Berechnung Isogenien elliptischer Kurven

Anita Krahmann

Fakultät für Mathematik
Technische Universität Berlin

15.02.2006

logo

Outline

Generalvoraussetzung

Sei K ein endlicher Primkörper der Charakteristik $p > 3$,
sei $\tilde{K}$ ein Erweiterungskörper von K.

Outline

logo

Elliptische Kurven

- *elliptische Kurve*: E/K Gleichung in zwei Variablen x und y
- $y^2 = x^3 + ax + b$ mit $a, b \in K$
- $\triangle(E) := -16(4a^3 + 27b^2) \neq 0$
- Dazu gehört auch noch ein Punkt $\mathcal{O}$ "im Unendlichen"
- *j-Invariante* $j(E) := -1728(4a^3)/\triangle(E)$

Elliptische Kurven

- *elliptische Kurve*: E/K Gleichung in zwei Variablen x und y
- $y^2 = x^3 + ax + b$ mit $a, b \in K$
- $\triangle(E) := -16(4a^3 + 27b^2) \neq 0$
- Dazu gehört auch noch ein Punkt $\mathcal{O}$ "im Unendlichen"
- *j-Invariante* $j(E) := -1728(4a^3)/\triangle(E)$

logo

Elliptische Kurven

- *elliptische Kurve*: E/K Gleichung in zwei Variablen x und y
- $y^2 = x^3 + ax + b$ mit $a, b \in K$
- $\triangle(E) := -16(4a^3 + 27b^2) \neq 0$
- Dazu gehört auch noch ein Punkt $\mathcal{O}$ "im Unendlichen"
- *j-Invariante* $j(E) := -1728(4a^3)/\triangle(E)$

Elliptische Kurven

- *elliptische Kurve*: E/K Gleichung in zwei Variablen x und y
- $y^2 = x^3 + ax + b$ mit $a, b \in K$
- $\triangle(E) := -16(4a^3 + 27b^2) \neq 0$
- Dazu gehört auch noch ein Punkt $\mathcal{O}$
  "im Unendlichen"
- *j-Invariante* $j(E) := -1728(4a^3)/\triangle(E)$

Elliptische Kurven

- *elliptische Kurve*: E/K Gleichung in zwei Variablen x und y
- $y^2 = x^3 + ax + b$ mit $a, b \in K$
- $\triangle(E) := -16(4a^3 + 27b^2) \neq 0$
- Dazu gehört auch noch ein Punkt $\mathcal{O}$
  "im Unendlichen"
- *j-Invariante* $j(E) := -1728(4a^3)/\triangle(E)$

Die Punktgruppe einer elliptischen Kurve

- $E(\tilde{K}) :=$
  $\{(x, y) \in \tilde{K} \times \tilde{K} | (x, y)$ erfüllen die Gleichung $E\} \cup \{\mathcal{O}\}$
- $E(\tilde{K})$ Gruppe bzgl. $+$ (tangent and chord), neutrales Element $\mathcal{O}$
- Es gilt: $\#E(\tilde{K}) < \infty$.
- $ord(P) := \min\{n \in \mathbb{N} \quad | \quad nP = \mathcal{O}\}$

logo

Die Punktgruppe einer elliptischen Kurve

- $E(\tilde{K}) :=$
  $\{(x, y) \in \tilde{K} \times \tilde{K} | (x, y)$ erfüllen die Gleichung $E\} \cup \{\mathcal{O}\}$
- $E(\tilde{K})$ Gruppe bzgl. $+$ (tangent and chord), neutrales Element $\mathcal{O}$
- Es gilt: $\#E(\tilde{K}) < \infty$.
- $ord(P) := \min\{n \in \mathbb{N} \quad | \quad nP = \mathcal{O}\}$

logo

Die Punktgruppe einer elliptischen Kurve

- $E(\tilde{K}) :=$
  $\{(x, y) \in \tilde{K} \times \tilde{K} | (x, y)$ erfüllen die Gleichung $E\} \cup \{\mathcal{O}\}$
- $E(\tilde{K})$ Gruppe bzgl. $+$ (tangent and chord), neutrales Element $\mathcal{O}$
- Es gilt: $\#E(\tilde{K}) < \infty$.
- $ord(P) := \min\{n \in \mathbb{N} \quad | \quad nP = \mathcal{O}\}$

logo

Die Punktgruppe einer elliptischen Kurve

- $E(\tilde{K}) :=$
  $\{(x, y) \in \tilde{K} \times \tilde{K} | (x, y)$ erfüllen die Gleichung $E\} \cup \{\mathcal{O}\}$
- $E(\tilde{K})$ Gruppe bzgl. $+$ (tangent and chord), neutrales Element $\mathcal{O}$
- Es gilt: $\#E(\tilde{K}) < \infty$.
- $ord(P) := \min\{n \in \mathbb{N} \quad | \quad nP = \mathcal{O}\}$

logo

Motivation

Übertragung des DLP von E_1/K nach E_2/K

- Isogenien sind Homomorphismen elliptischer Kurven: $\varphi : E_1 \to E_2$
- Sei $mP = Q$ ein DLP auf $E_1(\overline{K})$.
- Falls effizienter Algorithmus für DLP auf $E_2(\overline{K})$ existiert: Finde m' mit $m'\varphi(P) = \varphi(Q)$
- Dann können wir $m = m'$ annehmen.

Motivation

Übertragung des DLP von E_1/K nach E_2/K

- Isogenien sind Homomorphismen elliptischer Kurven: $\varphi : E_1 \to E_2$
- Sei $mP = Q$ ein DLP auf $E_1(\overline{K})$.
- Falls effizienter Algorithmus für DLP auf $E_2(\overline{K})$ existiert: Finde m' mit $m'\varphi(P) = \varphi(Q)$
- Dann können wir $m = m'$ annehmen.

Motivation

Übertragung des DLP von E_1/K nach E_2/K

- Isogenien sind Homomorphismen elliptischer Kurven: $\varphi : E_1 \to E_2$
- Sei $mP = Q$ ein DLP auf $E_1(\overline{K})$.
- Falls effizienter Algorithmus für DLP auf $E_2(\overline{K})$ existiert: Finde m' mit $m'\varphi(P) = \varphi(Q)$
- Dann können wir $m = m'$ annehmen.

Motivation

Übertragung des DLP von E_1/K nach E_2/K

- Isogenien sind Homomorphismen elliptischer Kurven: $\varphi : E_1 \to E_2$
- Sei $mP = Q$ ein DLP auf $E_1(\overline{K})$.
- Falls effizienter Algorithmus für DLP auf $E_2(\overline{K})$ existiert: Finde m' mit $m'\varphi(P) = \varphi(Q)$
- Dann können wir $m = m'$ annehmen.

Torsionsgruppen

- *m-te Torsionsgruppe* $E[m] := \{P \in E(\overline{K}) \quad | \quad mP = \mathcal{O}\}$
- $E/\mathbb{F}_p$ *supersingulär*: $E[p^r] = O \quad \forall r \in \mathbb{N}$, sonst *ordinär*.
- $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \forall m \in \mathbb{N}, p \nmid m$

Torsionsgruppen

- *m-te Torsionsgruppe* $E[m] := \{P \in E(\overline{K}) \quad | \quad mP = \mathcal{O}\}$
- $E/\mathbb{F}_p$ *supersingulär*: $E[p^r] = O \quad \forall r \in \mathbb{N}$, sonst *ordinär*.
- $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \forall m \in \mathbb{N}, p \nmid m$

Torsionsgruppen

- *m-te Torsionsgruppe* $E[m] := \{P \in E(\overline{K}) \quad | \quad mP = \mathcal{O}\}$
- $E/\mathbb{F}_p$ *supersingulär*: $E[p^r] = O \quad \forall r \in \mathbb{N}$, sonst *ordinär*.
- $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \forall m \in \mathbb{N}, p \nmid m$

Torsionsgruppen

- *m-te Torsionsgruppe* $E[m] := \{P \in E(\overline{K}) \quad | \quad mP = \mathcal{O}\}$
- $E/\mathbb{F}_p$ *supersingulär*: $E[p^r] = O \quad \forall r \in \mathbb{N}$, sonst *ordinär*.
- $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \forall m \in \mathbb{N}, p \nmid m$

Koordinatenabbildung

- $X : E(\overline{K}) \backslash \{\mathcal{O}\} \to \overline{K}, (x, y) \mapsto x$
- Y analog

Torsionsgruppen

- *m-te Torsionsgruppe* $E[m] := \{P \in E(\overline{K}) \quad | \quad mP = \mathcal{O}\}$
- $E/\mathbb{F}_p$ *supersingulär*: $E[p^r] = O \quad \forall r \in \mathbb{N}$, sonst *ordinär*.
- $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \forall m \in \mathbb{N}, p \nmid m$

Koordinatenabbildung

- $X : E(\overline{K})\backslash\{\mathcal{O}\} \to \overline{K}, (x, y) \mapsto x$
- Y analog

logo

Isogenien

- $\tilde{K}$-*Isogenie*: $\tilde{K}$-rationale Funktion $\varphi : E_1 \longrightarrow E_2$ mit $\varphi(\mathcal{O}) = \mathcal{O}$
- anwendbar als $\varphi : E_1(\overline{K}) \longrightarrow E_2(\overline{K})$, dann Gruppenhomomorphismus
- E_1 und E_2 heissen $\tilde{K}$-*isogen*, wenn eine $\tilde{K}$-Isogenie zwischen ihnen existiert
- $\varphi(x, y) = (\frac{\varphi_{x_1}(x)}{\varphi_{x_2}(x)}, \frac{\varphi_{y_1}(x,y)}{\varphi_{y_2}(x)})$
- $\deg(\varphi) := \deg(\varphi_{x_1})$
- Es gilt: $\deg(\varphi \circ \psi) = \deg(\varphi)\deg(\psi)$

Isogenien

- $\tilde{K}$-*Isogenie*: $\tilde{K}$-rationale Funktion $\varphi : E_1 \to E_2$ mit $\varphi(\mathcal{O}) = \mathcal{O}$
- anwendbar als $\varphi : E_1(\overline{K}) \to E_2(\overline{K})$, dann Gruppenhomomorphismus
- E_1 und E_2 heissen $\tilde{K}$-*isogen*, wenn eine $\tilde{K}$-Isogenie zwischen ihnen existiert
- $\varphi(x, y) = (\frac{\varphi_{x_1}(x)}{\varphi_{x_2}(x)}, \frac{\varphi_{y_1}(x,y)}{\varphi_{y_2}(x)})$
- $\deg(\varphi) := \deg(\varphi_{x_1})$
- Es gilt: $\deg(\varphi \circ \psi) = \deg(\varphi)\deg(\psi)$

Isogenien

- $\tilde{K}$-*Isogenie*: $\tilde{K}$-rationale Funktion $\varphi : E_1 \to E_2$ mit $\varphi(\mathcal{O}) = \mathcal{O}$
- anwendbar als $\varphi : E_1(\overline{K}) \to E_2(\overline{K})$, dann Gruppenhomomorphismus
- E_1 und E_2 heissen $\tilde{K}$-*isogen*, wenn eine $\tilde{K}$-Isogenie zwischen ihnen existiert
- $\varphi(x, y) = (\frac{\varphi_{x_1}(x)}{\varphi_{x_2}(x)}, \frac{\varphi_{y_1}(x,y)}{\varphi_{y_2}(x)})$
- $\deg(\varphi) := \deg(\varphi_{x_1})$
- Es gilt: $\deg(\varphi \circ \psi) = \deg(\varphi)\deg(\psi)$

Isogenien

- $\tilde{K}$-*Isogenie*: $\tilde{K}$-rationale Funktion $\varphi : E_1 \to E_2$ mit $\varphi(\mathcal{O}) = \mathcal{O}$
- anwendbar als $\varphi : E_1(\overline{K}) \to E_2(\overline{K})$, dann Gruppenhomomorphismus
- E_1 und E_2 heissen $\tilde{K}$-*isogen*, wenn eine $\tilde{K}$-Isogenie zwischen ihnen existiert
- $\varphi(x, y) = (\frac{\varphi_{x_1}(x)}{\varphi_{x_2}(x)}, \frac{\varphi_{y_1}(x,y)}{\varphi_{y_2}(x)})$
- $\deg(\varphi) := \deg(\varphi_{x_1})$
- Es gilt: $\deg(\varphi \circ \psi) = \deg(\varphi)\ \deg(\psi)$

Isogenien

- $\tilde{K}$-*Isogenie*: $\tilde{K}$-rationale Funktion $\varphi : E_1 \to E_2$ mit $\varphi(\mathcal{O}) = \mathcal{O}$
- anwendbar als $\varphi : E_1(\overline{K}) \to E_2(\overline{K})$, dann Gruppenhomomorphismus
- E_1 und E_2 heissen $\tilde{K}$-*isogen*, wenn eine $\tilde{K}$-Isogenie zwischen ihnen existiert
- $\varphi(x, y) = (\frac{\varphi_{x_1}(x)}{\varphi_{x_2}(x)}, \frac{\varphi_{y_1}(x,y)}{\varphi_{y_2}(x)})$
- $\deg(\varphi) := \deg(\varphi_{x_1})$
- Es gilt: $\deg(\varphi \circ \psi) = \deg(\varphi) \deg(\psi)$

Isogenien

- $\tilde{K}$-*Isogenie*: $\tilde{K}$-rationale Funktion $\varphi : E_1 \to E_2$ mit $\varphi(\mathcal{O}) = \mathcal{O}$
- anwendbar als $\varphi : E_1(\overline{K}) \to E_2(\overline{K})$, dann Gruppenhomomorphismus
- E_1 und E_2 heissen $\tilde{K}$-*isogen*, wenn eine $\tilde{K}$-Isogenie zwischen ihnen existiert
- $\varphi(x, y) = (\frac{\varphi_{x_1}(x)}{\varphi_{x_2}(x)}, \frac{\varphi_{y_1}(x,y)}{\varphi_{y_2}(x)})$
- $\deg(\varphi) := \deg(\varphi_{x_1})$
- Es gilt: $\deg(\varphi \circ \psi) = \deg(\varphi)\ \deg(\psi)$

Beispiel

Multiplikation-mit-m-Abbildung

- Für $m \in \mathbb{N}$ ist $[m] : E \longrightarrow E, P \mapsto mP$ eine Isogenie
- *Divisionspolynome* $\psi_{m,E} \in K[x]$:
  $\forall P \in E(\overline{K}) \backslash \{\mathcal{O}\} : \psi_{m,E}(X(P)) = 0 \quad \Leftrightarrow P \in E[m]$
- $[m]P = \left(\frac{\phi_m(X(P))}{\psi_{m,E}(X(P))^2}, \frac{\omega_m(X(P),Y(P))}{\psi_{m,E}(X(P))^3}\right)$
- Polstellen von $[m]$: alle $P \in E(\overline{K})$ mit $\psi_{m,E}(X(P)) = 0$
- setzen $[m]P = \mathcal{O}$ für alle P mit $\psi_{m,E}(X(P)) = 0$

logo

Beispiel

Multiplikation-mit-m-Abbildung

- Für $m \in \mathbb{N}$ ist $[m] : E \to E, P \mapsto mP$ eine Isogenie
- *Divisionspolynome* $\psi_{m,E} \in K[x]$:
  $\forall P \in E(\overline{K}) \backslash \{\mathcal{O}\} : \psi_{m,E}(X(P)) = 0 \quad \Leftrightarrow P \in E[m]$
- $[m]P = \left(\frac{\phi_m(X(P))}{\psi_{m,E}(X(P))^2}, \frac{\omega_m(X(P),Y(P))}{\psi_{m,E}(X(P))^3}\right)$
- Polstellen von $[m]$: alle $P \in E(\overline{K})$ mit $\psi_{m,E}(X(P)) = 0$
- setzen $[m]P = \mathcal{O}$ für alle P mit $\psi_{m,E}(X(P)) = 0$

logo

Beispiel

Multiplikation-mit-m-Abbildung

- Für $m \in \mathbb{N}$ ist $[m] : E \to E, P \mapsto mP$ eine Isogenie
- *Divisionspolynome* $\psi_{m,E} \in K[x]$:
  $\forall P \in E(\overline{K}) \backslash \{\mathcal{O}\} : \psi_{m,E}(X(P)) = 0 \quad \Leftrightarrow P \in E[m]$
- $[m]P = (\frac{\phi_m(X(P))}{\psi_{m,E}(X(P))^2}, \frac{\omega_m(X(P),Y(P))}{\psi_{m,E}(X(P))^3})$
- Polstellen von $[m]$: alle $P \in E(\overline{K})$ mit $\psi_{m,E}(X(P)) = 0$
- setzen $[m]P = \mathcal{O}$ für alle P mit $\psi_{m,E}(X(P)) = 0$

logo

Beispiel

Multiplikation-mit-m-Abbildung

- Für $m \in \mathbb{N}$ ist $[m] : E \to E, P \mapsto mP$ eine Isogenie
- *Divisionspolynome* $\psi_{m,E} \in K[x]$:
  $\forall P \in E(\overline{K}) \backslash \{\mathcal{O}\} : \psi_{m,E}(X(P)) = 0 \quad \Leftrightarrow P \in E[m]$
- $[m]P = (\frac{\phi_m(X(P))}{\psi_{m,E}(X(P))^2}, \frac{\omega_m(X(P),Y(P))}{\psi_{m,E}(X(P))^3})$
- Polstellen von $[m]$: alle $P \in E(\overline{K})$ mit $\psi_{m,E}(X(P)) = 0$
- setzen $[m]P = \mathcal{O}$ für alle P mit $\psi_{m,E}(X(P)) = 0$

logo

Beispiel

Multiplikation-mit-m-Abbildung

- Für $m \in \mathbb{N}$ ist $[m] : E \to E, P \mapsto mP$ eine Isogenie
- *Divisionspolynome* $\psi_{m,E} \in K[x]$:
  $\forall P \in E(\overline{K}) \backslash \{\mathcal{O}\} : \psi_{m,E}(X(P)) = 0 \quad \Leftrightarrow P \in E[m]$
- $[m]P = (\frac{\phi_m(X(P))}{\psi_{m,E}(X(P))^2}, \frac{\omega_m(X(P),Y(P))}{\psi_{m,E}(X(P))^3})$
- Polstellen von $[m]$: alle $P \in E(\overline{K})$ mit $\psi_{m,E}(X(P)) = 0$
- setzen $[m]P = \mathcal{O}$ für alle P mit $\psi_{m,E}(X(P)) = 0$

logo

Isomorphismen

- *Isomorphismus*: Isogenie $\varphi : E_1 \longrightarrow E_2$ vom Grad 1
- $j(E_1) = j(E_2) \Leftrightarrow$ Es existiert ein $\overline{K}$-Isomorphismus $\varphi : E_1 \longrightarrow E_2$
- $E_1/K : y^2 = x^3 + ax + b, E_2/K : y^2 = x^3 + Ax + B$ mit $j(E_1) = j(E_2)$
- $u := \sqrt[4]{\frac{a}{A}} = \sqrt[6]{\frac{b}{B}}$
- Dann ist $\varphi : E_1 \longrightarrow E_2, (x, y) \mapsto (x/u^2, y/u^3)$ ein Isomorphismus
- Gruppenisomorphismus für Punktgruppen über Erweiterungskörpern von $K(u)$

logo

Isomorphismen

- *Isomorphismus*: Isogenie $\varphi : E_1 \to E_2$ vom Grad 1
- $j(E_1) = j(E_2) \Leftrightarrow$ Es existiert ein $\overline{K}$-Isomorphismus $\varphi : E_1 \to E_2$
- $E_1/K : y^2 = x^3 + ax + b, E_2/K : y^2 = x^3 + Ax + B$ mit $j(E_1) = j(E_2)$
- $u := \sqrt[4]{\frac{a}{A}} = \sqrt[6]{\frac{b}{B}}$
- Dann ist $\varphi : E_1 \to E_2, (x, y) \mapsto (x/u^2, y/u^3)$ ein Isomorphismus
- Gruppenisomorphismus für Punktgruppen über Erweiterungskörpern von $K(u)$

Isomorphismen

- *Isomorphismus*: Isogenie $\varphi : E_1 \to E_2$ vom Grad 1
- $j(E_1) = j(E_2) \Leftrightarrow$ Es existiert ein $\overline{K}$-Isomorphismus $\varphi : E_1 \to E_2$
- $E_1/K : y^2 = x^3 + ax + b, E_2/K : y^2 = x^3 + Ax + B$ mit $j(E_1) = j(E_2)$
- $u := \sqrt[4]{\frac{a}{A}} = \sqrt[6]{\frac{b}{B}}$
- Dann ist $\varphi : E_1 \to E_2, (x, y) \mapsto (x/u^2, y/u^3)$ ein Isomorphismus
- Gruppenisomorphismus für Punktgruppen über Erweiterungskörpern von $K(u)$

logo

Isomorphismen

- *Isomorphismus*: Isogenie $\varphi : E_1 \to E_2$ vom Grad 1
- $j(E_1) = j(E_2) \Leftrightarrow$ Es existiert ein $\overline{K}$-Isomorphismus $\varphi : E_1 \to E_2$
- $E_1/K : y^2 = x^3 + ax + b, E_2/K : y^2 = x^3 + Ax + B$ mit $j(E_1) = j(E_2)$
- $u := \sqrt[4]{\frac{a}{A}} = \sqrt[6]{\frac{b}{B}}$
- Dann ist $\varphi : E_1 \to E_2, (x, y) \mapsto (x/u^2, y/u^3)$ ein Isomorphismus
- Gruppenisomorphismus für Punktgruppen über Erweiterungskörpern von $K(u)$

Isomorphismen

- *Isomorphismus*: Isogenie $\varphi : E_1 \to E_2$ vom Grad 1
- $j(E_1) = j(E_2) \Leftrightarrow$ Es existiert ein $\overline{K}$-Isomorphismus $\varphi : E_1 \to E_2$
- $E_1/K : y^2 = x^3 + ax + b, E_2/K : y^2 = x^3 + Ax + B$ mit $j(E_1) = j(E_2)$
- $u := \sqrt[4]{\frac{a}{A}} = \sqrt[6]{\frac{b}{B}}$
- Dann ist $\varphi : E_1 \to E_2, (x, y) \mapsto (x/u^2, y/u^3)$ ein Isomorphismus
- Gruppenisomorphismus für Punktgruppen über Erweiterungskörpern von $K(u)$

Isomorphismen

- *Isomorphismus*: Isogenie $\varphi : E_1 \to E_2$ vom Grad 1
- $j(E_1) = j(E_2) \Leftrightarrow$ Es existiert ein $\overline{K}$-Isomorphismus $\varphi : E_1 \to E_2$
- $E_1/K : y^2 = x^3 + ax + b, E_2/K : y^2 = x^3 + Ax + B$ mit $j(E_1) = j(E_2)$
- $u := \sqrt[4]{\frac{a}{A}} = \sqrt[6]{\frac{b}{B}}$
- Dann ist $\varphi : E_1 \to E_2, (x, y) \mapsto (x/u^2, y/u^3)$ ein Isomorphismus
- Gruppenisomorphismus für Punktgruppen über Erweiterungskörpern von $K(u)$

Zielsetzung

Satz von Tate

- E_1/K und E_2/K $\tilde{K}$-isogen
  $\Leftrightarrow \#E_1(\tilde{K}) = \#E_2(\tilde{K})$

Zielsetzung

Satz von Tate

- E_1/K und E_2/K $\tilde{K}$-isogen
  $\Leftrightarrow \#E_1(\tilde{K}) = \#E_2(\tilde{K})$

Ziel

- Algorithmus, der zu zwei K-isogenen Kurven eine passende Isogenie liefert

Outline

- *Galois-Gruppe* $G_{\overline{K}/K}$: Menge aller Automorphismen $\tau : \overline{K} \to \overline{K}$ mit $\tau_{|K} = id_K$, Gruppe bzgl. $\circ$ als Verknüpfung
- Untergruppe $H \subset E(\overline{K})$ heisst *galois-invariant*, wenn $\forall P \in H, \forall \tau \in G_{\overline{K}/K} : (\tau(X(P)), \tau(Y(P))) \in H$.
- Satz: E/K elliptische Kurve, $H \subset E(\tilde{K})$ galois-invariante Untergruppe, dann gibt es K-Isogenie $\varphi : E \to E/H$ mit $\mathrm{Kern}(\varphi) = H$.
- E/H ist hierbei eine passende über K definierte Kurve.

- *Galois-Gruppe* $G_{\overline{K}/K}$: Menge aller Automorphismen $\tau : \overline{K} \to \overline{K}$ mit $\tau_{|K} = id_K$, Gruppe bzgl. $\circ$ als Verknüpfung
- Untergruppe $H \subset E(\overline{K})$ heisst *galois-invariant*, wenn $\forall P \in H, \forall \tau \in G_{\overline{K}/K} : (\tau(X(P)), \tau(Y(P))) \in H$.
- Satz: E/K elliptische Kurve, $H \subset E(\tilde{K})$ galois-invariante Untergruppe, dann gibt es K-Isogenie $\varphi : E \to E/H$ mit $\mathrm{Kern}(\varphi) = H$.
- E/H ist hierbei eine passende über K definierte Kurve.

- *Galois-Gruppe* $G_{\overline{K}/K}$: Menge aller Automorphismen $\tau : \overline{K} \to \overline{K}$ mit $\tau_{|K} = id_K$, Gruppe bzgl. $\circ$ als Verknüpfung
- Untergruppe $H \subset E(\overline{K})$ heisst *galois-invariant*, wenn $\forall P \in H, \forall \tau \in G_{\overline{K}/K} : (\tau(X(P)), \tau(Y(P))) \in H$.
- Satz: E/K elliptische Kurve, $H \subset E(\tilde{K})$ galois-invariante Untergruppe, dann gibt es K-Isogenie $\varphi : E \to E/H$ mit $\text{Kern}(\varphi) = H$.
- E/H ist hierbei eine passende über K definierte Kurve.

- *Galois-Gruppe* $G_{\overline{K}/K}$: Menge aller Automorphismen $\tau : \overline{K} \to \overline{K}$ mit $\tau_{|K} = id_K$, Gruppe bzgl. $\circ$ als Verknüpfung
- Untergruppe $H \subset E(\overline{K})$ heisst *galois-invariant*, wenn $\forall P \in H, \forall \tau \in G_{\overline{K}/K} : (\tau(X(P)), \tau(Y(P))) \in H$.
- Satz: E/K elliptische Kurve, $H \subset E(\tilde{K})$ galois-invariante Untergruppe, dann gibt es K-Isogenie $\varphi : E \to E/H$ mit $\mathrm{Kern}(\varphi) = H$.
- E/H ist hierbei eine passende über K definierte Kurve.

Berechnung der Velu-Isogenie

- Für alle $P \in E(\overline{K})\backslash\{\mathcal{O}\}$ ist $\varphi(P) := (\varphi_x(P), \varphi_y(P))$ mit

$$\varphi_x(P) = X(P) + \Big(\sum_{Q \in H\backslash\{\mathcal{O}\}} X(P+Q) - X(Q)\Big)$$

$$\varphi_y(P) = Y(P) + \Big(\sum_{Q \in H\backslash\{\mathcal{O}\}} Y(P+Q) - Y(Q)\Big)$$

und

$$\varphi(\mathcal{O}) = \mathcal{O}.$$

- man kann auch konkrete rationale Funktionen für φ_x und φ_y angeben (Additionsformeln)

Berechnung der Velu-Isogenie

- Für alle $P \in E(\overline{K})\backslash\{\mathcal{O}\}$ ist $\varphi(P) := (\varphi_x(P), \varphi_y(P))$ mit

$$\varphi_x(P) = X(P) + \Big(\sum_{Q \in H\backslash\{\mathcal{O}\}} X(P+Q) - X(Q) \Big)$$

$$\varphi_y(P) = Y(P) + \Big(\sum_{Q \in H\backslash\{\mathcal{O}\}} Y(P+Q) - Y(Q) \Big)$$

  und

$$\varphi(\mathcal{O}) = \mathcal{O}.$$

- man kann auch konkrete rationale Funktionen für φ_x und φ_y angeben (Additionsformeln)

Zielkurve der Velu-Isogenie

- E/H wird aus den Koeffizienten von E und den Koordinaten von H berechnet
- betrachte allgemeinen Punkt $P \in E(\overline{K})$, setze ihn in die Formeln für φ_x und φ_y ein, berechne, welche Relation φ_x und φ_y erfüllen müssen

Zielkurve der Velu-Isogenie

- E/H wird aus den Koeffizienten von E und den Koordinaten von H berechnet
- betrachte allgemeinen Punkt $P \in E(\overline{K})$, setze ihn in die Formeln für φ_x und φ_y ein, berechne, welche Relation φ_x und φ_y erfüllen müssen

Outline

logo

- SEA(Schoof-Elkies-Atkin)-Algorithmus berechnet $\#E(\tilde{K})$ mittels Isogenien

- SEA(Schoof-Elkies-Atkin)-Algorithmus berechnet $\#E(\tilde{K})$ mittels Isogenien

Der Frobenius-Endomorphismus

- *Frobenius-Endomorphismus* von $E/\mathbb{F}_p$: $\pi : E \to E, (x, y) \mapsto (x^p, y^p)$
- $y_q^2 - x_q^3 + ax_q + b = 0 \Leftrightarrow$
- $(y_q^2)^p - (x_q^3)^p - (ax_q)^p - b^p = 0 \Leftrightarrow$
- $(y_q^p)^2 - (x_q^p)^3 - ax_q^p - b = 0$

- SEA(Schoof-Elkies-Atkin)-Algorithmus berechnet $\#E(\tilde{K})$ mittels Isogenien

Der Frobenius-Endomorphismus

- *Frobenius-Endomorphismus* von $E/\mathbb{F}_p$: $\pi : E \to E, (x, y) \mapsto (x^p, y^p)$
- $y_q^2 - x_q^3 + ax_q + b = 0 \Leftrightarrow$
- $(y_q^2)^p - (x_q^3)^p - (ax_q)^p - b^p = 0 \Leftrightarrow$
- $(y_q^p)^2 - (x_q^p)^3 - ax_q^p - b = 0$

- SEA(Schoof-Elkies-Atkin)-Algorithmus berechnet $\#E(\tilde{K})$ mittels Isogenien

Der Frobenius-Endomorphismus

- *Frobenius-Endomorphismus* von $E/\mathbb{F}_p$: $\pi : E \to E, (x, y) \mapsto (x^p, y^p)$
- $y_q^2 - x_q^3 + ax_q + b = 0 \Leftrightarrow$
- $(y_q^2)^p - (x_q^3)^p - (ax_q)^p - b^p = 0 \Leftrightarrow$
- $(y_q^p)^2 - (x_q^p)^3 - ax_q^p - b = 0$

- SEA(Schoof-Elkies-Atkin)-Algorithmus berechnet $\#E(\tilde{K})$ mittels Isogenien

Der Frobenius-Endomorphismus

- *Frobenius-Endomorphismus* von $E/\mathbb{F}_p$: $\pi : E \to E, (x, y) \mapsto (x^p, y^p)$
- $y_q^2 - x_q^3 + ax_q + b = 0 \Leftrightarrow$
- $(y_q^2)^p - (x_q^3)^p - (ax_q)^p - b^p = 0 \Leftrightarrow$
- $(y_q^p)^2 - (x_q^p)^3 - ax_q^p - b = 0$

Eigenschaften des Frobenius-Endomorphismus

- *Spur des Frobenius-Endomorphismus* $t := p + 1 - \#E(\mathbb{F}_p)$
- *charakteristische Gleichung von* π: $\pi^2 - t\pi + p = 0$
- für alle $P \in E(\overline{\mathbb{F}_p})$: $\pi(P)^2 - t\pi(P) + pP = \mathcal{O}$
- $P \in E(\mathbb{F}_p) \Leftrightarrow \pi(P) = P$

Eigenschaften des Frobenius-Endomorphismus

- *Spur des Frobenius-Endomorphismus* $t := p + 1 - \#E(\mathbb{F}_p)$
- *charakteristische Gleichung von* π: $\pi^2 - t\pi + p = 0$
- für alle $P \in E(\overline{\mathbb{F}_p})$: $\pi(P)^2 - t\pi(P) + pP = \mathcal{O}$
- $P \in E(\mathbb{F}_p) \Leftrightarrow \pi(P) = P$

Eigenschaften des Frobenius-Endomorphismus

- *Spur des Frobenius-Endomorphismus* $t := p + 1 - \#E(\mathbb{F}_p)$
- *charakteristische Gleichung von* π: $\pi^2 - t\pi + p = 0$
- für alle $P \in E(\overline{\mathbb{F}_p})$: $\pi(P)^2 - t\pi(P) + pP = \mathcal{O}$
- $P \in E(\mathbb{F}_p) \Leftrightarrow \pi(P) = P$

Eigenschaften des Frobenius-Endomorphismus

- *Spur des Frobenius-Endomorphismus* $t := p + 1 - \#E(\mathbb{F}_p)$
- *charakteristische Gleichung von* π: $\pi^2 - t\pi + p = 0$
- für alle $P \in E(\overline{\mathbb{F}_p})$: $\pi(P)^2 - t\pi(P) + pP = \mathcal{O}$
- $P \in E(\mathbb{F}_p) \Leftrightarrow \pi(P) = P$

Eigenschaften des Frobenius-Endomorphismus

- *Spur des Frobenius-Endomorphismus* $t := p + 1 - \#E(\mathbb{F}_p)$
- *charakteristische Gleichung von* π: $\pi^2 - t\pi + p = 0$
- für alle $P \in E(\overline{\mathbb{F}_p})$: $\pi(P)^2 - t\pi(P) + pP = \mathcal{O}$
- $P \in E(\mathbb{F}_p) \Leftrightarrow \pi(P) = P$

- *Endomorphismenring von* E: die Menge End(E) aller Isogenien $\varphi : E \to E$ zusammen mit Komposition und punktweiser Addition

zahlentheoretische Betrachtung des Endomorphismenrings

- Sei F eine Körpererweiterung von $\mathbb{Q}$ vom Grad n.
- *Ordnung von F*: jeder Teilring $1 \subset M \subset F$, welcher ein freier $\mathbb{Z}$-Modul vom Rang n ist
- *Maximalordnung von F*: Der bzgl. Inklusion grösster dieser Moduln $\mathcal{O}_F$
- Der Endomorphismenring einer ordinären elliptischen Kurve über einem endlichen Körper ist eine Ordnung in einem imaginärquadratischen Zahlkörper
- Wir betrachten ab jetzt nur noch ordinäre elliptische Kurven E, für die $\mathrm{End}(E) = \mathbb{Z}[\pi]$ die Maximalordnung ist.

zahlentheoretische Betrachtung des Endomorphismenrings

- Sei F eine Körpererweiterung von $\mathbb{Q}$ vom Grad n.
- *Ordnung von F*: jeder Teilring $1 \subset M \subset F$, welcher ein freier $\mathbb{Z}$-Modul vom Rang n ist
- *Maximalordnung von F*: Der bzgl. Inklusion grösster dieser Moduln $\mathcal{O}_F$
- Der Endomorphismenring einer ordinären elliptischen Kurve über einem endlichen Körper ist eine Ordnung in einem imaginärquadratischen Zahlkörper
- Wir betrachten ab jetzt nur noch ordinäre elliptische Kurven E, für die $\mathrm{End}(E) = \mathbb{Z}[\pi]$ die Maximalordnung ist.

zahlentheoretische Betrachtung des Endomorphismenrings

- Sei F eine Körpererweiterung von $\mathbb{Q}$ vom Grad n.
- *Ordnung von F*: jeder Teilring $1 \subset M \subset F$, welcher ein freier $\mathbb{Z}$-Modul vom Rang n ist
- *Maximalordnung von F*: Der bzgl. Inklusion grösster dieser Moduln $\mathcal{O}_F$
- Der Endomorphismenring einer ordinären elliptischen Kurve über einem endlichen Körper ist eine Ordnung in einem imaginärquadratischen Zahlkörper
- Wir betrachten ab jetzt nur noch ordinäre elliptische Kurven E, für die $\mathrm{End}(E) = \mathbb{Z}[\pi]$ die Maximalordnung ist.

zahlentheoretische Betrachtung des Endomorphismenrings

- Sei F eine Körpererweiterung von $\mathbb{Q}$ vom Grad n.
- *Ordnung von F*: jeder Teilring $1 \subset M \subset F$, welcher ein freier $\mathbb{Z}$-Modul vom Rang n ist
- *Maximalordnung von F*: Der bzgl. Inklusion grösster dieser Moduln $\mathcal{O}_F$
- Der Endomorphismenring einer ordinären elliptischen Kurve über einem endlichen Körper ist eine Ordnung in einem imaginärquadratischen Zahlkörper
- Wir betrachten ab jetzt nur noch ordinäre elliptische Kurven E, für die $\mathrm{End}(E) = \mathbb{Z}[\pi]$ die Maximalordnung ist.

zahlentheoretische Betrachtung des Endomorphismenrings

- Sei F eine Körpererweiterung von $\mathbb{Q}$ vom Grad n.
- *Ordnung von F*: jeder Teilring $1 \subset M \subset F$, welcher ein freier $\mathbb{Z}$-Modul vom Rang n ist
- *Maximalordnung von F*: Der bzgl. Inklusion grösster dieser Moduln $\mathcal{O}_F$
- Der Endomorphismenring einer ordinären elliptischen Kurve über einem endlichen Körper ist eine Ordnung in einem imaginärquadratischen Zahlkörper
- Wir betrachten ab jetzt nur noch ordinäre elliptische Kurven E, für die $\mathrm{End}(E) = \mathbb{Z}[\pi]$ die Maximalordnung ist.

modulare Polynome und Elkies-Primzahlen

- *modulares Polynom vom Grad* ℓ: $\Phi_\ell(t_1, t_2) \in K[x, y]$ mit E_1/K und E_2/K K-isogen $\Leftrightarrow \Phi_\ell(j(E_1), j(E_2)) = 0$ (ℓ ungerade Primzahl)
- E/K elliptische Kurve, π Frobenius, f charakteristische Gleichung von π. Eine ungerade Primzahl ℓ heisst *Elkies-Primzahl*, wenn $f \equiv (x - \lambda)(x - \mu) \bmod \ell$ mit $\lambda \neq \mu$
- $E[l]$ 2-dim $\mathbb{F}_\ell$-Vektorraum, $\pi_{|E[\ell]}$ Vektorraum-Endomorphismus. Wenn f mod ℓ zerfällt, dann gibt es eine Basis P, Q von $E[\ell]$ mit $\lambda P = \pi(P)$ und $\mu Q = \pi(Q)$

logo

modulare Polynome und Elkies-Primzahlen

- *modulares Polynom vom Grad* ℓ: $\Phi_\ell(t_1, t_2) \in K[x, y]$ mit E_1/K und E_2/K K-isogen $\Leftrightarrow \Phi_\ell(j(E_1), j(E_2)) = 0$ (ℓ ungerade Primzahl)
- E/K elliptische Kurve, π Frobenius, f charakteristische Gleichung von π. Eine ungerade Primzahl ℓ heisst *Elkies-Primzahl*, wenn $f \equiv (x - \lambda)(x - \mu) \bmod \ell$ mit $\lambda \neq \mu$
- $E[l]$ 2-dim $\mathbb{F}_\ell$-Vektorraum, $\pi_{|E[\ell]}$ Vektorraum-Endomorphismus. Wenn f mod ℓ zerfällt, dann gibt es eine Basis P, Q von $E[\ell]$ mit $\lambda P = \pi(P)$ und $\mu Q = \pi(Q)$

modulare Polynome und Elkies-Primzahlen

- *modulares Polynom vom Grad* ℓ: $\Phi_\ell(t_1, t_2) \in K[x, y]$ mit E_1/K und E_2/K K-isogen $\Leftrightarrow \Phi_\ell(j(E_1), j(E_2)) = 0$ (ℓ ungerade Primzahl)
- E/K elliptische Kurve, π Frobenius, f charakteristische Gleichung von π. Eine ungerade Primzahl ℓ heisst *Elkies-Primzahl*, wenn $f \equiv (x - \lambda)(x - \mu) \bmod \ell$ mit $\lambda \neq \mu$
- $E[l]$ 2-dim $\mathbb{F}_\ell$-Vektorraum, $\pi_{|E[\ell]}$ Vektorraum-Endomorphismus. Wenn f mod ℓ zerfällt, dann gibt es eine Basis P, Q von $E[\ell]$ mit $\lambda P = \pi(P)$ und $\mu Q = \pi(Q)$

Ein wichtiger Satz von Schoof

Sei $E/\mathbb{F}_p$ eine ordinäre elliptische Kurve (mit $j(E) \neq 0, 1728$. Dann gilt:
Das Polynom $\Phi_\ell(j(E), T)$ hat eine Nullstelle $j' \in \mathbb{F}_p \Leftrightarrow$ Es gibt eine $\mathbb{F}_p$-Isogenie $\varphi : E \to E/C$ vom Grad ℓ mit $j(E/C) = j'$, sodass Kern(φ) ein eindimensionaler Eigenraum von π in $E[\ell]$ ist.

Ein wichtiger Satz von Schoof

Sei $E/\mathbb{F}_p$ eine ordinäre elliptische Kurve (mit $j(E) \neq 0, 1728$. Dann gilt:
Das Polynom $\Phi_\ell(j(E), T)$ hat eine Nullstelle $j' \in \mathbb{F}_p \Leftrightarrow$ Es gibt eine $\mathbb{F}_p$-Isogenie $\varphi : E \to E/C$ vom Grad ℓ mit $j(E/C) = j'$, sodass Kern(φ) ein eindimensionaler Eigenraum von π in $E[\ell]$ ist.

Anwendung im Algorithmus zum Finden einer Isogenie

- E/F_p ordinäre elliptische Kurve, ℓ Elkies-Primzahl $\Rightarrow$ $\Phi_\ell(j(E), T)$ hat Nullstelle j' (es gibt entsprechenden Eigenraum C in $E[\ell]$). Im SEA-Algorithmus wird aus j' und Koeffizienten von E ein Faktor f des Divisionspolynoms ψ_ℓ berechnet, dessen Nullstellen Kern einer $\mathbb{F}_p$-Isogenie φ sind. Anschliessend φ mit Velus Formel berechnen.

erste Skizze des Algorithmus(1)

- INPUT:$E_1/\mathbb{F}_p$, $E_2/\mathbb{F}_p$ ordinäre elliptische Kurven mit $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$ und $\mathrm{End}(E_1) = \mathbb{Z}[\pi]$ ist Maximalordnung
- OUTPUT: Eine $\mathbb{F}_p$-Isogenie $\varphi : E_1 \to E_2$
- INITIALISIERUNG:
  L:= Elkies-Primzahlen von E_1 unter bestimmter Grenze
  E:= E_1
  j:= j(E_2)
- WHILE not j(E) = j DO
  Wähle l zufällig aus L
  Berechne mit Schoof & Velu eine Isogenie vom Grad l
  E:= Zielkurve der Isogenie
  END WHILE

erste Skizze des Algorithmus(1)

- INPUT:$E_1/\mathbb{F}_p$, $E_2/\mathbb{F}_p$ ordinäre elliptische Kurven mit $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$ und $\mathrm{End}(E_1) = \mathbb{Z}[\pi]$ ist Maximalordnung
- OUTPUT: Eine $\mathbb{F}_p$-Isogenie $\varphi : E_1 \to E_2$
- INITIALISIERUNG:
  L:= Elkies-Primzahlen von E_1 unter bestimmter Grenze
  E:= E_1
  j:= j(E_2)
- WHILE not j(E) = j DO
  Wähle l zufällig aus L
  Berechne mit Schoof & Velu eine Isogenie vom Grad l
  E:= Zielkurve der Isogenie
  END WHILE

erste Skizze des Algorithmus(1)

- INPUT:$E_1/\mathbb{F}_p$, $E_2/\mathbb{F}_p$ ordinäre elliptische Kurven mit $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$ und $\mathrm{End}(E_1) = \mathbb{Z}[\pi]$ ist Maximalordnung
- OUTPUT: Eine $\mathbb{F}_p$-Isogenie $\varphi : E_1 \to E_2$
- INITIALISIERUNG:
  L:= Elkies-Primzahlen von E_1 unter bestimmter Grenze
  E:= E_1
  j:= j(E_2)
- WHILE not j(E) = j DO
  Wähle l zufällig aus L
  Berechne mit Schoof & Velu eine Isogenie vom Grad l
  E:= Zielkurve der Isogenie
  END WHILE

erste Skizze des Algorithmus(1)

- INPUT:$E_1/\mathbb{F}_p$, $E_2/\mathbb{F}_p$ ordinäre elliptische Kurven mit $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$ und $\mathrm{End}(E_1) = \mathbb{Z}[\pi]$ ist Maximalordnung
- OUTPUT: Eine $\mathbb{F}_p$-Isogenie $\varphi : E_1 \to E_2$
- INITIALISIERUNG:
  L:= Elkies-Primzahlen von E_1 unter bestimmter Grenze
  E:= E_1
  j:= j(E_2)
- WHILE not j(E) = j DO
  Wähle l zufällig aus L
  Berechne mit Schoof & Velu eine Isogenie vom Grad l
  E:= Zielkurve der Isogenie
  END WHILE

erste Skizze des Algorithmus(2)

- Iso:= Komposition aller so erhaltenen Isogenien
- IF E = E_2 THEN
  return Iso
- ELSE
  return Komposition von Iso und einem Isomorphismus von E nach E_2

erste Skizze des Algorithmus(2)

- Iso:= Komposition aller so erhaltenen Isogenien
- IF E = E_2 THEN
  return Iso
- ELSE
  return Komposition von Iso und einem Isomorphismus von E nach E_2

erste Skizze des Algorithmus(2)

- Iso:= Komposition aller so erhaltenen Isogenien
- IF E = E_2 THEN
  return Iso
- ELSE
  return Komposition von Iso und einem Isomorphismus von E nach E_2

Problemfälle

- Φ_ℓ modulares Polynom zu einer Primzahl ℓ, j' eine Nullstelle von $\Phi_\ell(j(E), T)$
- Φ_x partielle Ableitung von Φ_ℓ nach x
- Wenn $\Phi_x(j(E), j') = 0$, dann kann die entsprechende Isogenie vom Grad ℓ mit dem Algorithmus von Schoof nicht berechnet werden
- Dann anderes ℓ wählen

Problemfälle

- Φ_ℓ modulares Polynom zu einer Primzahl ℓ, j' eine Nullstelle von $\Phi_\ell(j(E), T)$
- Φ_x partielle Ableitung von Φ_ℓ nach x
- Wenn $\Phi_x(j(E), j') = 0$, dann kann die entsprechende Isogenie vom Grad ℓ mit dem Algorithmus von Schoof nicht berechnet werden
- Dann anderes ℓ wählen

Problemfälle

- Φ_ℓ modulares Polynom zu einer Primzahl ℓ, j' eine Nullstelle von $\Phi_\ell(j(E), T)$
- Φ_x partielle Ableitung von Φ_ℓ nach x
- Wenn $\Phi_x(j(E), j') = 0$, dann kann die entsprechende Isogenie vom Grad ℓ mit dem Algorithmus von Schoof nicht berechnet werden
- Dann anderes ℓ wählen

Problemfälle

- Φ_ℓ modulares Polynom zu einer Primzahl ℓ, j' eine Nullstelle von $\Phi_\ell(j(E), T)$
- Φ_x partielle Ableitung von Φ_ℓ nach x
- Wenn $\Phi_x(j(E), j') = 0$, dann kann die entsprechende Isogenie vom Grad ℓ mit dem Algorithmus von Schoof nicht berechnet werden
- Dann anderes ℓ wählen

Outline

logo

Voraussetzungen für diesen Abschnitt

E_1 und E_2 K-isogene ordinäre elliptische Kurven mit $\mathrm{End}(E_1) = \mathbb{Z}[\pi]$ die Maximalordnung $\mathcal{O}$, $F := \mathbb{Q}(\pi)$

gebrochene Ideale und die Klassengruppe

- $\varnothing \neq \mathfrak{a} \subseteq F$ heisst *gebrochenes Ideal* von $\mathcal{O}$, wenn es ein $\xi \in \mathcal{O}\backslash\{0\}$ und ein Ideal $\{0\} \neq \mathfrak{b}$ in $\mathcal{O}$ gibt mit $\mathfrak{b} = \xi \cdot \mathfrak{a}$.
  $I_F :=$ Menge der gebrochenen Ideale von $\mathcal{O}$.
- gebrochenes Ideal von $\mathcal{O}$ ist freier $\mathbb{Z}$- Modul vom Rang n.
- Die *Norm* eines solchen Ideals $\mathfrak{b}$: Absolutbetrag der Determinante einer Transformationsmatrix einer $\mathbb{Z}$-Basis von $\mathcal{O}$ zu einer $\mathbb{Z}$-Basis von $\mathfrak{b}$.
- gebrochenes Ideal $\mathfrak{a}$ von $\mathcal{O}$ heisst *gebrochenes Hauptideal* von $\mathcal{O}$, wenn es ein $c \in \mathbb{F}\backslash\{0\}$ gibt mit $\mathfrak{a} = c \cdot F$.
  $H_F :=$ Menge der gebrochenen Hauptideale von $\mathcal{O}$
- *Klassengruppe* von $\mathcal{O}$: $\mathcal{CL}(\mathcal{O}) := I_F/H_F$.

logo

gebrochene Ideale und die Klassengruppe

- $\varnothing \neq \mathfrak{a} \subseteq F$ heisst *gebrochenes Ideal* von $\mathcal{O}$, wenn es ein $\xi \in \mathcal{O} \backslash \{0\}$ und ein Ideal $\{0\} \neq \mathfrak{b}$ in $\mathcal{O}$ gibt mit $\mathfrak{b} = \xi \cdot \mathfrak{a}$.
  $I_F :=$ Menge der gebrochenen Ideale von $\mathcal{O}$.
- gebrochenes Ideal von $\mathcal{O}$ ist freier $\mathbb{Z}$- Modul vom Rang n.
- Die *Norm* eines solchen Ideals $\mathfrak{b}$: Absolutbetrag der Determinante einer Transformationsmatrix einer $\mathbb{Z}$-Basis von $\mathcal{O}$ zu einer $\mathbb{Z}$-Basis von $\mathfrak{b}$.
- gebrochenes Ideal $\mathfrak{a}$ von $\mathcal{O}$ heisst *gebrochenes Hauptideal* von $\mathcal{O}$, wenn es ein $c \in \mathbb{F} \backslash \{0\}$ gibt mit $\mathfrak{a} = c \cdot F$.
  $H_F :=$ Menge der gebrochenen Hauptideale von $\mathcal{O}$
- *Klassengruppe* von $\mathcal{O}$: $\mathcal{CL}(\mathcal{O}) := I_F / H_F$.

logo

gebrochene Ideale und die Klassengruppe

- $\varnothing \neq \mathfrak{a} \subseteq F$ heisst *gebrochenes Ideal* von $\mathcal{O}$, wenn es ein $\xi \in \mathcal{O} \backslash \{0\}$ und ein Ideal $\{0\} \neq \mathfrak{b}$ in $\mathcal{O}$ gibt mit $\mathfrak{b} = \xi \cdot \mathfrak{a}$.
  $I_F :=$ Menge der gebrochenen Ideale von $\mathcal{O}$.
- gebrochenes Ideal von $\mathcal{O}$ ist freier $\mathbb{Z}$- Modul vom Rang n.
- Die *Norm* eines solchen Ideals $\mathfrak{b}$: Absolutbetrag der Determinante einer Transformationsmatrix einer $\mathbb{Z}$-Basis von $\mathcal{O}$ zu einer $\mathbb{Z}$-Basis von $\mathfrak{b}$.
- gebrochenes Ideal $\mathfrak{a}$ von $\mathcal{O}$ heisst *gebrochenes Hauptideal* von $\mathcal{O}$, wenn es ein $c \in \mathbb{F} \backslash \{0\}$ gibt mit $\mathfrak{a} = c \cdot F$.
  $H_F :=$ Menge der gebrochenen Hauptideale von $\mathcal{O}$
- *Klassengruppe* von $\mathcal{O}$: $\mathcal{CL}(\mathcal{O}) := I_F / H_F$.

logo

gebrochene Ideale und die Klassengruppe

- $\varnothing \neq \mathfrak{a} \subseteq F$ heisst *gebrochenes Ideal* von $\mathcal{O}$, wenn es ein $\xi \in \mathcal{O} \backslash \{0\}$ und ein Ideal $\{0\} \neq \mathfrak{b}$ in $\mathcal{O}$ gibt mit $\mathfrak{b} = \xi \cdot \mathfrak{a}$.
  $I_F :=$ Menge der gebrochenen Ideale von $\mathcal{O}$.
- gebrochenes Ideal von $\mathcal{O}$ ist freier $\mathbb{Z}$- Modul vom Rang n.
- Die *Norm* eines solchen Ideals $\mathfrak{b}$: Absolutbetrag der Determinante einer Transformationsmatrix einer $\mathbb{Z}$-Basis von $\mathcal{O}$ zu einer $\mathbb{Z}$-Basis von $\mathfrak{b}$.
- gebrochenes Ideal $\mathfrak{a}$ von $\mathcal{O}$ heisst *gebrochenes Hauptideal* von $\mathcal{O}$, wenn es ein $c \in \mathbb{F} \backslash \{0\}$ gibt mit $\mathfrak{a} = c \cdot F$.
  $H_F :=$ Menge der gebrochenen Hauptideale von $\mathcal{O}$
- *Klassengruppe* von $\mathcal{O}$: $\mathcal{CL}(\mathcal{O}) := I_F / H_F$.

logo

gebrochene Ideale und die Klassengruppe

- $\varnothing \neq \mathfrak{a} \subseteq F$ heisst *gebrochenes Ideal* von $\mathcal{O}$, wenn es ein $\xi \in \mathcal{O}\backslash\{0\}$ und ein Ideal $\{0\} \neq \mathfrak{b}$ in $\mathcal{O}$ gibt mit $\mathfrak{b} = \xi \cdot \mathfrak{a}$.
  $I_F :=$ Menge der gebrochenen Ideale von $\mathcal{O}$.
- gebrochenes Ideal von $\mathcal{O}$ ist freier $\mathbb{Z}$- Modul vom Rang n.
- Die *Norm* eines solchen Ideals $\mathfrak{b}$: Absolutbetrag der Determinante einer Transformationsmatrix einer $\mathbb{Z}$-Basis von $\mathcal{O}$ zu einer $\mathbb{Z}$-Basis von $\mathfrak{b}$.
- gebrochenes Ideal $\mathfrak{a}$ von $\mathcal{O}$ heisst *gebrochenes Hauptideal* von $\mathcal{O}$, wenn es ein $c \in \mathbb{F}\backslash\{0\}$ gibt mit $\mathfrak{a} = c \cdot F$.
  $H_F :=$ Menge der gebrochenen Hauptideale von $\mathcal{O}$
- *Klassengruppe* von $\mathcal{O}$: $\mathcal{CL}(\mathcal{O}) := I_F / H_F$.

logo

- *Klassenzahl von F:* $h_F := \#\mathcal{Cl}(\mathcal{O})$
- $\mathcal{Cl}(\mathcal{O}) \cong \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$

logo

- *Klassenzahl von* F: $h_F := \#\mathcal{Cl}(\mathcal{O})$
- $\mathcal{Cl}(\mathcal{O}) \cong \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$

Satz von Dedekind-Kummer

- $E := \mathbb{Q}(\alpha)$ Körpererweiterung von $\mathbb{Q}$ vom Grad 2
- $f(x) \in \mathbb{Z}[x]$ Minimalpolynom von α
- $B := \mathbb{Z}[\alpha]$ die Gleichungsordnung von f und gleichzeitig die Maximalordnung von E.
- $\mathfrak{p} := p\mathbb{Z}$ Primideal von $\mathbb{Z}$.
- $\overline{f(x)}$ Reduktion von $f(x)$ modulo $\mathfrak{p}$
- $\overline{f(x)} = \overline{p_1(x)} \cdot \overline{p_2(x)}$ die Faktorisierung von $\overline{f}(x)$ in irreduzible Polynome $\overline{p_i}(x) \in (\mathbb{Z}/\mathfrak{p})[x]$
- $p_i(x) \in \mathbb{Z}[x]$ Polynom mit $p_i(x) \equiv \overline{p_i(x)} \bmod \mathfrak{p}$ für i$\in \{1, 2\}$.
- $\mathfrak{p}_i := p\mathcal{O} + p_i(\alpha)\mathcal{O}$. Dann gilt:
- $$p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2.$$

logo

Satz von Dedekind-Kummer

- $E := \mathbb{Q}(\alpha)$ Körpererweiterung von $\mathbb{Q}$ vom Grad 2
- $f(x) \in \mathbb{Z}[x]$ Minimalpolynom von α
- $B := \mathbb{Z}[\alpha]$ die Gleichungsordnung von f und gleichzeitig die Maximalordnung von E.
- $\mathfrak{p} := p\mathbb{Z}$ Primideal von $\mathbb{Z}$.
- $\overline{f(x)}$ Reduktion von $f(x)$ modulo $\mathfrak{p}$
- $\overline{f(x)} = \overline{p_1(x)} \cdot \overline{p_2(x)}$ die Faktorisierung von $\overline{f}(x)$ in irreduzible Polynome $\overline{p_i}(x) \in (\mathbb{Z}/\mathfrak{p})[x]$
- $p_i(x) \in \mathbb{Z}[x]$ Polynom mit $p_i(x) \equiv \overline{p_i(x)} \bmod \mathfrak{p}$ für i$\in \{1, 2\}$.
- $\mathfrak{p}_i := p\mathcal{O} + p_i(\alpha)\mathcal{O}$. Dann gilt:
- $$p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2.$$

logo

Satz von Dedekind-Kummer

- $E := \mathbb{Q}(\alpha)$ Körpererweiterung von $\mathbb{Q}$ vom Grad 2
- $f(x) \in \mathbb{Z}[x]$ Minimalpolynom von α
- $B := \mathbb{Z}[\alpha]$ die Gleichungsordnung von f und gleichzeitig die Maximalordnung von E.
- $\mathfrak{p} := p\mathbb{Z}$ Primideal von $\mathbb{Z}$.
- $\overline{f(x)}$ Reduktion von $f(x)$ modulo $\mathfrak{p}$
- $\overline{f(x)} = \overline{p_1(x)} \cdot \overline{p_2(x)}$ die Faktorisierung von $\overline{f}(x)$ in irreduzible Polynome $\overline{p_i}(x) \in (\mathbb{Z}/\mathfrak{p})[x]$
- $p_i(x) \in \mathbb{Z}[x]$ Polynom mit $p_i(x) \equiv \overline{p_i(x)} \mod \mathfrak{p}$ für i$\in \{1, 2\}$.
- $\mathfrak{p}_i := p\mathcal{O} + p_i(\alpha)\mathcal{O}$. Dann gilt:
- $$p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2.$$

logo

Satz von Dedekind-Kummer

- $E := \mathbb{Q}(\alpha)$ Körpererweiterung von $\mathbb{Q}$ vom Grad 2
- $f(x) \in \mathbb{Z}[x]$ Minimalpolynom von α
- $B := \mathbb{Z}[\alpha]$ die Gleichungsordnung von f und gleichzeitig die Maximalordnung von E.
- $\mathfrak{p} := p\mathbb{Z}$ Primideal von $\mathbb{Z}$.
- $\overline{f(x)}$ Reduktion von $f(x)$ modulo $\mathfrak{p}$
- $\overline{f(x)} = \overline{p_1(x)} \cdot \overline{p_2(x)}$ die Faktorisierung von $\overline{f}(x)$ in irreduzible Polynome $\overline{p_i}(x) \in (\mathbb{Z}/\mathfrak{p})[x]$
- $p_i(x) \in \mathbb{Z}[x]$ Polynom mit $p_i(x) \equiv \overline{p_i(x)} \bmod \mathfrak{p}$ für i$\in \{1, 2\}$.
- $\mathfrak{p}_i := p\mathcal{O} + p_i(\alpha)\mathcal{O}$. Dann gilt:
- $$p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2.$$

logo

Satz von Dedekind-Kummer

- $E := \mathbb{Q}(\alpha)$ Körpererweiterung von $\mathbb{Q}$ vom Grad 2
- $f(x) \in \mathbb{Z}[x]$ Minimalpolynom von α
- $B := \mathbb{Z}[\alpha]$ die Gleichungsordnung von f und gleichzeitig die Maximalordnung von E.
- $\mathfrak{p} := p\mathbb{Z}$ Primideal von $\mathbb{Z}$.
- $\overline{f(x)}$ Reduktion von $f(x)$ modulo $\mathfrak{p}$
- $\overline{f(x)} = \overline{p_1(x)} \cdot \overline{p_2(x)}$ die Faktorisierung von $\overline{f}(x)$ in irreduzible Polynome $\overline{p_i}(x) \in (\mathbb{Z}/\mathfrak{p})[x]$
- $p_i(x) \in \mathbb{Z}[x]$ Polynom mit $p_i(x) \equiv \overline{p_i(x)} \mod \mathfrak{p}$ für i$\in \{1, 2\}$.
- $\mathfrak{p}_i := p\mathcal{O} + p_i(\alpha)\mathcal{O}$. Dann gilt:
- $$p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2.$$

logo

Satz von Dedekind-Kummer

- $E := \mathbb{Q}(\alpha)$ Körpererweiterung von $\mathbb{Q}$ vom Grad 2
- $f(x) \in \mathbb{Z}[x]$ Minimalpolynom von α
- $B := \mathbb{Z}[\alpha]$ die Gleichungsordnung von f und gleichzeitig die Maximalordnung von E.
- $\mathfrak{p} := p\mathbb{Z}$ Primideal von $\mathbb{Z}$.
- $\overline{f(x)}$ Reduktion von $f(x)$ modulo $\mathfrak{p}$
- $\overline{f(x)} = \overline{p_1(x)} \cdot \overline{p_2(x)}$ die Faktorisierung von $\overline{f}(x)$ in irreduzible Polynome $\overline{p_i}(x) \in (\mathbb{Z}/\mathfrak{p})[x]$
- $p_i(x) \in \mathbb{Z}[x]$ Polynom mit $p_i(x) \equiv \overline{p_i(x)} \mod \mathfrak{p}$ für i$\in \{1, 2\}$.
- $\mathfrak{p}_i := p\mathcal{O} + p_i(\alpha)\mathcal{O}$. Dann gilt:
- $$p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2.$$

logo

Satz von Dedekind-Kummer

- $E := \mathbb{Q}(\alpha)$ Körpererweiterung von $\mathbb{Q}$ vom Grad 2
- $f(x) \in \mathbb{Z}[x]$ Minimalpolynom von α
- $B := \mathbb{Z}[\alpha]$ die Gleichungsordnung von f und gleichzeitig die Maximalordnung von E.
- $\mathfrak{p} := p\mathbb{Z}$ Primideal von $\mathbb{Z}$.
- $\overline{f(x)}$ Reduktion von $f(x)$ modulo $\mathfrak{p}$
- $\overline{f(x)} = \overline{p_1(x)} \cdot \overline{p_2(x)}$ die Faktorisierung von $\overline{f}(x)$ in irreduzible Polynome $\overline{p_i}(x) \in (\mathbb{Z}/\mathfrak{p})[x]$
- $p_i(x) \in \mathbb{Z}[x]$ Polynom mit $p_i(x) \equiv \overline{p_i(x)}$ mod $\mathfrak{p}$ für i$\in \{1, 2\}$.
- $\mathfrak{p}_i := p\mathcal{O} + p_i(\alpha)\mathcal{O}$. Dann gilt:
- $$p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2.$$

Satz von Dedekind-Kummer

- $E := \mathbb{Q}(\alpha)$ Körpererweiterung von $\mathbb{Q}$ vom Grad 2
- $f(x) \in \mathbb{Z}[x]$ Minimalpolynom von α
- $B := \mathbb{Z}[\alpha]$ die Gleichungsordnung von f und gleichzeitig die Maximalordnung von E.
- $\mathfrak{p} := p\mathbb{Z}$ Primideal von $\mathbb{Z}$.
- $\overline{f(x)}$ Reduktion von $f(x)$ modulo $\mathfrak{p}$
- $\overline{f(x)} = \overline{p_1(x)} \cdot \overline{p_2(x)}$ die Faktorisierung von $\overline{f}(x)$ in irreduzible Polynome $\overline{p_i}(x) \in (\mathbb{Z}/\mathfrak{p})[x]$
- $p_i(x) \in \mathbb{Z}[x]$ Polynom mit $p_i(x) \equiv \overline{p_i(x)}$ mod $\mathfrak{p}$ für i$\in \{1, 2\}$.
- $\mathfrak{p}_i := p\mathcal{O} + p_i(\alpha)\mathcal{O}$. Dann gilt:
- $$p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2.$$

logo

Satz von Dedekind-Kummer

- $E := \mathbb{Q}(\alpha)$ Körpererweiterung von $\mathbb{Q}$ vom Grad 2
- $f(x) \in \mathbb{Z}[x]$ Minimalpolynom von α
- $B := \mathbb{Z}[\alpha]$ die Gleichungsordnung von f und gleichzeitig die Maximalordnung von E.
- $\mathfrak{p} := p\mathbb{Z}$ Primideal von $\mathbb{Z}$.
- $\overline{f(x)}$ Reduktion von $f(x)$ modulo $\mathfrak{p}$
- $\overline{f(x)} = \overline{p_1(x)} \cdot \overline{p_2(x)}$ die Faktorisierung von $\overline{f}(x)$ in irreduzible Polynome $\overline{p_i}(x) \in (\mathbb{Z}/\mathfrak{p})[x]$
- $p_i(x) \in \mathbb{Z}[x]$ Polynom mit $p_i(x) \equiv \overline{p_i(x)}$ mod $\mathfrak{p}$ für i$\in \{1, 2\}$.
- $\mathfrak{p}_i := p\mathcal{O} + p_i(\alpha)\mathcal{O}$. Dann gilt:
- $$p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2.$$

Verbindung zwischen Idealen und Isogenien

Isogenie

vom Grad ℓ mit Kern C, auf dem π den Eigenwert λ hat

Ideal

$\ell\mathcal{O} + (\pi - \lambda)\mathcal{O}$,
ℓ Elkies-Primzahl von E

Verbindung zwischen Idealen und Isogenien

Isogenie

vom Grad ℓ mit Kern C, auf dem π den Eigenwert λ hat

Ideal

$\ell\mathcal{O} + (\pi - \lambda)\mathcal{O}$,
ℓ Elkies-Primzahl von E

- Es gilt sogar: Isomorphieklassen der zu E_1 isogenen Kurven entsprechen Elementen der Klassengruppe $\mathcal{Cl}(\mathcal{O})$
- Zu jedem Klassengruppenelement $\ell\mathcal{O} + (\pi - \lambda)\mathcal{O}$ gibt es eine von E_1 ausgehende Isogenie vom Grad ℓ mit Kern C, auf dem π den Eigenwert λ hat
- Komposition von Isogenien entspricht Idealmultiplikation, Komposition mit einem Isomorphismus entspricht Multiplikation mit $\mathcal{O}$
- Was heisst das für den Algorithmus?
- beim Berechnen von Isogenien anstelle der Komposition zugehörige Ideale multiplizieren und passendes Klassengruppen-Ideal verwenden
- Reduktionsalgorithmus zum Finden eines besonders kleinen Restklassen-Vertreters

- Es gilt sogar: Isomorphieklassen der zu E_1 isogenen Kurven entsprechen Elementen der Klassengruppe $\mathcal{Cl}(\mathcal{O})$
- Zu jedem Klassengruppenelement $\ell\mathcal{O} + (\pi - \lambda)\mathcal{O}$ gibt es eine von E_1 ausgehende Isogenie vom Grad ℓ mit Kern C, auf dem π den Eigenwert λ hat
- Komposition von Isogenien entspricht Idealmultiplikation, Komposition mit einem Isomorphismus entspricht Multiplikation mit $\mathcal{O}$
- Was heisst das für den Algorithmus?
- beim Berechnen von Isogenien anstelle der Komposition zugehörige Ideale multiplizieren und passendes Klassengruppen-Ideal verwenden
- Reduktionsalgorithmus zum Finden eines besonders kleinen Restklassen-Vertreters

- Es gilt sogar: Isomorphieklassen der zu E_1 isogenen Kurven entsprechen Elementen der Klassengruppe $\mathcal{Cl}(\mathcal{O})$
- Zu jedem Klassengruppenelement $\ell\mathcal{O} + (\pi - \lambda)\mathcal{O}$ gibt es eine von E_1 ausgehende Isogenie vom Grad ℓ mit Kern C, auf dem π den Eigenwert λ hat
- Komposition von Isogenien entspricht Idealmultiplikation, Komposition mit einem Isomorphismus entspricht Multiplikation mit $\mathcal{O}$
- Was heisst das für den Algorithmus?
- beim Berechnen von Isogenien anstelle der Komposition zugehörige Ideale multiplizieren und passendes Klassengruppen-Ideal verwenden
- Reduktionsalgorithmus zum Finden eines besonders kleinen Restklassen-Vertreters

- Es gilt sogar: Isomorphieklassen der zu E_1 isogenen Kurven entsprechen Elementen der Klassengruppe $\mathcal{Cl}(\mathcal{O})$
- Zu jedem Klassengruppenelement $\ell\mathcal{O} + (\pi - \lambda)\mathcal{O}$ gibt es eine von E_1 ausgehende Isogenie vom Grad ℓ mit Kern C, auf dem π den Eigenwert λ hat
- Komposition von Isogenien entspricht Idealmultiplikation, Komposition mit einem Isomorphismus entspricht Multiplikation mit $\mathcal{O}$
- Was heisst das für den Algorithmus?
- beim Berechnen von Isogenien anstelle der Komposition zugehörige Ideale multiplizieren und passendes Klassengruppen-Ideal verwenden
- Reduktionsalgorithmus zum Finden eines besonders kleinen Restklassen-Vertreters

- Es gilt sogar: Isomorphieklassen der zu E_1 isogenen Kurven entsprechen Elementen der Klassengruppe $\mathcal{Cl}(\mathcal{O})$
- Zu jedem Klassengruppenelement $\ell\mathcal{O} + (\pi - \lambda)\mathcal{O}$ gibt es eine von E_1 ausgehende Isogenie vom Grad ℓ mit Kern C, auf dem π den Eigenwert λ hat
- Komposition von Isogenien entspricht Idealmultiplikation, Komposition mit einem Isomorphismus entspricht Multiplikation mit $\mathcal{O}$
- Was heisst das für den Algorithmus?
- beim Berechnen von Isogenien anstelle der Komposition zugehörige Ideale multiplizieren und passendes Klassengruppen-Ideal verwenden
- Reduktionsalgorithmus zum Finden eines besonders kleinen Restklassen-Vertreters

- Es gilt sogar: Isomorphieklassen der zu E_1 isogenen Kurven entsprechen Elementen der Klassengruppe $\mathcal{Cl}(\mathcal{O})$
- Zu jedem Klassengruppenelement $\ell\mathcal{O} + (\pi - \lambda)\mathcal{O}$ gibt es eine von E_1 ausgehende Isogenie vom Grad ℓ mit Kern C, auf dem π den Eigenwert λ hat
- Komposition von Isogenien entspricht Idealmultiplikation, Komposition mit einem Isomorphismus entspricht Multiplikation mit $\mathcal{O}$
- Was heisst das für den Algorithmus?
- beim Berechnen von Isogenien anstelle der Komposition zugehörige Ideale multiplizieren und passendes Klassengruppen-Ideal verwenden
- Reduktionsalgorithmus zum Finden eines besonders kleinen Restklassen-Vertreters

Pollard-λ-Algorithmus

- $f : \mathbb{F}_p \to L \times \{1, 2\}$ pseudozufällige Funktion: liefert zu jeder j-Invariante j Elkies-Primzahl ℓ, gibt an, welche Nullstelle von $\Phi_l(j, T)$ j-Invariante der neuen Zielkurve sein soll
- gehen von E_1 $r := \lceil \sqrt{h_F} \rceil$ Schritte weit
- auf dem Weg Multiplikation, Reduktion der zugehörigen Ideale
- merken uns das letzte Ideal I_r, letzte j-Invariante j_r
- starten von E_2, und gehen so lange (aber höchstens r Schritte), bis wir bei j-Invariante j_r ankommen
- wieder reduzieren und multiplizieren der auf dem Weg entstehenden Klassengruppen-Ideale
- resultierendes Ideal: I'_r
- I_r / I'_r entspricht einer Isogenie zwischen E_1 und E_2, wobei I'^{-1}_r die inverse Klassengruppenelement ist
- dieses faktorisieren und zugehörige Isogenie berechnen

Pollard-λ-Algorithmus

- $f : \mathbb{F}_p \to L \times \{1, 2\}$ pseudozufällige Funktion: liefert zu jeder j-Invariante j Elkies-Primzahl ℓ, gibt an, welche Nullstelle von $\Phi_l(j, T)$ j-Invariante der neuen Zielkurve sein soll
- gehen von E_1 $r := \lceil \sqrt{h_F} \rceil$ Schritte weit
- auf dem Weg Multiplikation, Reduktion der zugehörigen Ideale
- merken uns das letzte Ideal I_r, letzte j-Invariante j_r
- starten von E_2, und gehen so lange (aber höchstens r Schritte), bis wir bei j-Invariante j_r ankommen
- wieder reduzieren und multiplizieren der auf dem Weg entstehenden Klassengruppen-Ideale
- resultierendes Ideal: I'_r
- I_r / I'_r entspricht einer Isogenie zwischen E_1 und E_2, wobei I'^{-1}_r die inverse Klassengruppenelement ist
- dieses faktorisieren und zugehörige Isogenie berechnen

Pollard-λ-Algorithmus

- $f : \mathbb{F}_p \to L \times \{1, 2\}$ pseudozufällige Funktion: liefert zu jeder j-Invariante j Elkies-Primzahl ℓ, gibt an, welche Nullstelle von $\Phi_l(j, T)$ j-Invariante der neuen Zielkurve sein soll
- gehen von E_1 $r := \lceil \sqrt{h_F} \rceil$ Schritte weit
- auf dem Weg Multiplikation, Reduktion der zugehörigen Ideale
- merken uns das letzte Ideal I_r, letzte j-Invariante j_r
- starten von E_2, und gehen so lange (aber höchstens r Schritte), bis wir bei j-Invariante j_r ankommen
- wieder reduzieren und multiplizieren der auf dem Weg entstehenden Klassengruppen-Ideale
- resultierendes Ideal: I'_r
- I_r / I'_r entspricht einer Isogenie zwischen E_1 und E_2, wobei I'^{-1}_r die inverse Klassengruppenelement ist
- dieses faktorisieren und zugehörige Isogenie berechnen

Pollard-λ-Algorithmus

- $f : \mathbb{F}_p \to L \times \{1, 2\}$ pseudozufällige Funktion: liefert zu jeder j-Invariante j Elkies-Primzahl ℓ, gibt an, welche Nullstelle von $\Phi_l(j, T)$ j-Invariante der neuen Zielkurve sein soll
- gehen von E_1 $r := \lceil \sqrt{h_F} \rceil$ Schritte weit
- auf dem Weg Multiplikation, Reduktion der zugehörigen Ideale
- merken uns das letzte Ideal I_r, letzte j-Invariante j_r
- starten von E_2, und gehen so lange (aber höchstens r Schritte), bis wir bei j-Invariante j_r ankommen
- wieder reduzieren und multiplizieren der auf dem Weg entstehenden Klassengruppen-Ideale
- resultierendes Ideal: I'_r
- I_r / I'_r entspricht einer Isogenie zwischen E_1 und E_2, wobei I'^{-1}_r die inverse Klassengruppenelement ist
- dieses faktorisieren und zugehörige Isogenie berechnen

Pollard-λ-Algorithmus

- $f : \mathbb{F}_p \to L \times \{1, 2\}$ pseudozufällige Funktion: liefert zu jeder j-Invariante j Elkies-Primzahl ℓ, gibt an, welche Nullstelle von $\Phi_l(j, T)$ j-Invariante der neuen Zielkurve sein soll
- gehen von E_1 $r := \lceil \sqrt{h_F} \rceil$ Schritte weit
- auf dem Weg Multiplikation, Reduktion der zugehörigen Ideale
- merken uns das letzte Ideal I_r, letzte j-Invariante j_r
- starten von E_2, und gehen so lange (aber höchstens r Schritte), bis wir bei j-Invariante j_r ankommen
- wieder reduzieren und multiplizieren der auf dem Weg entstehenden Klassengruppen-Ideale
- resultierendes Ideal: I'_r
- I_r / I'_r entspricht einer Isogenie zwischen E_1 und E_2, wobei I'^{-1}_r die inverse Klassengruppenelement ist
- dieses faktorisieren und zugehörige Isogenie berechnen

Pollard-λ-Algorithmus

- $f : \mathbb{F}_p \to L \times \{1, 2\}$ pseudozufällige Funktion: liefert zu jeder j-Invariante j Elkies-Primzahl ℓ, gibt an, welche Nullstelle von $\Phi_l(j, T)$ j-Invariante der neuen Zielkurve sein soll
- gehen von E_1 $r := \lceil \sqrt{h_F} \rceil$ Schritte weit
- auf dem Weg Multiplikation, Reduktion der zugehörigen Ideale
- merken uns das letzte Ideal I_r, letzte j-Invariante j_r
- starten von E_2, und gehen so lange (aber höchstens r Schritte), bis wir bei j-Invariante j_r ankommen
- wieder reduzieren und multiplizieren der auf dem Weg entstehenden Klassengruppen-Ideale
- resultierendes Ideal: I'_r
- I_r / I'_r entspricht einer Isogenie zwischen E_1 und E_2, wobei I'^{-1}_r die inverse Klassengruppenelement ist
- dieses faktorisieren und zugehörige Isogenie berechnen

Pollard-λ-Algorithmus

- $f : \mathbb{F}_p \to L \times \{1, 2\}$ pseudozufällige Funktion: liefert zu jeder j-Invariante j Elkies-Primzahl ℓ, gibt an, welche Nullstelle von $\Phi_l(j, T)$ j-Invariante der neuen Zielkurve sein soll
- gehen von E_1 $r := \lceil \sqrt{h_F} \rceil$ Schritte weit
- auf dem Weg Multiplikation, Reduktion der zugehörigen Ideale
- merken uns das letzte Ideal I_r, letzte j-Invariante j_r
- starten von E_2, und gehen so lange (aber höchstens r Schritte), bis wir bei j-Invariante j_r ankommen
- wieder reduzieren und multiplizieren der auf dem Weg entstehenden Klassengruppen-Ideale
- resultierendes Ideal: I'_r
- I_r / I'_r entspricht einer Isogenie zwischen E_1 und E_2, wobei I'^{-1}_r die inverse Klassengruppenelement ist
- dieses faktorisieren und zugehörige Isogenie berechnen

Pollard-λ-Algorithmus

- $f : \mathbb{F}_p \to L \times \{1, 2\}$ pseudozufällige Funktion: liefert zu jeder j-Invariante j Elkies-Primzahl ℓ, gibt an, welche Nullstelle von $\Phi_l(j, T)$ j-Invariante der neuen Zielkurve sein soll
- gehen von E_1 $r := \lceil \sqrt{h_F} \rceil$ Schritte weit
- auf dem Weg Multiplikation, Reduktion der zugehörigen Ideale
- merken uns das letzte Ideal I_r, letzte j-Invariante j_r
- starten von E_2, und gehen so lange (aber höchstens r Schritte), bis wir bei j-Invariante j_r ankommen
- wieder reduzieren und multiplizieren der auf dem Weg entstehenden Klassengruppen-Ideale
- resultierendes Ideal: I'_r
- I_r / I'_r entspricht einer Isogenie zwischen E_1 und E_2, wobei I'^{-1}_r die inverse Klassengruppenelement ist
- dieses faktorisieren und zugehörige Isogenie berechnen

Pollard-λ-Algorithmus

- $f : \mathbb{F}_p \to L \times \{1, 2\}$ pseudozufällige Funktion: liefert zu jeder j-Invariante j Elkies-Primzahl ℓ, gibt an, welche Nullstelle von $\Phi_l(j, T)$ j-Invariante der neuen Zielkurve sein soll
- gehen von E_1 $r := \lceil \sqrt{h_F} \rceil$ Schritte weit
- auf dem Weg Multiplikation, Reduktion der zugehörigen Ideale
- merken uns das letzte Ideal I_r, letzte j-Invariante j_r
- starten von E_2, und gehen so lange (aber höchstens r Schritte), bis wir bei j-Invariante j_r ankommen
- wieder reduzieren und multiplizieren der auf dem Weg entstehenden Klassengruppen-Ideale
- resultierendes Ideal: I'_r
- I_r / I'_r entspricht einer Isogenie zwischen E_1 und E_2, wobei I'^{-1}_r die inverse Klassengruppenelement ist
- dieses faktorisieren und zugehörige Isogenie berechnen

Outline

logo

- Algorithmus für Kurven über Körpern der Charakteristik 2,3 anpassen
- Algorithmus für Kurven über Erweiterungskörpern von Primkörpern
- Algorithmus von Kohel: führt die Berechnung von Isogenien zwischen Kurven mit beliebigem Endomorphismenring auf schon behandelten Fall zurück

- Algorithmus für Kurven über Körpern der Charakteristik 2,3 anpassen
- Algorithmus für Kurven über Erweiterungskörpern von Primkörpern
- Algorithmus von Kohel: führt die Berechnung von Isogenien zwischen Kurven mit beliebigem Endomorphismenring auf schon behandelten Fall zurück

logo

- Algorithmus für Kurven über Körpern der Charakteristik 2,3 anpassen
- Algorithmus für Kurven über Erweiterungskörpern von Primkörpern
- Algorithmus von Kohel: führt die Berechnung von Isogenien zwischen Kurven mit beliebigem Endomorphismenring auf schon behandelten Fall zurück

Berechnung Isogenien elliptischer Kurven

- Vielen Dank!
- Fragen?

Berechnung Isogenien elliptischer Kurven

- Vielen Dank!
- Fragen?