\text{omotetia}} \longleftrightarrow \frac{\left\{\text{Curve ellittiche su } \mathbb{C}\right\}}{\text{isomorfismo}}$$

data da $\Lambda \mapsto E_\Lambda = \mathbb{C}/\Lambda$.

A meno di omotetia $\Lambda = \Lambda_\tau = \langle 1, \tau \rangle_{\mathbb{Z}}$ con $\tau \in \mathcal{H}$.

La funzione j

Fatto fondamentale

Esiste una corrispondenza biunivoca tra

$$\frac{\left\{\text{Reticoli in } \mathbb{C}\right\}}{\text{omotetia}} \longleftrightarrow \frac{\left\{\text{Curve ellittiche su } \mathbb{C}\right\}}{\text{isomorfismo}}$$

data da $\Lambda \mapsto E_\Lambda = \mathbb{C}/\Lambda$.

A meno di omotetia $\Lambda = \Lambda_\tau = \langle 1, \tau \rangle_{\mathbb{Z}}$ con $\tau \in \mathcal{H}$.

Conseguenza

Possiamo parametrizzare le curve ellittiche su $\mathbb{C}$ con $\tau \in \mathcal{H}$. La funzione j è

$$\begin{array}{rccc} j: & \mathcal{H} & \longrightarrow & \mathbb{C} \\ & \tau & \mapsto & j(E_{\Lambda_\tau}) \end{array}$$

La funzione γ

Definiamo per ogni $\tau \in \mathcal{H}$ la funzione γ come

$$\gamma(\tau) = j(\tau)^{1/3}.$$

La funzione γ

Definiamo per ogni $\tau \in \mathcal{H}$ la funzione γ come

$$\gamma(\tau) = j(\tau)^{1/3}.$$

In effetti esiste una determinazione olomorfa della radice cubica di $j(\tau)$ con la proprietà che sia reale per τ sull'asse immaginario positivo, e prendiamo quella.

Parametrizzare $\mathcal{ELL}(\mathcal{O}_D)$

L'insieme $\mathcal{ELL}(\mathcal{O}_D)$ è parametrizzato dalle terne di numeri interi (a, b, c) tali che

- $\gcd(a, b, c) = 1$ e $b^2 - 4ac = D$;
- $|b| \leq a \leq c$, $3a^2 \leq |D|$;
- $b \geq 0$ se $a = |b|$ oppure $a = c$.

Parametrizzare $\mathcal{ELL}(\mathcal{O}_D)$

L'insieme $\mathcal{ELL}(\mathcal{O}_D)$ è parametrizzato dalle terne di numeri interi (a, b, c) tali che

- $\gcd(a, b, c) = 1$ e $b^2 - 4ac = D$;
- $|b| \leq a \leq c$, $3a^2 \leq |D|$;
- $b \geq 0$ se $a = |b|$ oppure $a = c$.

$$(a, b, c) \longleftrightarrow \tau = \frac{-b + \sqrt{D}}{2a} \in \mathcal{H}$$

I polinomi di classe

Questa bigezione permette di calcolare il polinomio di Hilbert:

$$H_D(x) = \prod_{j(\tau) \in \mathcal{ELL}(\mathcal{O}_D)} (x - j(\tau))$$

calcolando in maniera approssimata $j(\tau)$ e troncando i coefficienti all'intero più vicino ($H_D(x) \in \mathbb{Z}[x]$).

I polinomi di classe

Questa bigezione permette di calcolare il polinomio di Hilbert:

$$H_D(x) = \prod_{j(\tau) \in \mathcal{ELL}(\mathcal{O}_D)} (x - j(\tau))$$

calcolando in maniera approssimata $j(\tau)$ e troncando i coefficienti all'intero più vicino ($H_D(x) \in \mathbb{Z}[x]$). E analogamente si più calcolare il polinomio

$$G_D(x) = \prod_{\tau \in L} (x - \gamma(\tau))$$

associato a γ.

I polinomi di classe

Questa bigezione permette di calcolare il polinomio di Hilbert:

$$H_D(x) = \prod_{j(\tau) \in \mathcal{ELL}(\mathcal{O}_D)} (x - j(\tau))$$

calcolando in maniera approssimata $j(\tau)$ e troncando i coefficienti all'intero più vicino ($H_D(x) \in \mathbb{Z}[x]$). E analogamente si più calcolare il polinomio

$$G_D(x) = \prod_{\tau \in L} (x - \gamma(\tau))$$

associato a γ.

Conseguenza

Essendo γ una radice cubica di j in effetti c'è un riscalamento nel numero di cifre dei coefficienti di un fattore 3.

Conseguenza

Teorema

Per ogni discriminante $D < 0$ coprimo con 3 e per ogni $\tau \in \mathcal{H}$ di discriminante D, $\gamma(\tau)$ genera il ring class field F su K:

$$F = K(\gamma(\tau)).$$

Conseguenza

Teorema

Per ogni discriminante $D < 0$ coprimo con 3 e per ogni $\tau \in \mathcal{H}$ di discriminante D, $\gamma(\tau)$ genera il ring class field F su K:

$$F = K(\gamma(\tau)).$$

Corollario

Per ogni D coprimo con 3 possiamo utilizzare $G_D(x)$ per calcolare $j(E_{\mathfrak{P}})$.

Un esempio

Vorremmo costruire una curva ellittica di cardinalità $N = 326132277207894252432172848851$ (N è primo).

Un esempio

Vorremmo costruire una curva ellittica di cardinalità $N = 326132277207894252432172848851$ (N è primo). Il nostro metodo produce

- un primo $p = 326132277207894333312854848063$ e un discriminante $D = -163$;

Un esempio

Vorremmo costruire una curva ellittica di cardinalità $N = 326132277207894252432172848851$ (N è primo). Il nostro metodo produce

- un primo $p = 326132277207894333312854848063$ e un discriminante $D = -163$;
- il polinomio di classe

$$G_D(x) = x + 640320;$$

Un esempio

Vorremmo costruire una curva ellittica di cardinalità $N = 326132277207894252432172848851$ (N è primo). Il nostro metodo produce

- un primo $p = 326132277207894333312854848063$ e un discriminante $D = -163$;
- il polinomio di classe
$$G_D(x) = x + 640320;$$
- un invariante $j_0 = 326132277207631795900214080063 \in \mathbb{F}_p$ che conduce alla curva

$$E : y^2 = x^3 + 294742070423344886529589199 53x + 8130401512858491361883408144$$

di cardinalità $|E(\mathbb{F}_p)| = N$.

Un esempio

Vorremmo costruire una curva ellittica di cardinalità $N = 326132277207894252432172848851$ (N è primo). Il nostro metodo produce

- un primo $p = 326132277207894333312854848063$ e un discriminante $D = -163$;
- il polinomio di classe
$$G_D(x) = x + 640320;$$
- un invariante $j_0 = 326132277207631795900214080063 \in \mathbb{F}_p$ che conduce alla curva

$$E : y^2 = x^3 + 294742070423344886529589199 53x + 8130401512858491361883408144$$

di cardinalità $|E(\mathbb{F}_p)| = N$.

Un esempio

Vorremmo costruire una curva ellittica di cardinalità $N = 32613227720789425243217284885 1$ (N è primo). Il nostro metodo produce

- un primo $p = 32613227720789433331285484806 3$ e un discriminante $D = -163$;
- il polinomio di classe
$$G_D(x) = x + 640320;$$
- un invariante $j_0 = 32613227720763179590021408006 3 \in \mathbb{F}_p$ che conduce alla curva
$$E : y^2 = x^3 + 29474207042334448865295891995 3x + 8130401512858491361883408144$$
di cardinalità $|E(\mathbb{F}_p)| = N$.

Nota

Osserviamo che $H_D(x) = x + 262537412640768000 = x + 640320^3$.

Grazie per la vostra attenzione !