# Beschreibung und Implementierung eines Algorithmus zur Punktezählung elliptischer Kurven über Körpern $\mathbb{F}_q$ mit kleiner ungerader Charakteristik $p$ nach Satoh

Diplomarbeit

Alexander Niske

Ludwig-Maximilians-Universität München
Fakultät für Mathematik, Informatik und Statistik
Mathematisches Institut

29. Januar 2009

# Gliederung

# Gliederung

# Gliederung

# Was ist eine elliptische Kurve?

Sei $K$ stets ein Körper der Charakteristik ungleich 2 und 3 (d. h. $1+1 \neq 0$ und $1+1+1 \neq 0$).
Den algebraischen Abschluss von $K$ bezeichnen wir mit $\overline{K}$.

# Was ist eine elliptische Kurve?

Sei $K$ stets ein Körper der Charakteristik ungleich 2 und 3 (d. h. $1+1 \neq 0$ und $1+1+1 \neq 0$).
Den algebraischen Abschluss von $K$ bezeichnen wir mit $\overline{K}$.

## Definition

Seien $a, b \in K$ mit $4a^3 + 27b^2 \neq 0$. Unter einer elliptischen Kurve (über $K$) verstehen wir die Menge

$$E = E(\overline{K}) := \{(x, y) \in \overline{K} \times \overline{K} \quad : \underbrace{y^2 = x^3 + ax + b}_{\textit{Weierstraß-Gleichung}}\} \cup \{\mathcal{O}\}.$$

# Was ist eine elliptische Kurve?

Sei $K$ stets ein Körper der Charakteristik ungleich 2 und 3 (d. h. $1+1 \neq 0$ und $1+1+1 \neq 0$).
Den algebraischen Abschluss von $K$ bezeichnen wir mit $\overline{K}$.

## Definition

Seien $a, b \in K$ mit $4a^3 + 27b^2 \neq 0$. Unter einer elliptischen Kurve (über $K$) verstehen wir die Menge

$$E = E(\overline{K}) := \{(x,y) \in \overline{K} \times \overline{K} \quad : \underbrace{y^2 = x^3 + ax + b}_{\textit{Weierstraß-Gleichung}}\} \cup \{\mathcal{O}\}.$$

Für jede Körpererweiterung $L \supset K$ ist die Menge der $L$-rationalen Punkte von $E$ gegeben durch

$$E(L) := \{(x,y) \in L \times L \quad : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

# Bemerkungen zur Definition

- Man verwendet die Notation $E: \; y^2 = x^3 + ax + b$.
- *Achtung*: $E/K$ bzw. über $K$ bedeutet $a, b \in K$.
  $E \setminus \{\mathcal{O}\}$ ist allerdings eine Teilmenge von $\overline{K} \times \overline{K}$.
- $\mathcal{O} := (0 : 1 : 0) \in \mathbb{P}_2(K)$ heißt unendlich-ferner Punkt.
  *Herkunft*: Eine elliptische Kurve ist eigentlich eine *glatte projektive Kurve vom Grad 3*.

# Bemerkungen zur Definition

- Man verwendet die Notation $E/K: \; y^2 = x^3 + ax + b$.
- *Achtung*: $E/K$ bzw. über $K$ bedeutet $a, b \in K$.
  $E \setminus \{\mathcal{O}\}$ ist allerdings eine Teilmenge von $\overline{K} \times \overline{K}$.
- $\mathcal{O} := (0 : 1 : 0) \in \mathbb{P}_2(K)$ heißt unendlich-ferner Punkt.
  *Herkunft*: Eine elliptische Kurve ist eigentlich eine *glatte projektive Kurve vom Grad 3*.

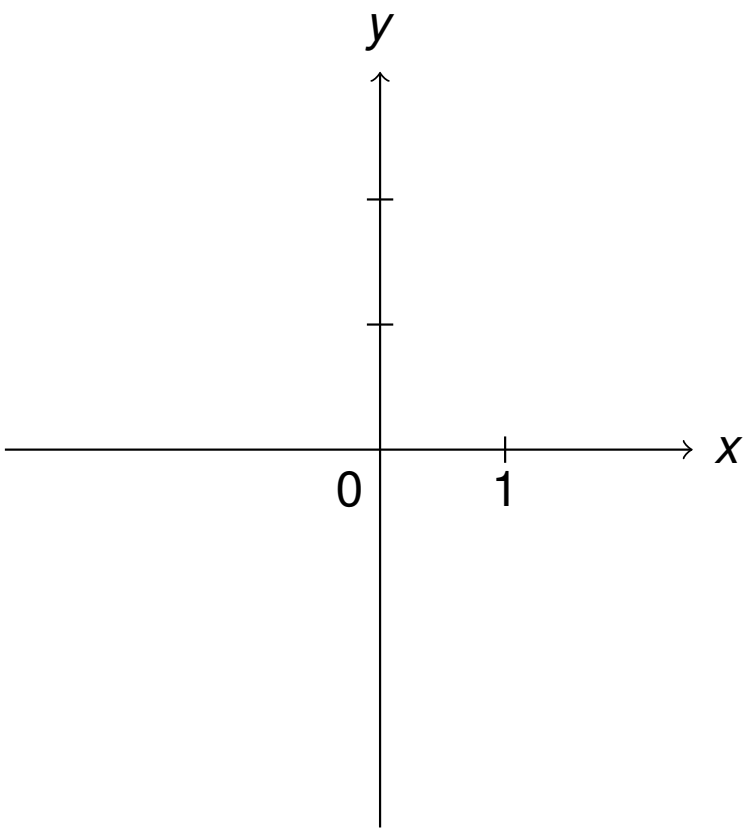
# Bemerkungen zur Definition

- Man verwendet die Notation $E/K: \ y^2 = x^3 + ax + b$.
- *Achtung*: $E/K$ bzw. über $K$ bedeutet $a, b \in K$.
  $E \setminus \{\mathcal{O}\}$ ist allerdings eine Teilmenge von $\overline{K} \times \overline{K}$.
- $\mathcal{O} := (0:1:0) \in \mathbb{P}_2(K)$ heißt unendlich-ferner Punkt.
  *Herkunft*: Eine elliptische Kurve ist eigentlich eine *glatte projektive Kurve vom Grad 3*.

# Bemerkungen zur Definition

- Man verwendet die Notation $E/K: \; y^2 = x^3 + ax + b$.
- *Achtung*: $E/K$ bzw. über $K$ bedeutet $a, b \in K$.
  $E \setminus \{\mathcal{O}\}$ ist allerdings eine Teilmenge von $\overline{K} \times \overline{K}$.
- $\mathcal{O} := (0 : 1 : 0) \in \mathbb{P}_2(K)$ heißt unendlich-ferner Punkt.
  *Herkunft*: Eine elliptische Kurve ist eigentlich eine *glatte projektive Kurve vom Grad 3*.

# Beispielkurven



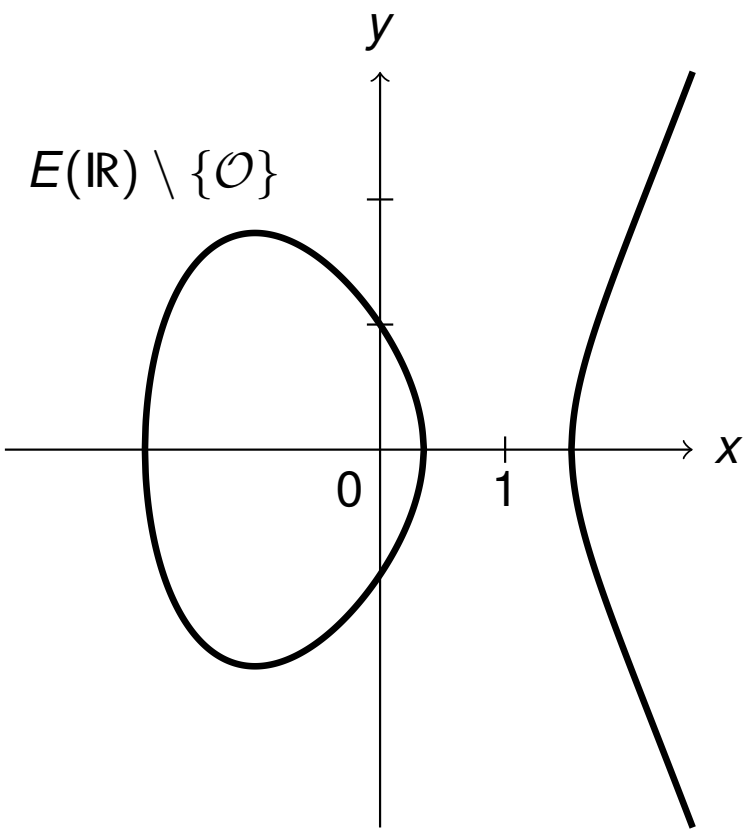

(a) $y^2 = x^3 - 3x + 1$




(b) $y^2 = x^3 - 4x + 5$

Abbildung : Elliptische Kurven über $\mathbb{R}$

# Beispielkurven



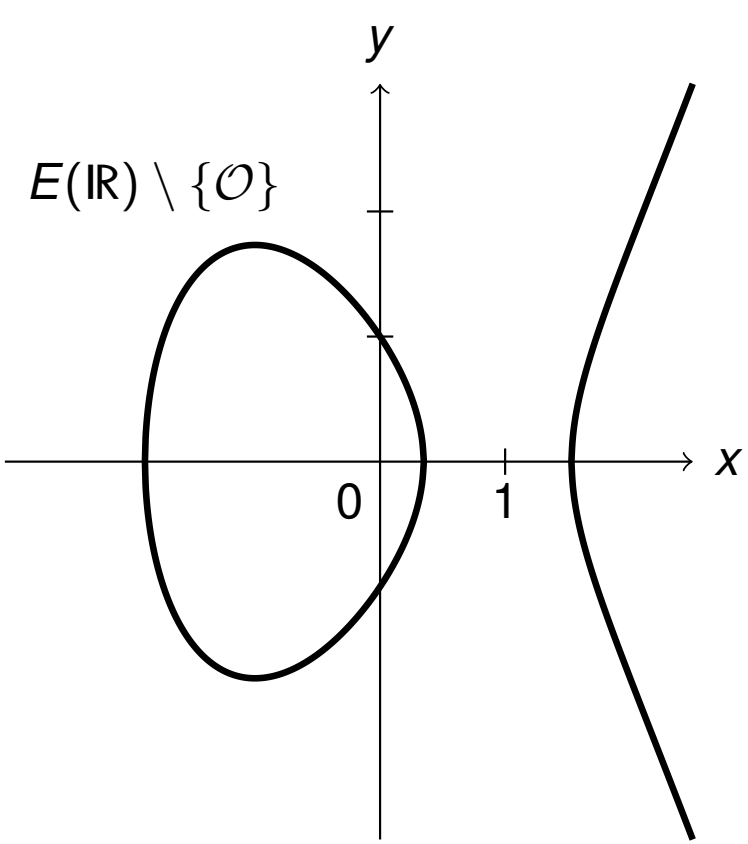

(a) $y^2 = x^3 - 3x + 1$



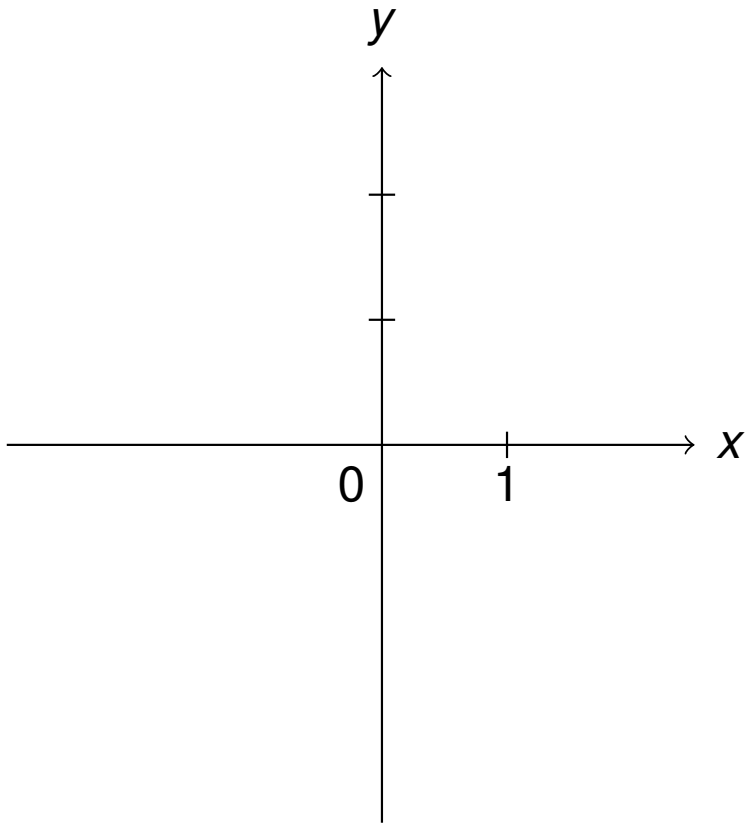

(b) $y^2 = x^3 - 4x + 5$

Abbildung : Elliptische Kurven über $\mathbb{R}$

# Beispielkurven



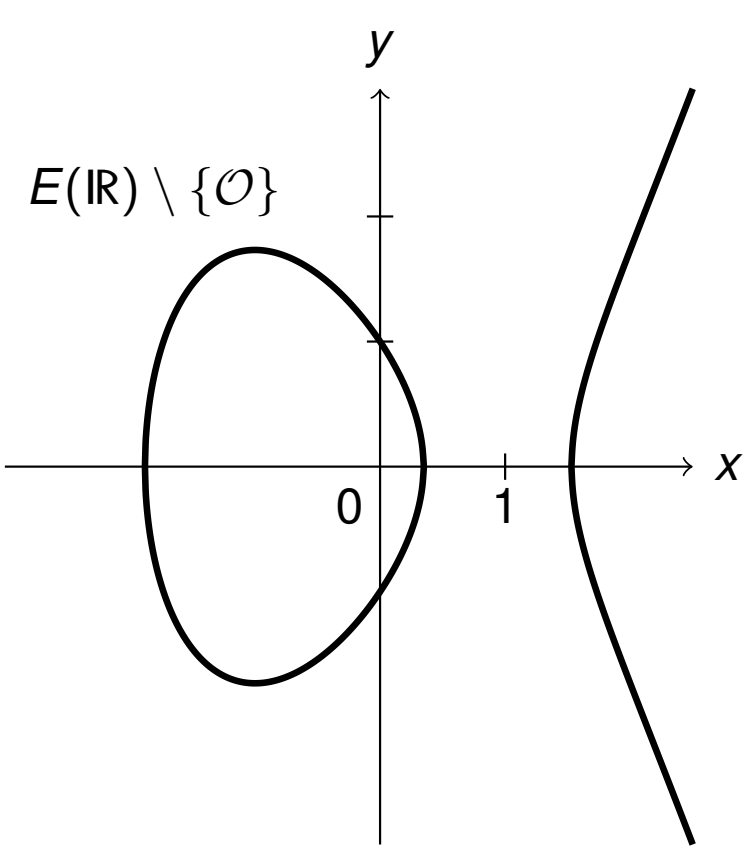

(a) $y^2 = x^3 - 3x + 1$



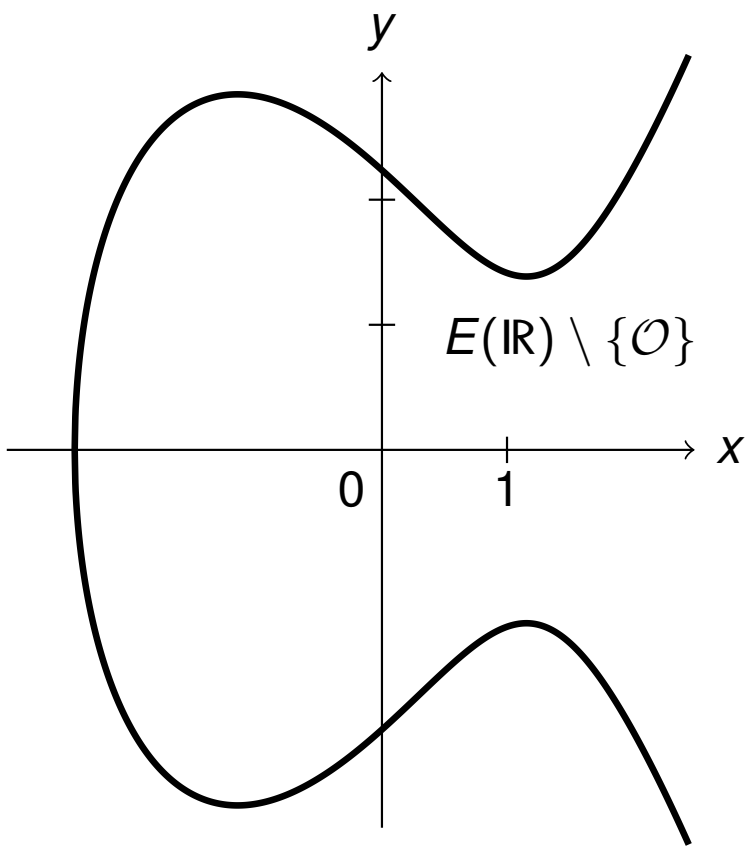

(b) $y^2 = x^3 - 4x + 5$

Abbildung : Elliptische Kurven über $\mathbb{R}$

# Beispielkurven




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




(b) $y^2 = x^3 - 4x + 5$

Abbildung : Elliptische Kurven über $\mathbb{R}$

# Eine elliptische Kurve ist eine abelsche Gruppe.

## Satz (Gruppengesetz)

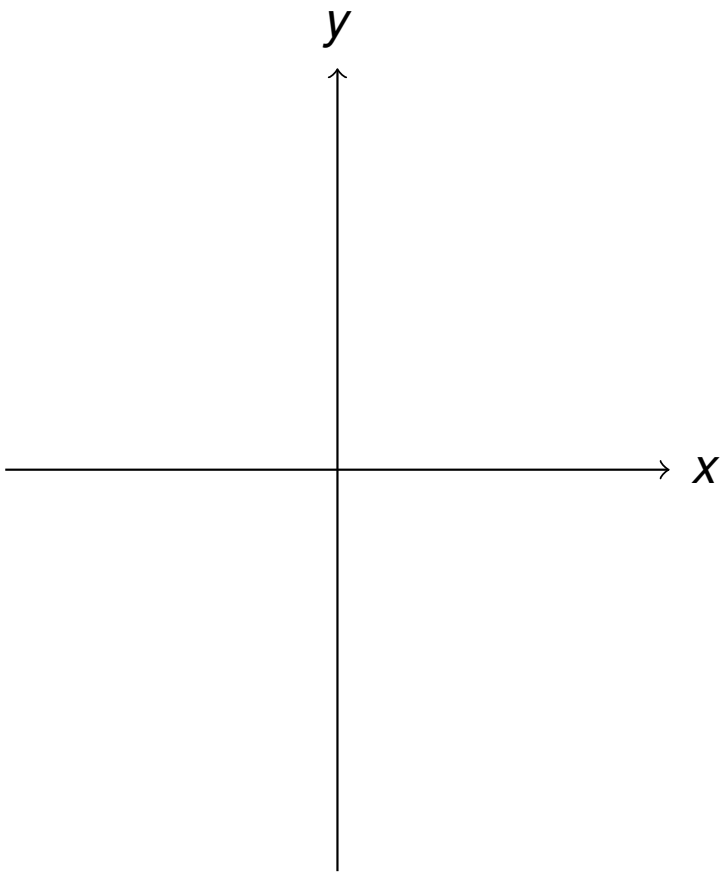
*Sei $E/K$ eine elliptische Kurve und $\mathcal{O} \neq P, Q \in E$.*
*Mit folgender Addition wird $(E, +, \mathcal{O})$ zu einer abelschen Gruppe (und $E(K)$ zu einer Untergruppe von $E$):*

$$P + Q := \begin{cases} \mathcal{O} & \text{falls } P = -Q, \\ (\lambda^2 - x_P - x_Q, \lambda(x_P - x_{P+Q}) - y_P) & \text{sonst,} \end{cases}$$

*wobei*

$$-Q = (x_Q, -y_Q) \quad \text{und} \quad \lambda := \begin{cases} \frac{3x_P^2 + a}{2y_P} & \text{falls } P = Q, \\ \frac{y_P - y_Q}{x_P - x_Q} & \text{sonst.} \end{cases}$$

# Geometrische Interpretation des Gruppengesetzes



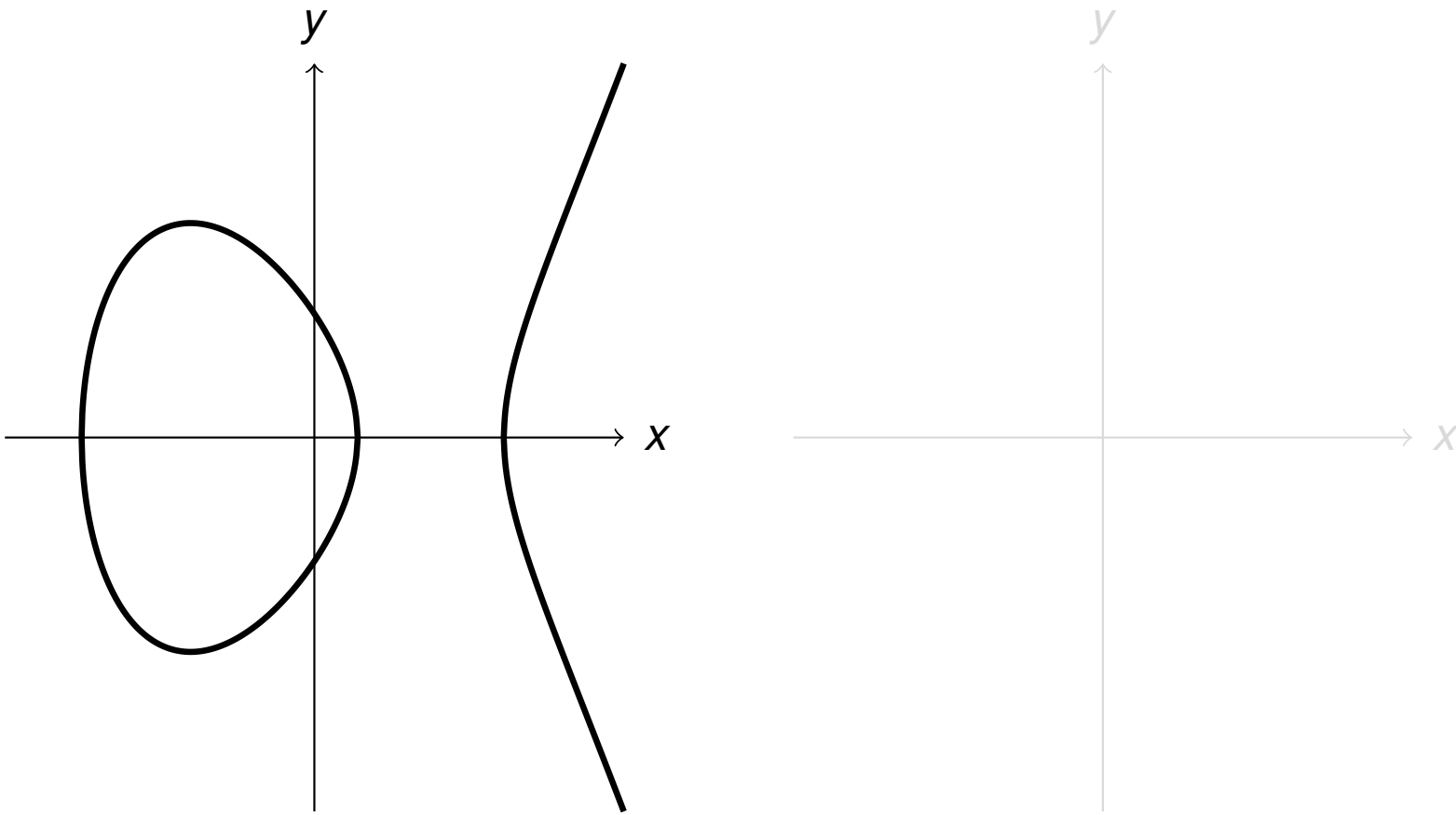

(a) Addition




(b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

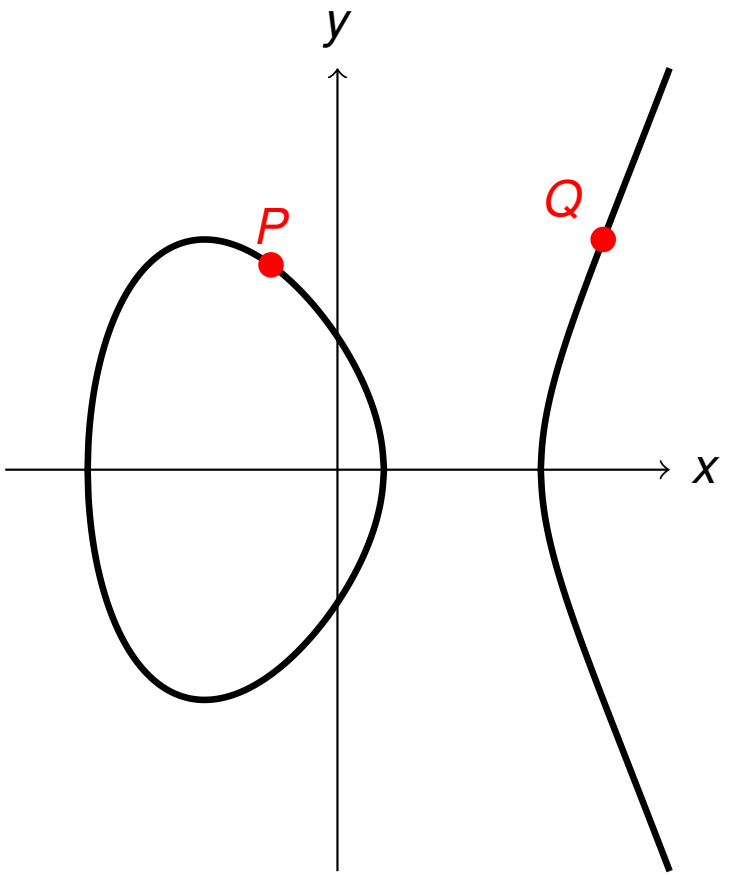
# Geometrische Interpretation des Gruppengesetzes




(a) Addition (b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

# Geometrische Interpretation des Gruppengesetzes



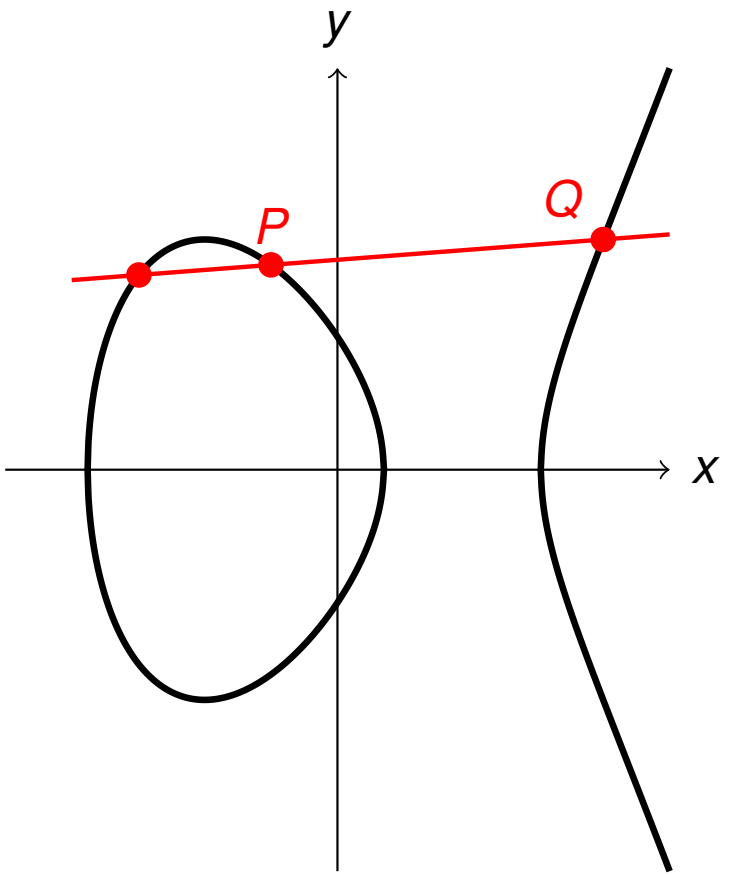

(a) Addition




(b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

# Geometrische Interpretation des Gruppengesetzes



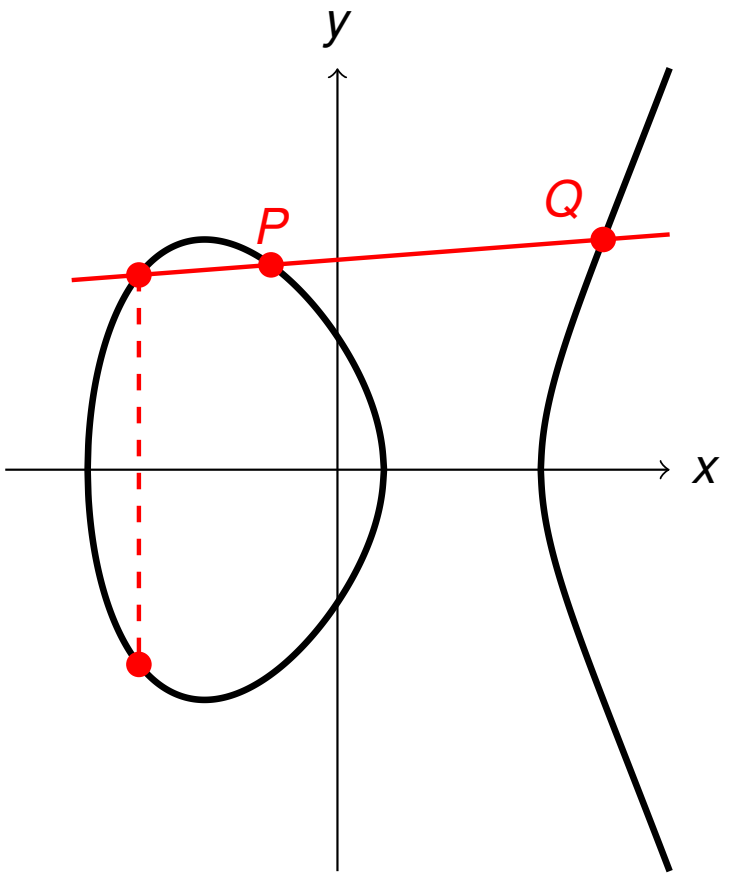

(a) Addition




(b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

# Geometrische Interpretation des Gruppengesetzes



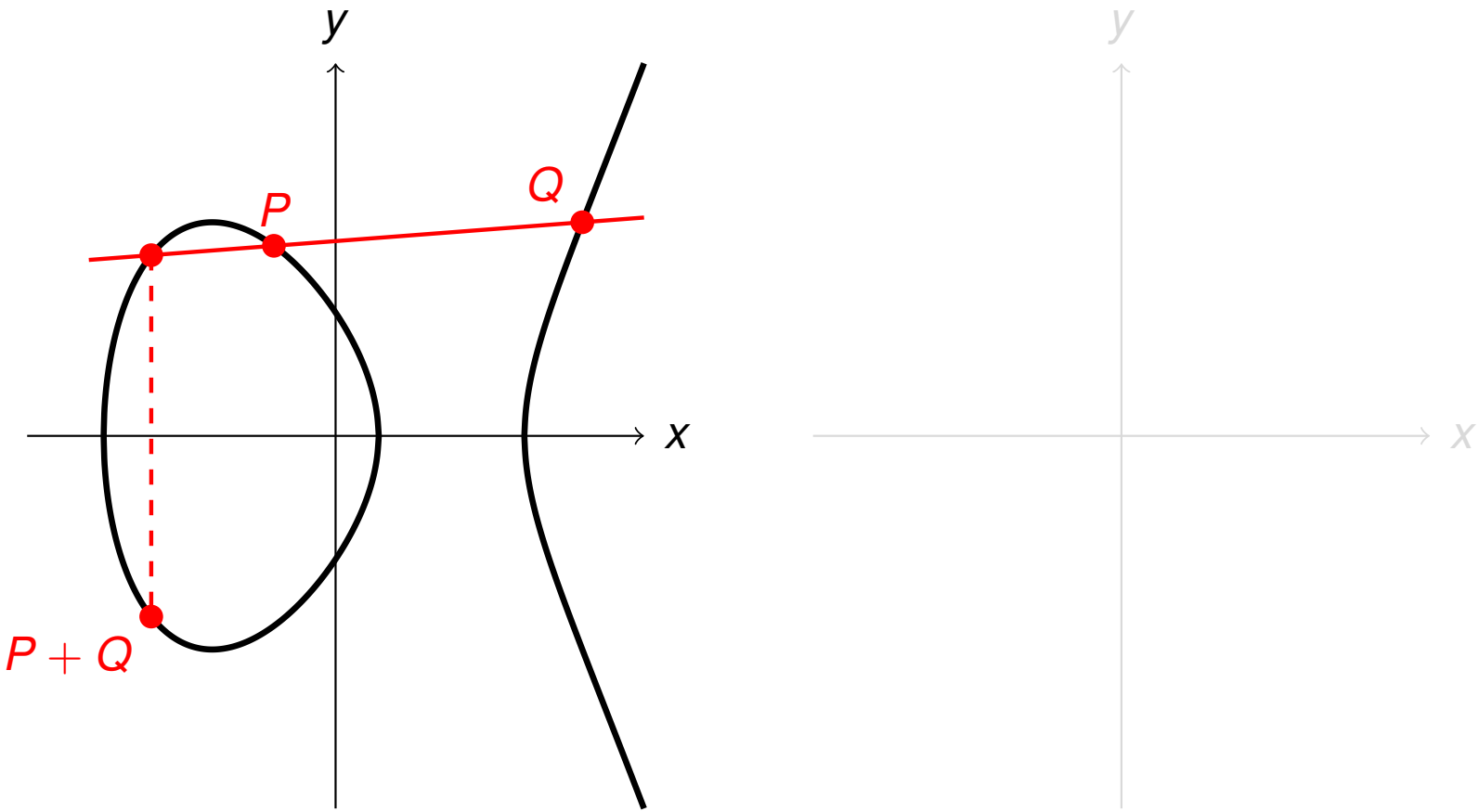

(a) Addition




(b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

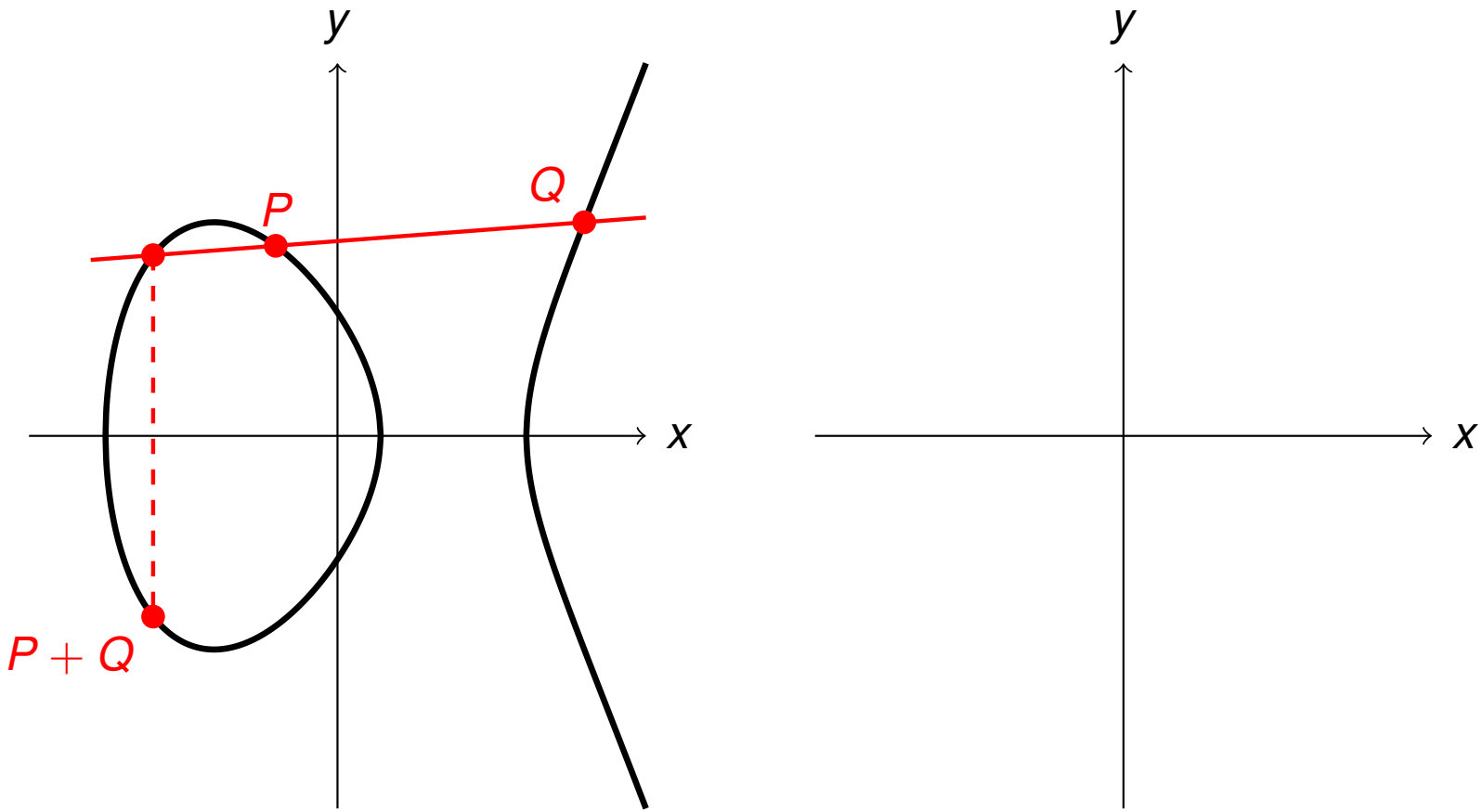
# Geometrische Interpretation des Gruppengesetzes




(a) Addition (b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

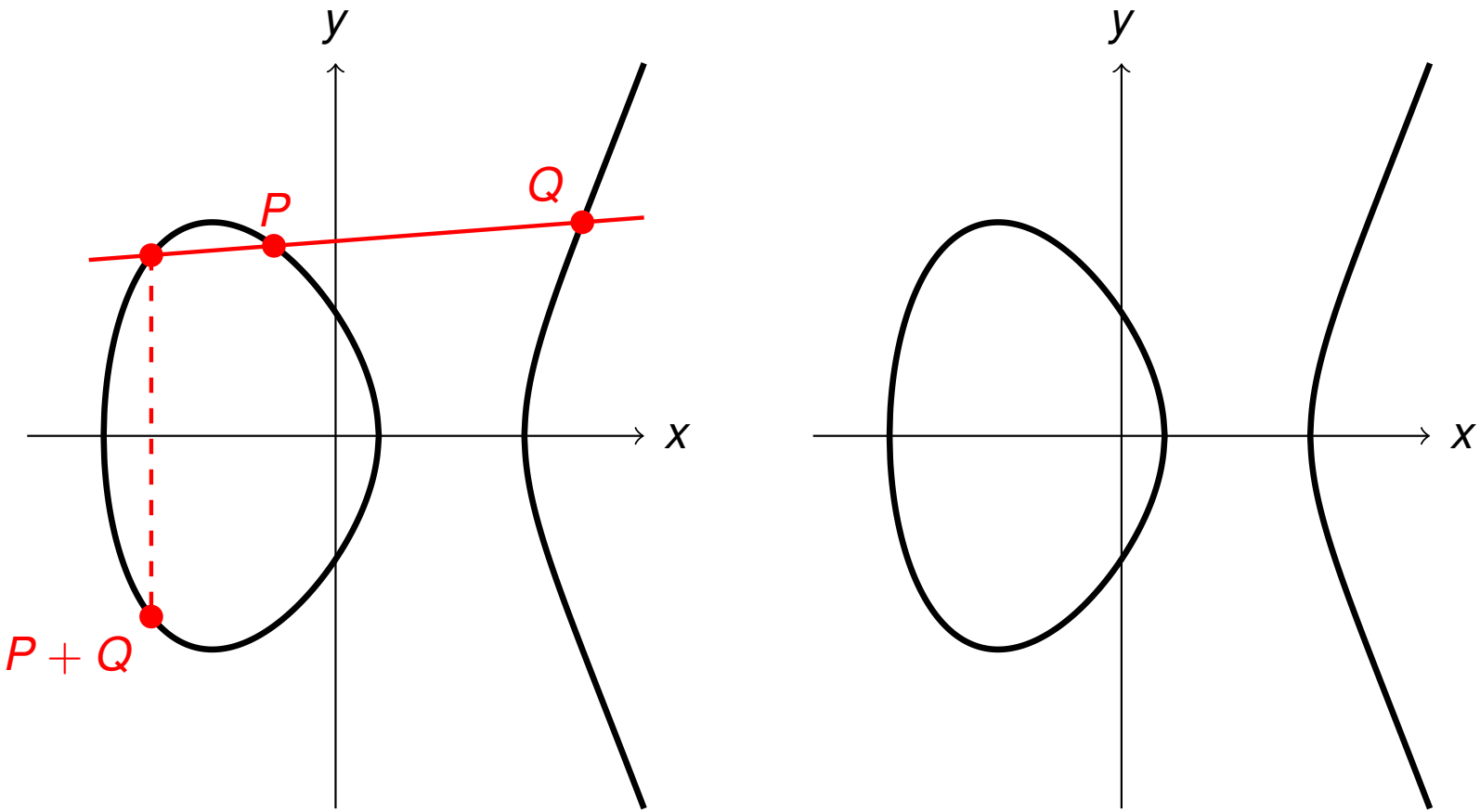
# Geometrische Interpretation des Gruppengesetzes




(a) Addition (b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

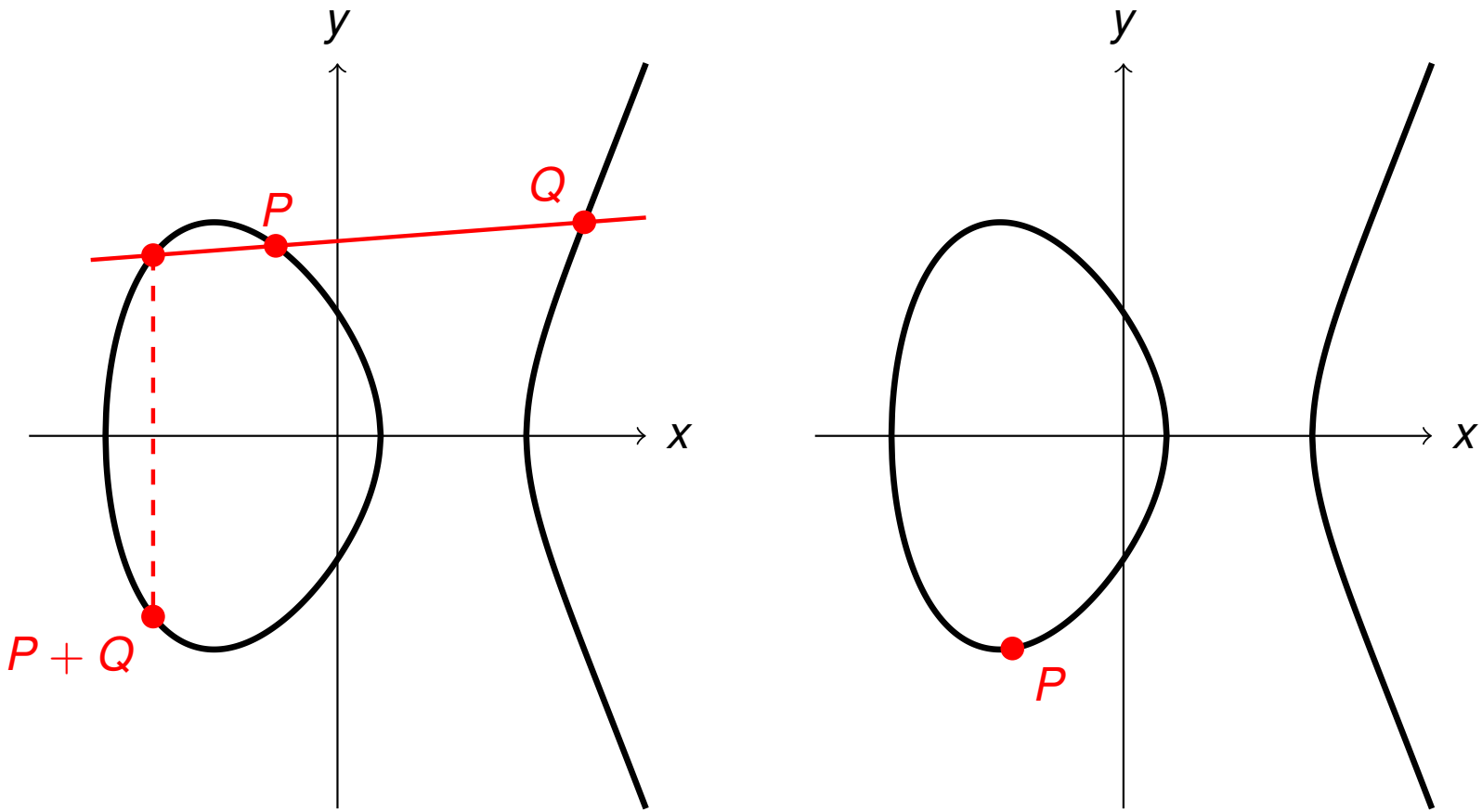
# Geometrische Interpretation des Gruppengesetzes




(a) Addition (b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

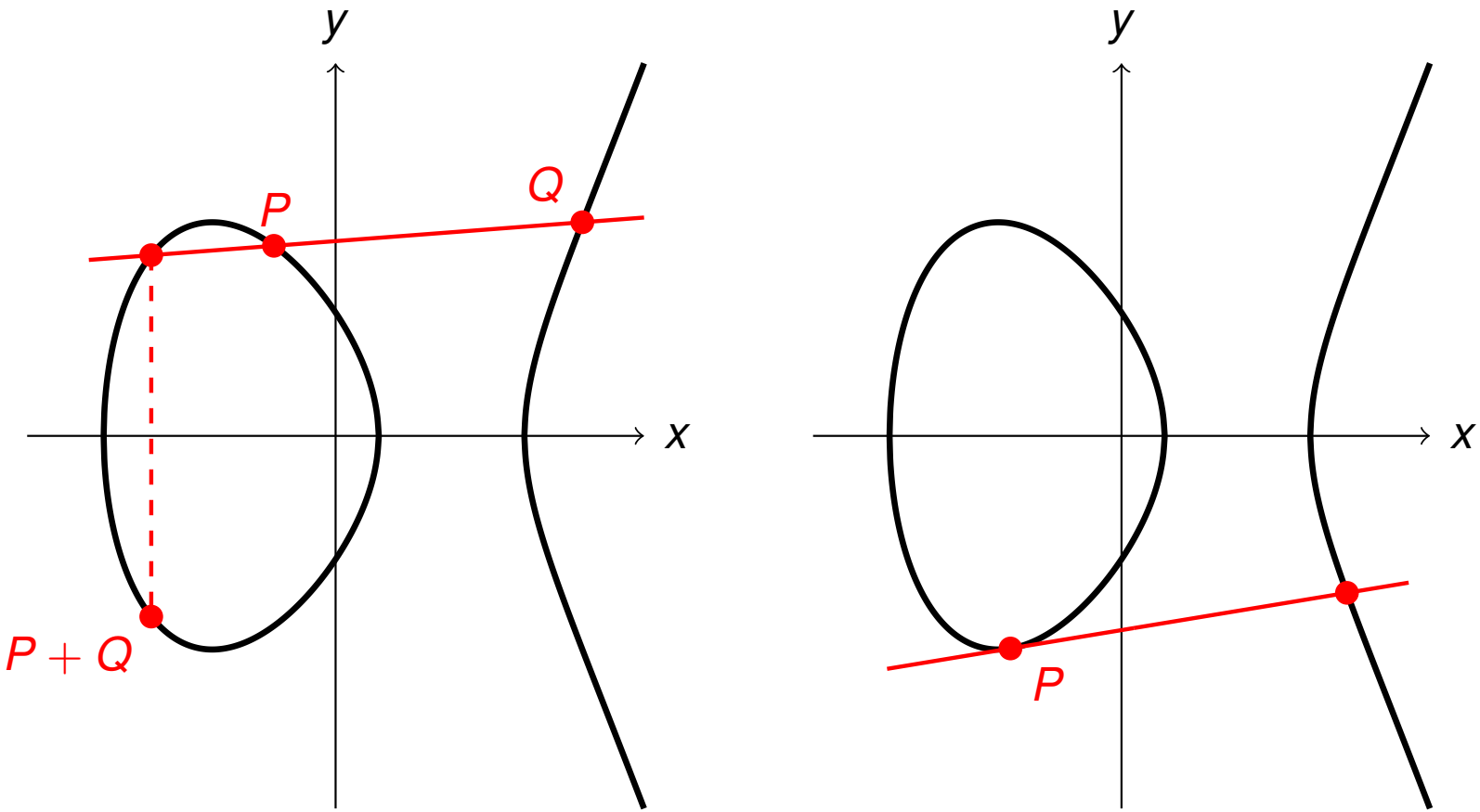
# Geometrische Interpretation des Gruppengesetzes




(a) Addition (b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

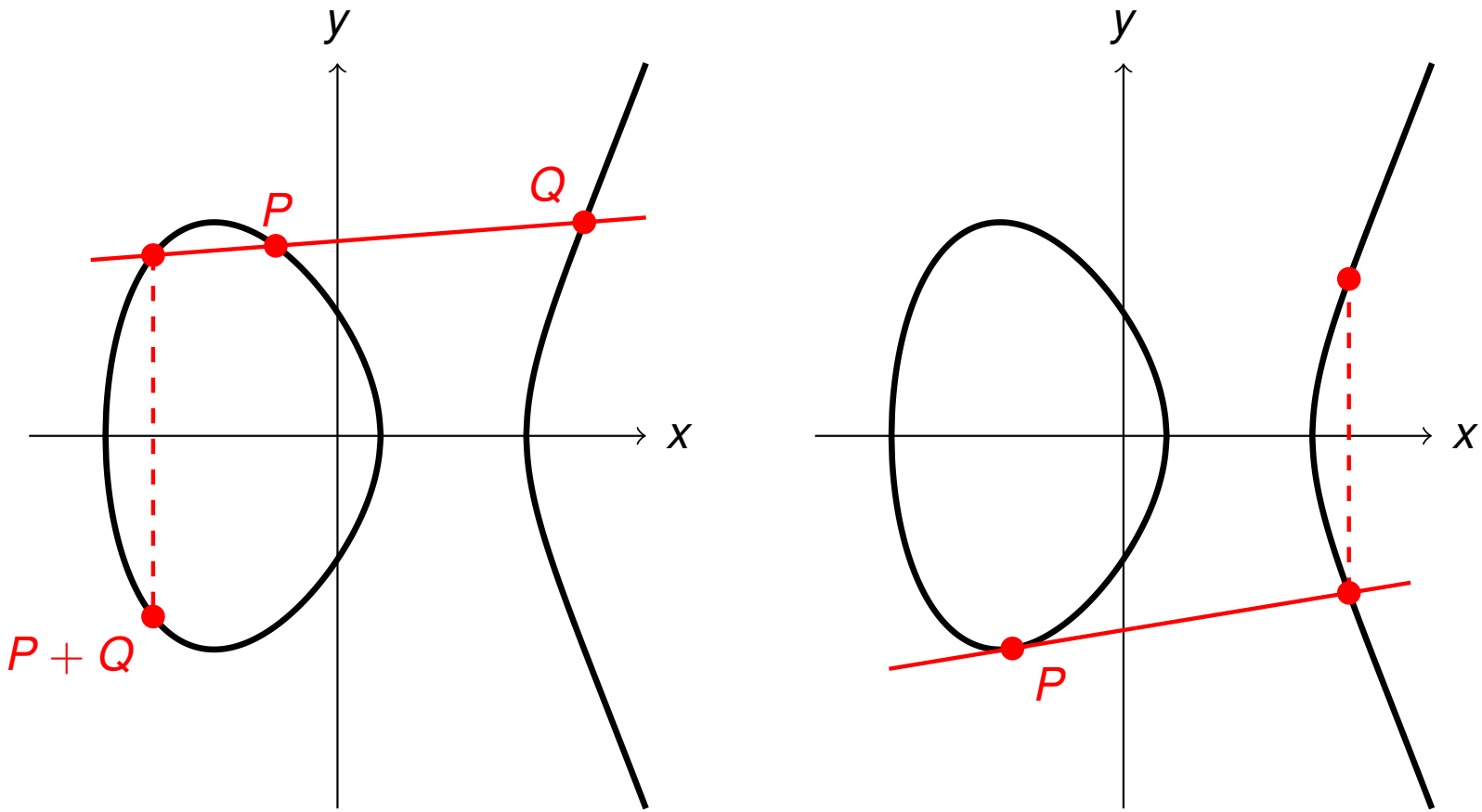
# Geometrische Interpretation des Gruppengesetzes




(a) Addition (b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

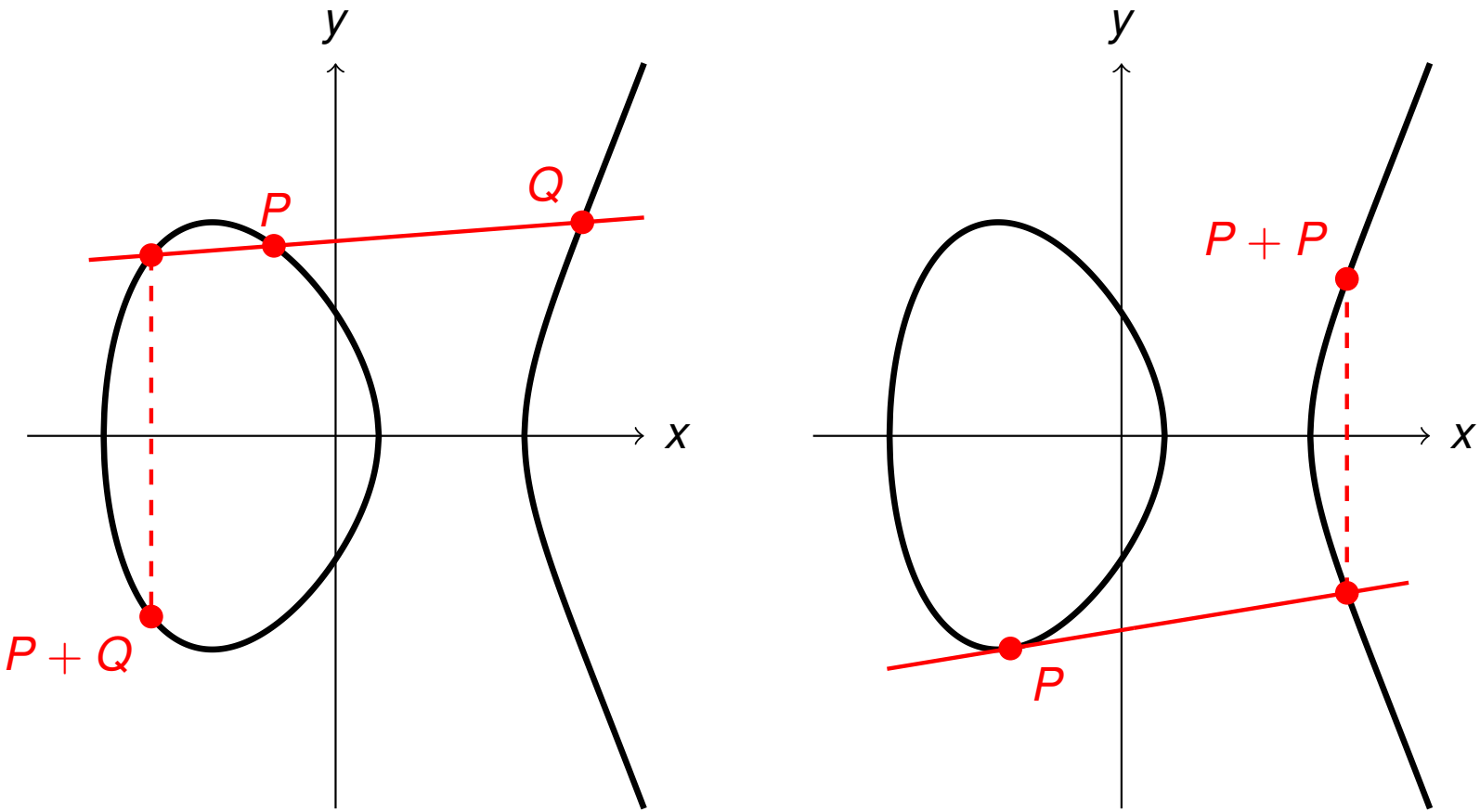
# Geometrische Interpretation des Gruppengesetzes




(a) Addition (b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

# Geometrische Interpretation des Gruppengesetzes




(a) Addition (b) Verdoppelung

Abbildung : Das Gruppengesetz auf elliptischen Kurven

# Elliptische Kurven in der Kryptographie

Sei $p \geq 5$ eine Primzahl. Den endlichen Körper mit $q := p^n$ Elementen bezeichnen wir mit $\mathbb{F}_q$. Sei weiter $E/\mathbb{F}_q$ eine elliptische Kurve. Es gilt offenbar $\#E(\mathbb{F}_q) < \infty$.

# Elliptische Kurven in der Kryptographie

Sei $p \geq 5$ eine Primzahl. Den endlichen Körper mit $q := p^n$ Elementen bezeichnen wir mit $\mathbb{F}_q$. Sei weiter $E/\mathbb{F}_q$ eine elliptische Kurve. Es gilt offenbar $\#E(\mathbb{F}_q) < \infty$.

## *Elliptic Curve Discrete Logarithm Problem*

*Gegeben*: $P, Q \in E(\mathbb{F}_q)$ mit $P \in \{\mathcal{O}, Q, 2Q, 3Q, \ldots\}$.
*Gesucht*: $k \in \mathbb{N}$, so dass $P = kQ$.

# Elliptische Kurven in der Kryptographie

Sei $p \geq 5$ eine Primzahl. Den endlichen Körper mit $q := p^n$ Elementen bezeichnen wir mit $\mathbb{F}_q$. Sei weiter $E/\mathbb{F}_q$ eine elliptische Kurve. Es gilt offenbar $\#E(\mathbb{F}_q) < \infty$.

## *Elliptic Curve Discrete Logarithm Problem*

*Gegeben*: $P, Q \in E(\mathbb{F}_q)$ mit $P \in \{\mathcal{O}, Q, 2Q, 3Q, \ldots\}$.
*Gesucht*: $k \in \mathbb{N}$, so dass $P = kQ$.

Das ECDLP ist Grundlage für

- Schlüsselaustausch (*Diffie-Hellman Key Exchange*),
- Verschlüsselung (*ElGamal Encryption*),
- digitale Signaturen und Hashfunktionen.

# Elliptische Kurven in der Kryptographie

Sei $p \geq 5$ eine Primzahl. Den endlichen Körper mit $q := p^n$ Elementen bezeichnen wir mit $\mathbb{F}_q$. Sei weiter $E/\mathbb{F}_q$ eine elliptische Kurve. Es gilt offenbar $\#E(\mathbb{F}_q) < \infty$.

## *Elliptic Curve Discrete Logarithm Problem*

*Gegeben*: $P, Q \in E(\mathbb{F}_q)$ mit $P \in \{\mathcal{O}, Q, 2Q, 3Q, \ldots\}$.
*Gesucht*: $k \in \mathbb{N}$, so dass $P = kQ$.

Das ECDLP ist Grundlage für

- Schlüsselaustausch (*Diffie-Hellman Key Exchange*),
- Verschlüsselung (*ElGamal Encryption*),
- digitale Signaturen und Hashfunktionen.

# Elliptische Kurven in der Kryptographie

Sei $p \geq 5$ eine Primzahl. Den endlichen Körper mit $q := p^n$ Elementen bezeichnen wir mit $\mathbb{F}_q$. Sei weiter $E/\mathbb{F}_q$ eine elliptische Kurve. Es gilt offenbar $\#E(\mathbb{F}_q) < \infty$.

## *Elliptic Curve Discrete Logarithm Problem*

*Gegeben*: $P, Q \in E(\mathbb{F}_q)$ mit $P \in \{\mathcal{O}, Q, 2Q, 3Q, \ldots\}$.
*Gesucht*: $k \in \mathbb{N}$, so dass $P = kQ$.

Das ECDLP ist Grundlage für

- Schlüsselaustausch (*Diffie-Hellman Key Exchange*),
- Verschlüsselung (*ElGamal Encryption*),
- digitale Signaturen und Hashfunktionen.

# Elliptische Kurven in der Kryptographie

Sei $p \geq 5$ eine Primzahl. Den endlichen Körper mit $q := p^n$ Elementen bezeichnen wir mit $\mathbb{F}_q$. Sei weiter $E/\mathbb{F}_q$ eine elliptische Kurve. Es gilt offenbar $\#E(\mathbb{F}_q) < \infty$.

## *Elliptic Curve Discrete Logarithm Problem*

*Gegeben*: $P, Q \in E(\mathbb{F}_q)$ mit $P \in \{\mathcal{O}, Q, 2Q, 3Q, \ldots\}$.
*Gesucht*: $k \in \mathbb{N}$, so dass $P = kQ$.

Das ECDLP ist Grundlage für

- Schlüsselaustausch (*Diffie-Hellman Key Exchange*),
- Verschlüsselung (*ElGamal Encryption*),
- digitale Signaturen und Hashfunktionen.

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

*Idee*: Man zählt alle konstruierbaren Punkte.
Sei dazu $c \in \mathbb{F}_q$ und $g(x) := x^3 + ax + b$.

- Falls $g(c) = 0$, so gilt $(c, 0) \in E(\mathbb{F}_q)$.
- Falls $g(c) = d^2$ $(d \in \mathbb{F}_q^*)$, so gilt $(c, \pm d) \in E(\mathbb{F}_q)$.

Dieses Verfahren ist nur für kleine endliche Körper praktikabel!

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

*Idee*: Man zählt alle konstruierbaren Punkte.
Sei dazu $c \in \mathbb{F}_q$ und $g(x) := x^3 + ax + b$.

- Falls $g(c) = 0$, so gilt $(c, 0) \in E(\mathbb{F}_q)$.
- Falls $g(c) = d^2$ $(d \in \mathbb{F}_q^*)$, so gilt $(c, \pm d) \in E(\mathbb{F}_q)$.

Dieses Verfahren ist nur für kleine endliche Körper praktikabel!

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

*Idee*: Man zählt alle konstruierbaren Punkte.
Sei dazu $c \in \mathbb{F}_q$ und $g(x) := x^3 + ax + b$.

- Falls $g(c) = 0$, so gilt $(c, 0) \in E(\mathbb{F}_q)$.
- Falls $g(c) = d^2$ $(d \in \mathbb{F}_q^*)$, so gilt $(c, \pm d) \in E(\mathbb{F}_q)$.

Dieses Verfahren ist nur für kleine endliche Körper praktikabel!

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

*Idee*: Man zählt alle konstruierbaren Punkte.
Sei dazu $c \in \mathbb{F}_q$ und $g(x) := x^3 + ax + b$.

- Falls $g(c) = 0$, so gilt $(c, 0) \in E(\mathbb{F}_q)$.
- Falls $g(c) = d^2$ $(d \in \mathbb{F}_q^*)$, so gilt $(c, \pm d) \in E(\mathbb{F}_q)$.

Dieses Verfahren ist nur für kleine endliche Körper praktikabel!

**Beispiel** ($\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, $E/\mathbb{F}_5 : \; y^2 = g(x) = x^3 + 2$)

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

*Idee*: Man zählt alle konstruierbaren Punkte.
Sei dazu $c \in \mathbb{F}_q$ und $g(x) := x^3 + ax + b$.

- Falls $g(c) = 0$, so gilt $(c, 0) \in E(\mathbb{F}_q)$.
- Falls $g(c) = d^2$ $(d \in \mathbb{F}_q^*)$, so gilt $(c, \pm d) \in E(\mathbb{F}_q)$.

Dieses Verfahren ist nur für kleine endliche Körper praktikabel!

**Beispiel** ($\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, $E/\mathbb{F}_5 : \; y^2 = g(x) = x^3 + 2$)

$g(0) = 2,\; g(1) = 3,\; g(2) = 0,\; g(3) = 4 = 2^2,\; g(4) = 1 = 1^2$

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

*Idee*: Man zählt alle konstruierbaren Punkte.
Sei dazu $c \in \mathbb{F}_q$ und $g(x) := x^3 + ax + b$.

- Falls $g(c) = 0$, so gilt $(c, 0) \in E(\mathbb{F}_q)$.
- Falls $g(c) = d^2$ $(d \in \mathbb{F}_q^*)$, so gilt $(c, \pm d) \in E(\mathbb{F}_q)$.

Dieses Verfahren ist nur für kleine endliche Körper praktikabel!

**Beispiel** ($\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, $E/\mathbb{F}_5 : \; y^2 = g(x) = x^3 + 2$)

$g(0) = 2, \; g(1) = 3, \; g(2) = 0, \; g(3) = 4 = 2^2, \; g(4) = 1 = 1^2$

$E(\mathbb{F}_5) = \{\mathcal{O}\} \cup \{ \qquad \}$

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

*Idee*: Man zählt alle konstruierbaren Punkte.
Sei dazu $c \in \mathbb{F}_q$ und $g(x) := x^3 + ax + b$.

- Falls $g(c) = 0$, so gilt $(c, 0) \in E(\mathbb{F}_q)$.
- Falls $g(c) = d^2$ $(d \in \mathbb{F}_q^*)$, so gilt $(c, \pm d) \in E(\mathbb{F}_q)$.

Dieses Verfahren ist nur für kleine endliche Körper praktikabel!

**Beispiel** ($\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, $E/\mathbb{F}_5 : \; y^2 = g(x) = x^3 + 2$)

$g(0) = 2, \; g(1) = 3, \; g(2) = 0, \; g(3) = 4 = 2^2, \; g(4) = 1 = 1^2$

$E(\mathbb{F}_5) = \{\mathcal{O}\} \cup \{(2, 0) \qquad\qquad\qquad\qquad\}$

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

*Idee*: Man zählt alle konstruierbaren Punkte.
Sei dazu $c \in \mathbb{F}_q$ und $g(x) := x^3 + ax + b$.

- Falls $g(c) = 0$, so gilt $(c, 0) \in E(\mathbb{F}_q)$.
- Falls $g(c) = d^2$ $(d \in \mathbb{F}_q^*)$, so gilt $(c, \pm d) \in E(\mathbb{F}_q)$.

Dieses Verfahren ist nur für kleine endliche Körper praktikabel!

**Beispiel** ($\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, $E/\mathbb{F}_5 : \; y^2 = g(x) = x^3 + 2$)

$g(0) = 2, \; g(1) = 3, \; g(2) = 0, \; g(3) = 4 = 2^2, \; g(4) = 1 = 1^2$

$E(\mathbb{F}_5) = \{\mathcal{O}\} \cup \{(2, 0), (3, \pm 2) \qquad\}$

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

*Idee*: Man zählt alle konstruierbaren Punkte.
Sei dazu $c \in \mathbb{F}_q$ und $g(x) := x^3 + ax + b$.

- Falls $g(c) = 0$, so gilt $(c, 0) \in E(\mathbb{F}_q)$.
- Falls $g(c) = d^2$ $(d \in \mathbb{F}_q^*)$, so gilt $(c, \pm d) \in E(\mathbb{F}_q)$.

Dieses Verfahren ist nur für kleine endliche Körper praktikabel!

**Beispiel** ($\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, $E/\mathbb{F}_5 : \; y^2 = g(x) = x^3 + 2$)

$g(0) = 2, \; g(1) = 3, \; g(2) = 0, \; g(3) = 4 = 2^2, \; g(4) = 1 = 1^2$

$E(\mathbb{F}_5) = \{\mathcal{O}\} \cup \{(2, 0), (3, \pm 2), (4, \pm 1)\}$

# Triviale Bestimmung der Gruppenordnung

Die kryptographische Eignung von $E$ hängt vor allem von der Gruppenordnung $\#E(\mathbb{F}_q)$ ab. Wie berechnet man diese?

*Idee*: Man zählt alle konstruierbaren Punkte.
Sei dazu $c \in \mathbb{F}_q$ und $g(x) := x^3 + ax + b$.

- Falls $g(c) = 0$, so gilt $(c, 0) \in E(\mathbb{F}_q)$.
- Falls $g(c) = d^2$ $(d \in \mathbb{F}_q^*)$, so gilt $(c, \pm d) \in E(\mathbb{F}_q)$.

Dieses Verfahren ist nur für kleine endliche Körper praktikabel!

**Beispiel** ($\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, $E/\mathbb{F}_5 : \; y^2 = g(x) = x^3 + 2$)

$g(0) = 2, \; g(1) = 3, \; g(2) = 0, \; g(3) = 4 = 2^2, \; g(4) = 1 = 1^2$

$E(\mathbb{F}_5) = \{\mathcal{O}\} \cup \{(2, 0), (3, \pm 2), (4, \pm 1)\}$

$\#E(\mathbb{F}_5) = 1 + 1 + 2 + 2 = 6$

# Eine Isogenie ist eine spezielle Abbildung $E \to E'$.

Seien $E$ und $E'$ elliptische Kurven über $K$.

# Eine Isogenie ist eine spezielle Abbildung $E \to E'$.

Seien $E$ und $E'$ elliptische Kurven über $K$.

## Definition

Eine Isogenie ist ein Homomorphismus $\phi : E \to E'$, der durch rationale Funktionen gegeben ist, d. h.

- $\phi(P + Q) = \phi(P) + \phi(Q)$ und
- es gibt $r, s \in \overline{K}(X)$, so dass $\phi(\ (x, y)\ ) = (r(x), s(x) \cdot y)$ für alle $(x, y) \in E \setminus \ker \phi$.

# Eine Isogenie ist eine spezielle Abbildung $E \to E'$.

Seien $E$ und $E'$ elliptische Kurven über $K$.

## Definition

Eine Isogenie ist ein Homomorphismus $\phi : E \to E'$, der durch rationale Funktionen gegeben ist, d. h.

- $\phi(P + Q) = \phi(P) + \phi(Q)$ und
- es gibt $r, s \in \overline{K}(X)$, so dass $\phi(\ (x, y)\ ) = (r(x), s(x) \cdot y)$ für alle $(x, y) \in E \setminus \ker \phi$.

Im Fall $E = E'$ heißt eine Isogenie auch Endomorphismus.

# Eine Isogenie ist eine spezielle Abbildung $E \to E'$.

Seien $E$ und $E'$ elliptische Kurven über $K$.

## Definition

Eine Isogenie ist ein Homomorphismus $\phi : E \to E'$, der durch rationale Funktionen gegeben ist, d. h.

- $\phi(P + Q) = \phi(P) + \phi(Q)$ und
- es gibt $r, s \in \overline{K}(X)$, so dass $\phi(\ (x, y)\ ) = (r(x), s(x) \cdot y)$ für alle $(x, y) \in E \setminus \ker \phi$.

Im Fall $E = E'$ heißt eine Isogenie auch Endomorphismus.

Schreibt man $r = v/w$ (teilerfremde Polynome), so heißt $\deg(\phi) := \max(\deg(v), \deg(w))$ der Grad von $\phi$.

# Eine Isogenie ist eine spezielle Abbildung $E \to E'$.

Seien $E$ und $E'$ elliptische Kurven über $K$.

## Definition

Eine Isogenie ist ein Homomorphismus $\phi: E \to E'$, der durch rationale Funktionen gegeben ist, d. h.

- $\phi(P+Q) = \phi(P) + \phi(Q)$ und
- es gibt $r, s \in \overline{K}(X)$, so dass $\phi(\,(x,y)\,) = (r(x), s(x)\cdot y)$ für alle $(x,y) \in E \setminus \ker\phi$.

Im Fall $E = E'$ heißt eine Isogenie auch Endomorphismus.

Schreibt man $r = v/w$ (teilerfremde Polynome), so heißt $\deg(\phi) := \max(\deg(v), \deg(w))$ der Grad von $\phi$.

Menge aller Isogenien $E \to E'$: $\mathrm{Hom}(E, E')$ (Gruppe mit $+$).
Menge aller Isogenien $E \to E$ : $\mathrm{End}(E)$ (Ring mit $+, \circ$).

# Eine Isogenie ist eine spezielle Abbildung $E \to E'$.

Seien $E$ und $E'$ elliptische Kurven über $K$.

## Definition

Eine Isogenie ist ein Homomorphismus $\phi: E \to E'$, der durch rationale Funktionen gegeben ist, d. h.

- $\phi(P+Q) = \phi(P) + \phi(Q)$ und
- es gibt $r, s \in \overline{K}(X)$, so dass $\phi(\,(x,y)\,) = (r(x), s(x)\cdot y)$ für alle $(x,y) \in E \setminus \ker\phi$.

Im Fall $E = E'$ heißt eine Isogenie auch Endomorphismus.

Schreibt man $r = v/w$ (teilerfremde Polynome), so heißt $\deg(\phi) := \max(\deg(v), \deg(w))$ der Grad von $\phi$.

Menge aller Isogenien $E \to E'$: $\mathrm{Hom}(E, E')$ (Gruppe mit $+$).
Menge aller Isogenien $E \to E$ : $\mathrm{End}(E)$ (Ring mit $+, \circ$).

# Divisionspolynome beschreiben den Kern von $[m]$.

## Beispiel

Für $m \in \mathbb{Z}$ ist $[m]: \ E \to E, \ P \mapsto mP$ ein Endomorphismus.
Man nennt $P \in \ker[m] = \{P \in E: \ mP = \mathcal{O}\}$ Torsionspunkt.

# Divisionspolynome beschreiben den Kern von $[m]$.

## Beispiel

Für $m \in \mathbb{Z}$ ist $[m]: E \to E,\ P \mapsto mP$ ein Endomorphismus.
Man nennt $P \in \ker[m] = \{P \in E : mP = \mathcal{O}\}$ Torsionspunkt.

Sei $m \geq 1$. Es gibt Polynome $\psi_m, \theta_m, \omega_m \in K[X, Y]$, so dass

$$mP = \left(\frac{\theta_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)}\right) \text{ für alle } P \in E \setminus \ker[m].$$

Das Polynom $\psi_m$ heißt $m$-tes Divisionspolynom.

# Divisionspolynome beschreiben den Kern von $[m]$.

## Beispiel

Für $m \in \mathbb{Z}$ ist $[m]: E \to E,\ P \mapsto mP$ ein Endomorphismus.
Man nennt $P \in \ker[m] = \{P \in E : mP = \mathcal{O}\}$ Torsionspunkt.

Sei $m \geq 1$. Es gibt Polynome $\psi_m, \theta_m, \omega_m \in K[X, Y]$, so dass

$$mP = \left(\frac{\theta_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)}\right) \text{ für alle } P \in E \setminus \ker[m].$$

Das Polynom $\psi_m$ heißt $m$-tes Divisionspolynom.

## Satz

*Für $\mathcal{O} \neq P \in E$ gilt $mP = \mathcal{O} \iff \psi_m(P) = 0$.*
*Falls m ungerade, so gilt $\psi_m \in K[X]$ und damit sind die Nullstellen des m-ten Divisionspolynoms genau die x-Koordinaten der nicht-trivialen Torsionspunkte.*

# Divisionspolynome in Satohs Algorithmus

In Satohs Algorithmus zur Bestimmung von $\#E(\mathbb{F}_{p^n})$ muss man $p$-te Divisionspolynome berechnen.

*Problem*: $\deg(\psi_p) = O(p^2)$. Die rekursive Berechnung ist zudem aufwändig (keine Details).

# Divisionspolynome in Satohs Algorithmus

In Satohs Algorithmus zur Bestimmung von $\#E(\mathbb{F}_{p^n})$ muss man $p$-te Divisionspolynome berechnen.

*Problem*: $\deg(\psi_p) = O(p^2)$. Die rekursive Berechnung ist zudem aufwändig (keine Details).

James McKee veröffentlichte 1994 Formeln, mit denen sich Vorberechnungen durchführen lassen (erstmalige praktische Anwendung).

Tabelle : Berechnung von $p$-ten Divisionspolynomen in $\mathbb{F}_{p^{23}}$

| $p$ | $\deg(\psi_p)$ | $t_{\text{rekursiv}}$ | $t_{\text{mckee}}$ |
|---|---|---|---|
| 137 | 9 316 | 6,5 sec | 0,1 sec |
| 293 | 42 778 | 31,0 sec | 0,5 sec |

# Divisionspolynome in Satohs Algorithmus

In Satohs Algorithmus zur Bestimmung von $\#E(\mathbb{F}_{p^n})$ muss man $p$-te Divisionspolynome berechnen.

*Problem*: $\deg(\psi_p) = O(p^2)$. Die rekursive Berechnung ist zudem aufwändig (keine Details).

James McKee veröffentlichte 1994 Formeln, mit denen sich Vorberechnungen durchführen lassen (erstmalige praktische Anwendung).

Bei der Suche nach starken Kurven wird eine Early-Abort Strategie mit Hilfe von Divisionspolynomen realisiert.

Tabelle : Berechnung von $p$-ten Divisionspolynomen in $\mathbb{F}_{p^{23}}$

| $p$ | $\deg(\psi_p)$ | $t_{\text{rekursiv}}$ | $t_{\text{mckee}}$ |
|---|---|---|---|
| 137 | 9 316 | 6,5 sec | 0,1 sec |
| 293 | 42 778 | 31,0 sec | 0,5 sec |

# Warum ist McKees Methode so effizient?

$p$-te Divisionspolynome von elliptischen Kurven über $\mathbb{F}_{p^n}$ haben eine spezielle Struktur:

$$\begin{aligned}\mathbb{F}_{p^n}[X] \ni \psi_p(X) &= \left(a_0 + a_1 X + \cdots + a_{\frac{p-1}{2}} X^{\frac{p-1}{2}}\right)^p \\ &= (a_0)^p + (a_1)^p X^p + \cdots + (a_{\frac{p-1}{2}})^p X^{\frac{p(p-1)}{2}}\end{aligned}$$

# Warum ist McKees Methode so effizient?

$p$-te Divisionspolynome von elliptischen Kurven über $\mathbb{F}_{p^n}$ haben eine spezielle Struktur:

$$\begin{aligned}\mathbb{F}_{p^n}[X] \ni \psi_p(X) &= \left(a_0 + a_1 X + \cdots + a_{\frac{p-1}{2}} X^{\frac{p-1}{2}}\right)^p \\ &= (a_0)^p + (a_1)^p X^p + \cdots + (a_{\frac{p-1}{2}})^p X^{\frac{p(p-1)}{2}}\end{aligned}$$

Mit Hilfe von McKees Formeln kann man alle Koeffizienten direkt berechnen (zusätzlich Vorberechnungen möglich).

# Warum ist McKees Methode so effizient?

$p$-te Divisionspolynome von elliptischen Kurven über $\mathbb{F}_{p^n}$ haben eine spezielle Struktur:

$$\begin{aligned}\mathbb{F}_{p^n}[X] \ni \psi_p(X) &= \left(a_0 + a_1 X + \cdots + a_{\frac{p-1}{2}} X^{\frac{p-1}{2}}\right)^p \\ &= (a_0)^p + (a_1)^p X^p + \cdots + (a_{\frac{p-1}{2}})^p X^{\frac{p(p-1)}{2}}\end{aligned}$$

Mit Hilfe von McKees Formeln kann man alle Koeffizienten direkt berechnen (zusätzlich Vorberechnungen möglich).

Die obige Darstellung ist für die rekursive Berechnung nutzlos.

# Duale Isogenie und Spur eines Endomorphismus

## Satz

*Sei $\phi: E \to E'$ eine nicht-triviale Isogenie. Dann gibt es genau eine Isogenie $\widehat{\phi}: E' \to E$ (die zu $\phi$ duale Isogenie) mit*

$$\widehat{\phi} \circ \phi = [\deg(\phi)] \in \mathrm{End}(E)$$

# Duale Isogenie und Spur eines Endomorphismus

## Satz

*Sei $\phi: E \to E'$ eine nicht-triviale Isogenie. Dann gibt es genau eine Isogenie $\widehat{\phi}: E' \to E$ (die zu $\phi$ duale Isogenie) mit*

$$\widehat{\phi} \circ \phi = [\deg(\phi)] \in \mathrm{End}(E)$$

Sei $\phi$ ein Endomorphismus. Die Spur von $\phi$ ist definiert als

$$\mathrm{Tr}(\phi) := \phi + \widehat{\phi} \in \mathrm{End}(E).$$

# Duale Isogenie und Spur eines Endomorphismus

## Satz

*Sei $\phi: E \to E'$ eine nicht-triviale Isogenie. Dann gibt es genau eine Isogenie $\widehat{\phi}: E' \to E$ (die zu $\phi$ duale Isogenie) mit*

$$\widehat{\phi} \circ \phi = [\deg(\phi)] \in \mathrm{End}(E)$$

Sei $\phi$ ein Endomorphismus. Die Spur von $\phi$ ist definiert als

$$\mathrm{Tr}(\phi) := \phi + \widehat{\phi} \in \mathrm{End}(E).$$

## Lemma

*Die Spur eines Endomorphismus ist eine ganze Zahl, d. h. es existiert ein $m \in \mathbb{Z}$, so dass $\mathrm{Tr}(\phi) = [m]$.*

# Der Frobenius-Endomorphismus

## Erinnerung

In $\mathbb{F}_{p^n}$ gilt $(c+d)^p = c^p + d^p$ und $c^{(p^n)} = c$.

# Der Frobenius-Endomorphismus

## Erinnerung

In $\mathbb{F}_{p^n}$ gilt $(c+d)^p = c^p + d^p$ und $c^{(p^n)} = c$.

Sei $E$ eine elliptische Kurve über $\mathbb{F}_{p^n}$. Für $k \in \mathbb{N}$ ist dann auch $E^{(k)}: \; y^2 = x^3 + a^{(p^k)}x + b^{(p^k)}$ eine elliptische Kurve.

# Der Frobenius-Endomorphismus

## Erinnerung

In $\mathbb{F}_{p^n}$ gilt $(c+d)^p = c^p + d^p$ und $c^{(p^n)} = c$.

Sei $E$ eine elliptische Kurve über $\mathbb{F}_{p^n}$. Für $k \in \mathbb{N}$ ist dann auch $E^{(k)}: \; y^2 = x^3 + a^{(p^k)}x + b^{(p^k)}$ eine elliptische Kurve.

Die Abbildung

$$\phi_p: \; E^{(k)} \to E^{(k+1)}, \; \begin{cases} \mathcal{O} & \mapsto \mathcal{O} \\ (x,y) & \mapsto (x^p, y^p) \end{cases}$$

ist eine Isogenie.

# Der Frobenius-Endomorphismus

## Erinnerung

In $\mathbb{F}_{p^n}$ gilt $(c+d)^p = c^p + d^p$ und $c^{(p^n)} = c$.

Sei $E$ eine elliptische Kurve über $\mathbb{F}_{p^n}$. Für $k \in \mathbb{N}$ ist dann auch $E^{(k)}: \; y^2 = x^3 + a^{(p^k)}x + b^{(p^k)}$ eine elliptische Kurve.

Die Abbildung

$$\phi_p: \; E^{(k)} \to E^{(k+1)}, \begin{cases} \mathcal{O} & \mapsto \mathcal{O} \\ (x,y) & \mapsto (x^p, y^p) \end{cases}$$

ist eine Isogenie. Man erhält folgenden Zyklus:

$$E = E^{(0)} \xrightarrow{\phi_p} E^{(1)} \xrightarrow{\phi_p} \dots \xrightarrow{\phi_p} E^{(n-1)} \xrightarrow{\phi_p} E^{(n)} = E.$$

# Der Frobenius-Endomorphismus

## Erinnerung

In $\mathbb{F}_{p^n}$ gilt $(c+d)^p = c^p + d^p$ und $c^{(p^n)} = c$.

Sei $E$ eine elliptische Kurve über $\mathbb{F}_{p^n}$. Für $k \in \mathbb{N}$ ist dann auch $E^{(k)}: \; y^2 = x^3 + a^{(p^k)}x + b^{(p^k)}$ eine elliptische Kurve.

Die Abbildung

$$\phi_p: \; E^{(k)} \to E^{(k+1)}, \begin{cases} \mathcal{O} & \mapsto \mathcal{O} \\ (x,y) & \mapsto (x^p, y^p) \end{cases}$$

ist eine Isogenie. Man erhält folgenden Zyklus:

$$E = E^{(0)} \xrightarrow{\phi_p} E^{(1)} \xrightarrow{\phi_p} \dots \xrightarrow{\phi_p} E^{(n-1)} \xrightarrow{\phi_p} E^{(n)} = E.$$

$\phi_{p^n} := \phi_p \circ \dots \circ \phi_p \in \mathrm{End}(E)$ heißt Frobenius-Endomorphismus.

# Die Spur des Frobenius bestimmt $\#E(\mathbb{F}_q)$.

*Bemerkung:* Der Frobenius(-Endomorphismus) ist auf $E(\mathbb{F}_q)$ die Identität: $(x, y) \mapsto (x^q, y^q) = (x, y)$. Nicht aber auf $E = E(\overline{\mathbb{F}}_q)$!

# Die Spur des Frobenius bestimmt $\#E(\mathbb{F}_q)$.

*Bemerkung:* Der Frobenius(-Endomorphismus) ist auf $E(\mathbb{F}_q)$ die Identität: $(x, y) \mapsto (x^q, y^q) = (x, y)$. Nicht aber auf $E = E(\overline{\mathbb{F}}_q)$!

**Satz**

$$\#E(\mathbb{F}_q) = q + 1 - \mathrm{Tr}(\phi_q)$$

Kennt man also die Spur des Frobenius, so kennt man die Gruppenordnung!

# Die Spur des Frobenius bestimmt $\#E(\mathbb{F}_q)$.

*Bemerkung:* Der Frobenius(-Endomorphismus) ist auf $E(\mathbb{F}_q)$ die Identität: $(x, y) \mapsto (x^q, y^q) = (x, y)$. Nicht aber auf $E = E(\overline{\mathbb{F}}_q)$!

**Satz**

$$\#E(\mathbb{F}_q) = q + 1 - \mathrm{Tr}(\phi_q)$$

Kennt man also die Spur des Frobenius, so kennt man die Gruppenordnung!

Es gilt folgende Abschätzung:

**Satz (Hasse)**

$$\left|\mathrm{Tr}(\phi_q)\right| \leq 2\sqrt{q}$$

# Satoh berechnet die Spur des Frobenius modulo $p^N$.

Die obigen Überlegungen sind der Ausgangspunkt für alle effizienten Punktezählalgorithmen.

- Der SEA-Algorithmus (Schoof, Elkies, Atkin) berechnet $\mathrm{Tr}(\phi_q)$ modulo vieler Primzahlen und rekonstruiert den Wert mit Hilfe des chinesischen Restsatz.

  *Zeitkomplexität*: $O(\log^{4+\varepsilon} q)$.

- Satoh hingegen wählt $N \geq 1$ genügend groß (Hasse!) und bestimmt $\mathrm{Tr}(\phi_q)$ modulo $p^N$ ($p$ die Charakteristik von $\mathbb{F}_q$).

  *Zeitkomplexität*: $O(\log^{3+\varepsilon} q)$ (Konstante hängt stark von $p$ ab, nur für kleine Charakteristiken praktikabel)

# Satoh berechnet die Spur des Frobenius modulo $p^N$.

Die obigen Überlegungen sind der Ausgangspunkt für alle effizienten Punktezählalgorithmen.

- Der SEA-Algorithmus (Schoof, Elkies, Atkin) berechnet $\mathrm{Tr}(\phi_q)$ modulo vieler Primzahlen und rekonstruiert den Wert mit Hilfe des chinesischen Restsatz.

  *Zeitkomplexität*: $O(\log^{4+\varepsilon} q)$.

- Satoh hingegen wählt $N \geq 1$ genügend groß (Hasse!) und bestimmt $\mathrm{Tr}(\phi_q)$ modulo $p^N$ ($p$ die Charakteristik von $\mathbb{F}_q$).

  *Zeitkomplexität*: $O(\log^{3+\varepsilon} q)$ (Konstante hängt stark von $p$ ab, nur für kleine Charakteristiken praktikabel)

# Satoh berechnet die Spur des Frobenius modulo $p^N$.

Die obigen Überlegungen sind der Ausgangspunkt für alle effizienten Punktezählalgorithmen.

- Der SEA-Algorithmus (Schoof, Elkies, Atkin) berechnet $\mathrm{Tr}(\phi_q)$ modulo vieler Primzahlen und rekonstruiert den Wert mit Hilfe des chinesischen Restsatz.

  *Zeitkomplexität*: $O(\log^{4+\varepsilon} q)$.

- Satoh hingegen wählt $N \geq 1$ genügend groß (Hasse!) und bestimmt $\mathrm{Tr}(\phi_q)$ modulo $p^N$ ($p$ die Charakteristik von $\mathbb{F}_q$).

  *Zeitkomplexität*: $O(\log^{3+\varepsilon} q)$ (Konstante hängt stark von $p$ ab, nur für kleine Charakteristiken praktikabel)

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$.

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$. Die Menge der ganzen $p$-adischen Zahlen heißt $\mathbb{Z}_p$ und wird durch komponentenweise Addition und Multiplikation zu einem Integritätsring.

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$. Die Menge der ganzen $p$-adischen Zahlen heißt $\mathbb{Z}_p$ und wird durch komponentenweise Addition und Multiplikation zu einem Integritätsring.

## Beispiel ($p$-adische Entwicklung ganzer Zahlen)

$7 = (\quad\quad , \quad\quad , \quad\quad , \ldots) = (\ , \ , \ , \ldots) \in \mathbb{Z}_2$

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$. Die Menge der ganzen $p$-adischen Zahlen heißt $\mathbb{Z}_p$ und wird durch komponentenweise Addition und Multiplikation zu einem Integritätsring.

## Beispiel ($p$-adische Entwicklung ganzer Zahlen)

$7 = (7 \bmod 2, \quad , \quad , \ldots) = (1, \ , \ , \ldots) \in \mathbb{Z}_2$

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$. Die Menge der ganzen $p$-adischen Zahlen heißt $\mathbb{Z}_p$ und wird durch komponentenweise Addition und Multiplikation zu einem Integritätsring.

## Beispiel ($p$-adische Entwicklung ganzer Zahlen)

$$7 = (7 \bmod 2, 7 \bmod 4, \quad , \ldots) = (1, 3, \quad , \ldots) \in \mathbb{Z}_2$$

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$. Die Menge der ganzen $p$-adischen Zahlen heißt $\mathbb{Z}_p$ und wird durch komponentenweise Addition und Multiplikation zu einem Integritätsring.

## Beispiel ($p$-adische Entwicklung ganzer Zahlen)

$$7 = (7 \bmod 2, 7 \bmod 4, 7 \bmod 8, \ldots) = (1, 3, 7, \ldots) \in \mathbb{Z}_2$$

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$. Die Menge der ganzen $p$-adischen Zahlen heißt $\mathbb{Z}_p$ und wird durch komponentenweise Addition und Multiplikation zu einem Integritätsring.

## Beispiel ($p$-adische Entwicklung ganzer Zahlen)

$$7 = (7 \bmod 2, 7 \bmod 4, 7 \bmod 8, \ldots) = (1, 3, 7, \ldots) \in \mathbb{Z}_2$$
$$-6 = (\ ,\ \ ,\ \ ,\ \ , \ldots) \in \mathbb{Z}_5$$

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$. Die Menge der ganzen $p$-adischen Zahlen heißt $\mathbb{Z}_p$ und wird durch komponentenweise Addition und Multiplikation zu einem Integritätsring.

## Beispiel ($p$-adische Entwicklung ganzer Zahlen)

$$7 = (7 \bmod 2, 7 \bmod 4, 7 \bmod 8, \ldots) = (1, 3, 7, \ldots) \in \mathbb{Z}_2$$
$$-6 = (4, \quad , \quad , \quad , \ldots) \in \mathbb{Z}_5$$

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$. Die Menge der ganzen $p$-adischen Zahlen heißt $\mathbb{Z}_p$ und wird durch komponentenweise Addition und Multiplikation zu einem Integritätsring.

## Beispiel ($p$-adische Entwicklung ganzer Zahlen)

$$7 = (7 \bmod 2, 7 \bmod 4, 7 \bmod 8, \ldots) = (1, 3, 7, \ldots) \in \mathbb{Z}_2$$
$$-6 = (4, 19, \quad , \quad , \ldots) \in \mathbb{Z}_5$$

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$. Die Menge der ganzen $p$-adischen Zahlen heißt $\mathbb{Z}_p$ und wird durch komponentenweise Addition und Multiplikation zu einem Integritätsring.

## Beispiel ($p$-adische Entwicklung ganzer Zahlen)

$$7 = (7 \bmod 2, 7 \bmod 4, 7 \bmod 8, \ldots) = (1, 3, 7, \ldots) \in \mathbb{Z}_2$$
$$-6 = (4, 19, 119, \quad , \ldots) \in \mathbb{Z}_5$$

# Der Ring $\mathbb{Z}_p$

Sei $p$ eine Primzahl.

## Definition

Eine ganze $p$-adische Zahl ist eine unendliche Folge

$$(x_1, x_2, x_3, \ldots) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^3\mathbb{Z}) \times \cdots,$$

wobei $x_{i+1} \equiv x_i \pmod{p^i}$. Die Menge der ganzen $p$-adischen Zahlen heißt $\mathbb{Z}_p$ und wird durch komponentenweise Addition und Multiplikation zu einem Integritätsring.

## Beispiel ($p$-adische Entwicklung ganzer Zahlen)

$$7 = (7 \bmod 2, 7 \bmod 4, 7 \bmod 8, \ldots) = (1, 3, 7, \ldots) \in \mathbb{Z}_2$$
$$-6 = (4, 19, 119, 619, \ldots) \in \mathbb{Z}_5$$

# Der Körper der $p$-adischen Zahlen

In einer Implementierung genügt es $N \geq 1$ ausreichend groß zu wählen und in $\mathbb{Z}/p^N\mathbb{Z}$ zu rechnen.

# Der Körper der *p*-adischen Zahlen

In einer Implementierung genügt es $N \geq 1$ ausreichend groß zu wählen und in $\mathbb{Z}/p^N\mathbb{Z}$ zu rechnen.

## Definition

$\mathbb{Q}_p := \mathrm{Quot}(\mathbb{Z}_p)$ heißt Körper der *p*-adischen Zahlen.

# Der Körper der $p$-adischen Zahlen

In einer Implementierung genügt es $N \geq 1$ ausreichend groß zu wählen und in $\mathbb{Z}/p^N\mathbb{Z}$ zu rechnen.

## Definition

$\mathbb{Q}_p := \mathrm{Quot}(\mathbb{Z}_p)$ heißt Körper der $p$-adischen Zahlen.

Sei $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(F(X))$, wobei $F(X) = X^n + \cdots \in \mathbb{F}_p[X]$ irreduzibel über $\mathbb{F}_p$ ist.

# Der Körper der $p$-adischen Zahlen

In einer Implementierung genügt es $N \geq 1$ ausreichend groß zu wählen und in $\mathbb{Z}/p^N\mathbb{Z}$ zu rechnen.

## Definition

$\mathbb{Q}_p := \mathrm{Quot}(\mathbb{Z}_p)$ heißt Körper der $p$-adischen Zahlen.

Sei $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(F(X))$, wobei $F(X) = X^n + \cdots \in \mathbb{F}_p[X]$ irreduzibel über $\mathbb{F}_p$ ist. Fasst man $F(X)$ als Polynom mit Koeffizienten aus $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}$ auf, so ist

$$\mathbb{Q}_{p^n} := \mathbb{Q}_p[X]/(F(X))$$

ein *Erweiterungskörper* von $\mathbb{Q}_p$

# Der Körper der *p*-adischen Zahlen

In einer Implementierung genügt es $N \geq 1$ ausreichend groß zu wählen und in $\mathbb{Z}/p^N\mathbb{Z}$ zu rechnen.

## Definition

$\mathbb{Q}_p := \mathrm{Quot}(\mathbb{Z}_p)$ heißt Körper der *p*-adischen Zahlen.

Sei $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(F(X))$, wobei $F(X) = X^n + \cdots \in \mathbb{F}_p[X]$ irreduzibel über $\mathbb{F}_p$ ist. Fasst man $F(X)$ als Polynom mit Koeffizienten aus $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}$ auf, so ist

$$\mathbb{Q}_{p^n} := \mathbb{Q}_p[X]/(F(X))$$

ein *Erweiterungskörper* von $\mathbb{Q}_p$ und $\mathbb{Z}_{p^n} := \mathbb{Z}_p[X]/(F(X))$ eine *Ringerweiterung* von $\mathbb{Z}_p$ (jeweils vom Grad $n$).

# Der Körper der $p$-adischen Zahlen

In einer Implementierung genügt es $N \geq 1$ ausreichend groß zu wählen und in $\mathbb{Z}/p^N\mathbb{Z}$ zu rechnen.

## Definition

$\mathbb{Q}_p := \mathrm{Quot}(\mathbb{Z}_p)$ heißt Körper der $p$-adischen Zahlen.

Sei $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(F(X))$, wobei $F(X) = X^n + \cdots \in \mathbb{F}_p[X]$ irreduzibel über $\mathbb{F}_p$ ist. Fasst man $F(X)$ als Polynom mit Koeffizienten aus $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}$ auf, so ist

$$\mathbb{Q}_{p^n} := \mathbb{Q}_p[X]/(F(X))$$

ein *Erweiterungskörper* von $\mathbb{Q}_p$ und $\mathbb{Z}_{p^n} := \mathbb{Z}_p[X]/(F(X))$ eine *Ringerweiterung* von $\mathbb{Z}_p$ (jeweils vom Grad $n$).

(Genauer: Bis auf Isomorphie gibt es nur eine unverzweigte Erweiterung $K \supset \mathbb{Q}_p$ mit $[K : \mathbb{Q}_p] = n$. Bezeichnung: $\mathbb{Q}_{p^n}$.)

# Von Charakteristik $p$ nach Charakteristik 0

- In der praktischen Umsetzung benötigen wir nur $\mathbb{Z}_{p^n}$.
- Approximierung durch $n$-dimensionale Vektoren mit Einträgen aus $\{0, 1, \ldots, p^N - 1\}$.
  *Vergleiche*: $\mathbb{F}_{p^n} \cong \{0, 1, \ldots, p-1\}^n$.
- *Ausgangsproblem*: In $\mathbb{F}_{p^n}$ können wir $\mathrm{Tr}(\phi_{p^n}) \in \mathbb{Z}$ nur modulo $p$ berechnen...

# Von Charakteristik $p$ nach Charakteristik 0

- In der praktischen Umsetzung benötigen wir nur $\mathbb{Z}_{p^n}$.
- Approximierung durch $n$-dimensionale Vektoren mit Einträgen aus $\{0, 1, \ldots, p^N - 1\}$.
  *Vergleiche*: $\mathbb{F}_{p^n} \cong \{0, 1, \ldots, p-1\}^n$.
- *Ausgangsproblem*: In $\mathbb{F}_{p^n}$ können wir $\mathrm{Tr}(\phi_{p^n}) \in \mathbb{Z}$ nur modulo $p$ berechnen...

# Von Charakteristik $p$ nach Charakteristik 0

- In der praktischen Umsetzung benötigen wir nur $\mathbb{Z}_{p^n}$.
- Approximierung durch $n$-dimensionale Vektoren mit Einträgen aus $\{0, 1, \ldots, p^N - 1\}$.
  *Vergleiche*: $\mathbb{F}_{p^n} \cong \{0, 1, \ldots, p-1\}^n$.
- *Ausgangsproblem*: In $\mathbb{F}_{p^n}$ können wir $\mathrm{Tr}(\phi_{p^n}) \in \mathbb{Z}$ nur modulo $p$ berechnen...

# Von Charakteristik $p$ nach Charakteristik 0

- In der praktischen Umsetzung benötigen wir nur $\mathbb{Z}_{p^n}$.
- Approximierung durch $n$-dimensionale Vektoren mit Einträgen aus $\{0, 1, \ldots, p^N - 1\}$.
  *Vergleiche*: $\mathbb{F}_{p^n} \cong \{0, 1, \ldots, p-1\}^n$.
- *Ausgangsproblem*: In $\mathbb{F}_{p^n}$ können wir $\mathrm{Tr}(\phi_{p^n}) \in \mathbb{Z}$ nur modulo $p$ berechnen...

## Lemma

*Es gilt* $\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{F}_p$ *und* $\mathbb{Z}_{p^n} / p\mathbb{Z}_{p^n} \cong \mathbb{F}_{p^n}$.

$\mathbb{Z}_{p^n}$ (Charakteristik 0) ist also direkt mit $\mathbb{F}_{p^n}$ (Charakteristik $p$) verbunden!

# Von Charakteristik $p$ nach Charakteristik 0

- In der praktischen Umsetzung benötigen wir nur $\mathbb{Z}_{p^n}$.
- Approximierung durch $n$-dimensionale Vektoren mit Einträgen aus $\{0, 1, \ldots, p^N - 1\}$.
  *Vergleiche*: $\mathbb{F}_{p^n} \cong \{0, 1, \ldots, p-1\}^n$.
- *Ausgangsproblem*: In $\mathbb{F}_{p^n}$ können wir $\mathrm{Tr}(\phi_{p^n}) \in \mathbb{Z}$ nur modulo $p$ berechnen...

## Lemma

*Es gilt* $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ *und* $\mathbb{Z}_{p^n}/p\mathbb{Z}_{p^n} \cong \mathbb{F}_{p^n}$.

$\mathbb{Z}_{p^n}$ (Charakteristik 0) ist also direkt mit $\mathbb{F}_{p^n}$ (Charakteristik $p$) verbunden!

*Grundprinzip von Satohs Algorithmus*: Man „liftet“ die Kurve $E/\mathbb{F}_{p^n}$ nach $\mathbb{Z}_{p^n}$ und kann die (unveränderte) Spur des Frobenius in Charakteristik 0 exakt bestimmen.

# Die kanonische Projektion $\pi : \mathbb{Z}_q \to \mathbb{F}_q$

Algorithmen berechnen Lösungen stets modulo einer Potenz von $p$, d. h. der Approximationsfehler ist durch $p^N$ teilbar.

*Notation*: $a \equiv b \pmod{p^N} :\Longleftrightarrow (a - b) \in p^N\mathbb{Z}_q$

# Die kanonische Projektion $\pi : \mathbb{Z}_q \to \mathbb{F}_q$

Algorithmen berechnen Lösungen stets modulo einer Potenz von $p$, d. h. der Approximationsfehler ist durch $p^N$ teilbar.

*Notation*: $a \equiv b \pmod{p^N} :\Longleftrightarrow (a-b) \in p^N\mathbb{Z}_q$

Betrachte $\mathbb{Z}_q$ als $n$-dimensionalen $\mathbb{Z}_p$-Vektorraum:

$$\mathbb{Z}_q \ni a = (a_0, a_1, \ldots, a_{n-1}) \mathrel{\widehat{=}} a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + (F(X)).$$

Die kanonische Projektion $\pi : \mathbb{Z}_q \to \mathbb{F}_q$ ist gegeben durch

$$a \mapsto (\pi(a_0), \pi(a_1), \ldots, \pi(a_{n-1})), \text{ wobei } \pi(\,(x_1, x_2, \ldots)\,) := x_1.$$

# Die kanonische Projektion $\pi : \mathbb{Z}_q \to \mathbb{F}_q$

Algorithmen berechnen Lösungen stets modulo einer Potenz von $p$, d. h. der Approximationsfehler ist durch $p^N$ teilbar.

*Notation*: $a \equiv b \pmod{p^N} :\Longleftrightarrow (a-b) \in p^N\mathbb{Z}_q$

Betrachte $\mathbb{Z}_q$ als $n$-dimensionalen $\mathbb{Z}_p$-Vektorraum:

$$\mathbb{Z}_q \ni a = (a_0, a_1, \ldots, a_{n-1}) \mathrel{\widehat{=}} a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + (F(X)).$$

Die kanonische Projektion $\pi : \mathbb{Z}_q \to \mathbb{F}_q$ ist gegeben durch

$$a \mapsto (\pi(a_0), \pi(a_1), \ldots, \pi(a_{n-1})), \text{ wobei } \pi(\,(x_1, x_2, \ldots)\,) := x_1.$$

Man nennt $a \in \mathbb{Z}_q$ mit $\pi(a) = b \in \mathbb{F}_q$ einen Lift von $b$.

# Die kanonische Projektion $\pi : \mathbb{Z}_q \to \mathbb{F}_q$

Algorithmen berechnen Lösungen stets modulo einer Potenz von $p$, d. h. der Approximationsfehler ist durch $p^N$ teilbar.

*Notation*: $a \equiv b \pmod{p^N} :\Longleftrightarrow (a-b) \in p^N\mathbb{Z}_q$

Betrachte $\mathbb{Z}_q$ als $n$-dimensionalen $\mathbb{Z}_p$-Vektorraum:

$$\mathbb{Z}_q \ni a = (a_0, a_1, \ldots, a_{n-1}) \mathrel{\widehat{=}} a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + (F(X)).$$

Die kanonische Projektion $\pi : \mathbb{Z}_q \to \mathbb{F}_q$ ist gegeben durch

$$a \mapsto (\pi(a_0), \pi(a_1), \ldots, \pi(a_{n-1})), \text{ wobei } \pi(\ (x_1, x_2, \ldots)\ ) := x_1.$$

Man nennt $a \in \mathbb{Z}_q$ mit $\pi(a) = b \in \mathbb{F}_q$ einen Lift von $b$.

## Beispiel

$(\ (3, 8, \ldots)\ ,\ (1, 6, \ldots)\ ,\ (2, 7, \ldots)\ ) \in \mathbb{Z}_{5^3}$ ist ein Lift von $(3, 1, 2) = 3 + X + 2X^2 + (F(X)) \in \mathbb{F}_{5^3}$.

# Effiziente Nullstellenberechnung in $\mathbb{Z}_q$

Inverse, Quadratwurzeln uvm. berechnet man mit

## Lemma (Hensel)

*Sei* $f(X) \in \mathbb{Z}_q[X]$ *und* $a \in \mathbb{Z}_q$ *mit* $f(a) \equiv 0 \pmod{p^N}$ *und* $f'(a) \in \mathbb{Z}_q^*$. *Dann gilt für*

$$b := a - \frac{f(a)}{f'(a)}, \qquad \text{(Newtoniteration)}$$

*dass* $f(b) \equiv 0 \pmod{p^{2N}}$, $b \equiv a \pmod{p^N}$ *und* $f'(b) \in \mathbb{Z}_q^*$.

# Effiziente Nullstellenberechnung in $\mathbb{Z}_q$

Inverse, Quadratwurzeln uvm. berechnet man mit

## Lemma (Hensel)

*Sei* $f(X) \in \mathbb{Z}_q[X]$ *und* $a \in \mathbb{Z}_q$ *mit* $f(a) \equiv 0 \pmod{p^N}$ *und* $f'(a) \in \mathbb{Z}_q^*$. *Dann gilt für*

$$b := a - \frac{f(a)}{f'(a)}, \qquad \text{(Newtoniteration)}$$

*dass* $f(b) \equiv 0 \pmod{p^{2N}}$, $b \equiv a \pmod{p^N}$ *und* $f'(b) \in \mathbb{Z}_q^*$.

- Verfahren konvergiert immer
- Quadratische Konvergenzgeschwindigkeit
- Startnäherung ($N = 1$) wird in $\mathbb{F}_q$ bestimmt (nicht so trivial)

# Effiziente Nullstellenberechnung in $\mathbb{Z}_q$

Inverse, Quadratwurzeln uvm. berechnet man mit

## Lemma (Hensel)

*Sei* $f(X) \in \mathbb{Z}_q[X]$ *und* $a \in \mathbb{Z}_q$ *mit* $f(a) \equiv 0 \pmod{p^N}$ *und* $f'(a) \in \mathbb{Z}_q^*$. *Dann gilt für*

$$b := a - \frac{f(a)}{f'(a)}, \qquad \text{(Newtoniteration)}$$

*dass* $f(b) \equiv 0 \pmod{p^{2N}}$, $b \equiv a \pmod{p^N}$ *und* $f'(b) \in \mathbb{Z}_q^*$.

- Verfahren konvergiert immer
- Quadratische Konvergenzgeschwindigkeit
- Startnäherung ($N = 1$) wird in $\mathbb{F}_q$ bestimmt (nicht so trivial)

# Effiziente Nullstellenberechnung in $\mathbb{Z}_q$

Inverse, Quadratwurzeln uvm. berechnet man mit

## Lemma (Hensel)

*Sei* $f(X) \in \mathbb{Z}_q[X]$ *und* $a \in \mathbb{Z}_q$ *mit* $f(a) \equiv 0 \pmod{p^N}$ *und* $f'(a) \in \mathbb{Z}_q^*$. *Dann gilt für*

$$b := a - \frac{f(a)}{f'(a)}, \qquad \text{(Newtoniteration)}$$

*dass* $f(b) \equiv 0 \pmod{p^{2N}}$, $b \equiv a \pmod{p^N}$ *und* $f'(b) \in \mathbb{Z}_q^*$.

- Verfahren konvergiert immer
- Quadratische Konvergenzgeschwindigkeit
- Startnäherung ($N = 1$) wird in $\mathbb{F}_q$ bestimmt (nicht so trivial)

# Die $j$-Invariante einer elliptischen Kurve

Sei $E/K: \ y^2 = x^3 + ax + b$ eine elliptische Kurve.

## Definition

Die $j$-Invariante von $E$ ist definiert als $j(E) := \dfrac{1728 \cdot 4a^3}{4a^3 + 27b^2}$.

# Die $j$-Invariante einer elliptischen Kurve

Sei $E/K: \ y^2 = x^3 + ax + b$ eine elliptische Kurve.

## Definition

Die $j$-Invariante von $E$ ist definiert als $j(E) := \dfrac{1728 \cdot 4a^3}{4a^3 + 27b^2}$.

- Isomorphe Kurven haben dieselbe $j$-Invariante. Umgekehrt sind Kurven mit identischer $j$-Invariante isomorph über $\overline{K}$.
- $j(E)$ kodiert die wichtigsten Eigenschaften von $E$
- Zu jedem $j \in K$ gibt es bis auf Isomorphie genau eine elliptische Kurve $E/K$ mit $j(E) = j$.

$$y^2 = x^3 + 1 \quad \rightsquigarrow \quad j(E) = 0$$

$$y^2 = x^3 + x \quad \rightsquigarrow \quad j(E) = 1728$$

$$y^2 = x^3 + \left(\frac{3j}{1728 - j}\right) x + \left(\frac{2j}{1728 - j}\right) \quad \rightsquigarrow \quad j(E) = j \notin \{0, 1728\}$$

# Die $j$-Invariante einer elliptischen Kurve

Sei $E/K: \; y^2 = x^3 + ax + b$ eine elliptische Kurve.

## Definition

Die $j$-Invariante von $E$ ist definiert als $j(E) := \dfrac{1728 \cdot 4a^3}{4a^3 + 27b^2}$.

- Isomorphe Kurven haben dieselbe $j$-Invariante. Umgekehrt sind Kurven mit identischer $j$-Invariante isomorph über $\overline{K}$.
- $j(E)$ kodiert die wichtigsten Eigenschaften von $E$
- Zu jedem $j \in K$ gibt es bis auf Isomorphie genau eine elliptische Kurve $E/K$ mit $j(E) = j$.

$$y^2 = x^3 + 1 \quad \rightsquigarrow \quad j(E) = 0$$

$$y^2 = x^3 + x \quad \rightsquigarrow \quad j(E) = 1728$$

$$y^2 = x^3 + \left(\frac{3j}{1728 - j}\right) x + \left(\frac{2j}{1728 - j}\right) \quad \rightsquigarrow \quad j(E) = j \notin \{0, 1728\}$$

# Die $j$-Invariante einer elliptischen Kurve

Sei $E/K: \ y^2 = x^3 + ax + b$ eine elliptische Kurve.

## Definition

Die $j$-Invariante von $E$ ist definiert als $j(E) := \dfrac{1728 \cdot 4a^3}{4a^3 + 27b^2}$.

- Isomorphe Kurven haben dieselbe $j$-Invariante. Umgekehrt sind Kurven mit identischer $j$-Invariante isomorph über $\overline{K}$.
- $j(E)$ kodiert die wichtigsten Eigenschaften von $E$
- Zu jedem $j \in K$ gibt es bis auf Isomorphie genau eine elliptische Kurve $E/K$ mit $j(E) = j$.

$$y^2 = x^3 + 1 \quad \rightsquigarrow \quad j(E) = 0$$

$$y^2 = x^3 + x \quad \rightsquigarrow \quad j(E) = 1728$$

$$y^2 = x^3 + \left(\frac{3j}{1728 - j}\right) x + \left(\frac{2j}{1728 - j}\right) \quad \rightsquigarrow \quad j(E) = j \notin \{0, 1728\}$$

# Die $j$-Invariante einer elliptischen Kurve

Sei $E/K: \; y^2 = x^3 + ax + b$ eine elliptische Kurve.

## Definition

Die $j$-Invariante von $E$ ist definiert als $j(E) := \dfrac{1728 \cdot 4a^3}{4a^3 + 27b^2}$.

- Isomorphe Kurven haben dieselbe $j$-Invariante. Umgekehrt sind Kurven mit identischer $j$-Invariante isomorph über $\overline{K}$.
- $j(E)$ kodiert die wichtigsten Eigenschaften von $E$
- Zu jedem $j \in K$ gibt es bis auf Isomorphie genau eine elliptische Kurve $E/K$ mit $j(E) = j$.

$$y^2 = x^3 + 1 \quad \rightsquigarrow \quad j(E) = 0$$

$$y^2 = x^3 + x \quad \rightsquigarrow \quad j(E) = 1728$$

$$y^2 = x^3 + \left(\frac{3j}{1728 - j}\right) x + \left(\frac{2j}{1728 - j}\right) \quad \rightsquigarrow \quad j(E) = j \notin \{0, 1728\}$$

# Der kanonische Lift einer elliptischen Kurve $E/\mathbb{F}_q$

Seien $E/\mathbb{F}_q: \ y^2 = x^3 + ax + b$ und $E'/\mathbb{Z}_q: \ y^2 = x^3 + Ax + B$ zwei elliptische Kurven, wobei $j(E) \notin \mathbb{F}_{p^2}$.

# Der kanonische Lift einer elliptischen Kurve $E/\mathbb{F}_q$

Seien $E/\mathbb{F}_q: \ y^2 = x^3 + ax + b$ und $E'/\mathbb{Z}_q: \ y^2 = x^3 + Ax + B$ zwei elliptische Kurven, wobei $j(E) \notin \mathbb{F}_{p^2}$.

## Definition

$E'$ heißt kanonischer Lift von $E$, wenn

$$(\pi(A), \pi(B)) = (a, b) \quad \text{und} \quad \mathrm{End}(E') \cong \mathrm{End}(E) \ \text{(bzgl. } \pi)$$

# Der kanonische Lift einer elliptischen Kurve $E/\mathbb{F}_q$

Seien $E/\mathbb{F}_q: \; y^2 = x^3 + ax + b$ und $E'/\mathbb{Z}_q: \; y^2 = x^3 + Ax + B$ zwei elliptische Kurven, wobei $j(E) \notin \mathbb{F}_{p^2}$.

## Definition

$E'$ heißt kanonischer Lift von $E$, wenn

$$(\pi(A), \pi(B)) = (a, b) \quad \text{und} \quad \mathrm{End}(E') \cong \mathrm{End}(E) \;\; (\text{bzgl. } \pi)$$

Es existiert stets ein (bis auf Isomorphie eindeutiger) kanonischer Lift. *Bezeichnung*: $E^{\uparrow}$
Das Bild von $\phi \in \mathrm{End}(E)$ bezeichnen wir mit $\phi^{\uparrow}$.

# Der kanonische Lift einer elliptischen Kurve $E/\mathbb{F}_q$

Seien $E/\mathbb{F}_q: \ y^2 = x^3 + ax + b$ und $E'/\mathbb{Z}_q: \ y^2 = x^3 + Ax + B$ zwei elliptische Kurven, wobei $j(E) \notin \mathbb{F}_{p^2}$.

## Definition

$E'$ heißt kanonischer Lift von $E$, wenn

$$(\pi(A), \pi(B)) = (a, b) \quad \text{und} \quad \mathrm{End}(E') \cong \mathrm{End}(E) \ \text{(bzgl. } \pi)$$

Es existiert stets ein (bis auf Isomorphie eindeutiger) kanonischer Lift. *Bezeichnung*: $E^{\uparrow}$
Das Bild von $\phi \in \mathrm{End}(E)$ bezeichnen wir mit $\phi^{\uparrow}$.

Satohs Algorithmus beruht mathematisch auf dem folgenden

## Lemma

*Die Spur des Frobenius ist invariant unter* $^{\uparrow}$*:* $\mathrm{Tr}(\phi_q) = \mathrm{Tr}(\phi_q^{\uparrow})$.

# Wie bestimmt man den kanonischen Lift von $E$?

*Aufgabe*: Berechnung von $A$ und $B$

*Lösung*: Man berechnet zunächst $J := j(E^{\uparrow})$ mit Hilfe von $j(E)$ und arbeitet mit der Kurve

$$y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right).$$

# Wie bestimmt man den kanonischen Lift von $E$?

*Aufgabe*: Berechnung von $A$ und $B$

*Lösung*: Man berechnet zunächst $J := j(E^{\uparrow})$ mit Hilfe von $j(E)$ und arbeitet mit der Kurve

$$y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right).$$

*Bemerkung*: Man liftet eventuell nur eine zu $E$ isomorphe Kurve! Für uns aber unerheblich, da sich (wenn überhaupt) nur das Vorzeichen der Spur ändert.

# Wie bestimmt man den kanonischen Lift von $E$?

*Aufgabe*: Berechnung von $A$ und $B$

*Lösung*: Man berechnet zunächst $J := j(E^{\uparrow})$ mit Hilfe von $j(E)$ und arbeitet mit der Kurve

$$y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right).$$

*Bemerkung*: Man liftet eventuell nur eine zu $E$ isomorphe Kurve! Für uns aber unerheblich, da sich (wenn überhaupt) nur das Vorzeichen der Spur ändert.

*Hilfsmittel*: $p$-te modulare Polynome $\Phi_p(X, Y) \in \mathbb{Z}[X, Y]$

*Eigenschaften*: $\deg(\Phi_p) = p + 1$, symmetrisch & enormes Koeffizientenwachstum (in Abhängigkeit von $p$)

# Wie bestimmt man den kanonischen Lift von $E$?

*Aufgabe*: Berechnung von $A$ und $B$

*Lösung*: Man berechnet zunächst $J := j(E^{\uparrow})$ mit Hilfe von $j(E)$ und arbeitet mit der Kurve

$$y^2 = x^3 + \left(\frac{3J}{1728-J}\right)x + \left(\frac{2J}{1728-J}\right).$$

*Bemerkung*: Man liftet eventuell nur eine zu $E$ isomorphe Kurve! Für uns aber unerheblich, da sich (wenn überhaupt) nur das Vorzeichen der Spur ändert.

*Hilfsmittel*: $p$-te modulare Polynome $\Phi_p(X, Y) \in \mathbb{Z}[X, Y]$

*Eigenschaften*: $\deg(\Phi_p) = p + 1$, symmetrisch & enormes Koeffizientenwachstum (in Abhängigkeit von $p$)

**Beispiel**

$$\Phi_2(X, Y) = X^3 + \cdots + 8748000000(X + Y) - 157464000000000$$

# Wie bestimmt man den kanonischen Lift von $E$?

*Aufgabe*: Berechnung von $A$ und $B$

*Lösung*: Man berechnet zunächst $J := j(E^{\uparrow})$ mit Hilfe von $j(E)$ und arbeitet mit der Kurve

$$y^2 = x^3 + \left(\frac{3J}{1728-J}\right)x + \left(\frac{2J}{1728-J}\right).$$

*Bemerkung*: Man liftet eventuell nur eine zu $E$ isomorphe Kurve! Für uns aber unerheblich, da sich (wenn überhaupt) nur das Vorzeichen der Spur ändert.

*Hilfsmittel*: $p$-te modulare Polynome $\Phi_p(X, Y) \in \mathbb{Z}[X, Y]$

*Eigenschaften*: $\deg(\Phi_p) = p + 1$, symmetrisch & enormes Koeffizientenwachstum (in Abhängigkeit von $p$)

**Beispiel**

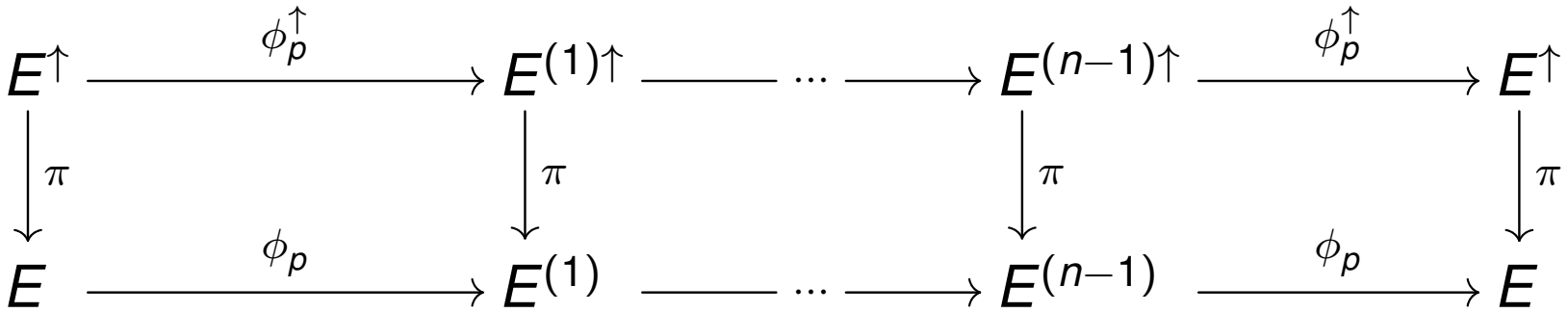
$$\Phi_2(X, Y) = X^3 + \cdots + 8748000000(X + Y) - 157464000000000$$

$\Phi_p$ für $p \leq 353$: `http://www.math.uwaterloo.ca/~mrubinst/`

# Vercauterens Algorithmus (zur Berechnung von $j(E^{\uparrow})$)

$$\begin{array}{ccccccccc}
E^{\uparrow} & \xrightarrow{\phi_p^{\uparrow}} & E^{(1)\uparrow} & \longrightarrow & \cdots & \longrightarrow & E^{(n-1)\uparrow} & \xrightarrow{\phi_p^{\uparrow}} & E^{\uparrow} \\
\downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} & & & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\
E & \xrightarrow{\phi_p} & E^{(1)} & \longrightarrow & \cdots & \longrightarrow & E^{(n-1)} & \xrightarrow{\phi_p} & E
\end{array}$$

# Vercauterens Algorithmus (zur Berechnung von $j(E^{\uparrow})$)




## Lemma (Lubin, Serre, Tate, Vercauteren)

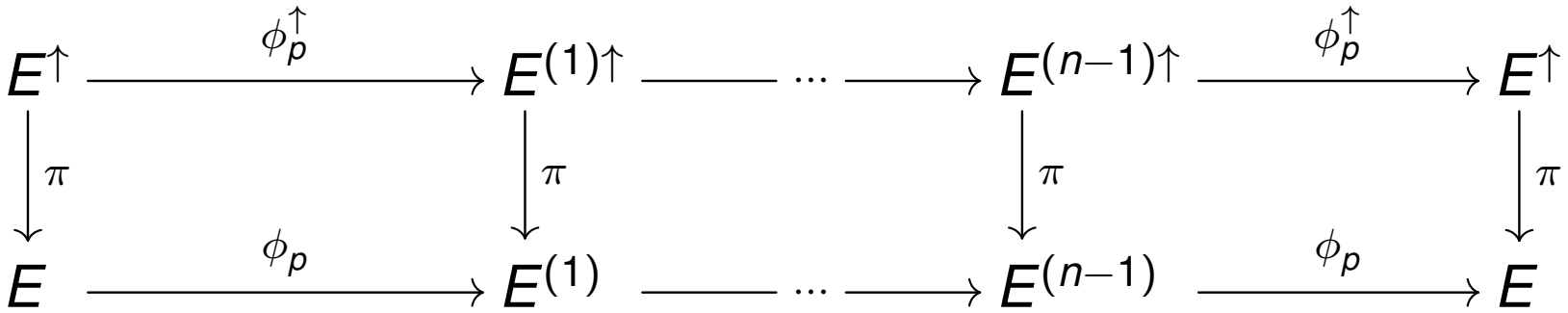
*Sei $J \in \mathbb{Z}_q$ mit*

$$J \equiv j(E^{(i)\uparrow}) \pmod{p^N}.$$

*Dann gilt für die (eindeutige) Nullstelle $L$ von $\Phi_p(J, Y)$, dass*

$$L \equiv j(E^{(i+1)\uparrow}) \pmod{p^{N+1}}.$$

# Vercauterens Algorithmus (zur Berechnung von $j(E^{\uparrow})$)




## Lemma (Lubin, Serre, Tate, Vercauteren)

*Sei $J \in \mathbb{Z}_q$ mit*

$$J \equiv j(E^{(i)\uparrow}) \pmod{p^N}.$$

*Dann gilt für die (eindeutige) Nullstelle $L$ von $\Phi_p(J, Y)$, dass*

$$L \equiv j(E^{(i+1)\uparrow}) \pmod{p^{N+1}}.$$

Formel für die Startnäherung: $\pi(j(E^{(i)\uparrow})) = j(E^{(i)}) = j(E)^{(p^i)}$.

# Vercauterens Algorithmus schematisch

$$E^{\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{(1)\uparrow} \longrightarrow \dots \longrightarrow E^{(n-1)\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{\uparrow}$$

*Ziel*: Berechnung der $j$-Invariante von $E^{\uparrow}$ zur Genauigkeit $N$.

Man betritt dazu den Zyklus an der Stelle $m := (1 - N) \bmod n$ und erreicht nach $N - 1$ Schritten die Ausgangskurve. Eine Newtoniteration berechnet jeweils die Nullstelle von $\Phi_p(J, Y)$.

$$\begin{array}{ccc}
 & & j(E^{\uparrow}) \bmod p^N \\
 & & \uparrow +1 \\
 & L \equiv j(E^{(n-1)\uparrow}) \pmod{p^{N-1}} & \to J \\
 & \Big\uparrow +(N-3) & \\
L \equiv j(E^{(2-N)\uparrow}) \pmod{p^2} & \longrightarrow & J \\
\uparrow +1 & & \\
J := \pi^{-1}(\, j(E)^{(p^m)}\,) & &
\end{array}$$

# Isogenien und formale Potenzreihen

$$E\uparrow \xrightarrow{\phi_p^{\uparrow}} E^{(1)}\uparrow \longrightarrow \dots \longrightarrow E^{(n-1)}\uparrow \xrightarrow{\phi_p^{\uparrow}} E\uparrow$$

Sei $y^2 = x^3 + \left(\frac{3J}{1728-J}\right)x + \left(\frac{2J}{1728-J}\right)$ der kanonische Lift von $E$ (bzw. einer zu $E$ isomorphen Kurve). Wie berechnet man daraus die Spur des (gelifteten) Frobenius?

# Isogenien und formale Potenzreihen

$$E\uparrow \xrightarrow{\phi_p^{\uparrow}} E^{(1)}\uparrow \longrightarrow \dots \longrightarrow E^{(n-1)}\uparrow \xrightarrow{\phi_p^{\uparrow}} E\uparrow$$

Sei $y^2 = x^3 + \left(\frac{3J}{1728-J}\right)x + \left(\frac{2J}{1728-J}\right)$ der kanonische Lift von $E$ (bzw. einer zu $E$ isomorphen Kurve). Wie berechnet man daraus die Spur des (gelifteten) Frobenius?

Der letzte Schritt in Satohs Algorithmus ist theoretisch recht anspruchsvoll. Zunächst werden Isogenien formale Potenzreihen zugeordnet.

# Isogenien und formale Potenzreihen

$$E^{\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{(1)\uparrow} \longrightarrow \dots \longrightarrow E^{(n-1)\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{\uparrow}$$

Sei $y^2 = x^3 + \left(\frac{3J}{1728-J}\right)x + \left(\frac{2J}{1728-J}\right)$ der kanonische Lift von $E$ (bzw. einer zu $E$ isomorphen Kurve). Wie berechnet man daraus die Spur des (gelifteten) Frobenius?

Der letzte Schritt in Satohs Algorithmus ist theoretisch recht anspruchsvoll. Zunächst werden Isogenien formale Potenzreihen zugeordnet.

Mit $\left(\widehat{\phi_p^{\uparrow}} : \ E^{\uparrow} \to E^{(n-1)\uparrow}\right) \mapsto \sum_{\nu=0}^{\infty} c_\nu X^\nu \in \overline{\mathbb{Q}}_q[\![X]\!]$ gilt dann $c_1 \in \mathbb{Z}_q$ und für $N \leq n$

$$\mathrm{Tr}(\phi_q) \equiv \mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(c_1) \pmod{p^N}.$$

# Isogenien und formale Potenzreihen

$$E^{\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{(1)\uparrow} \longrightarrow \dots \longrightarrow E^{(n-1)\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{\uparrow}$$

Sei $y^2 = x^3 + \left(\frac{3J}{1728-J}\right)x + \left(\frac{2J}{1728-J}\right)$ der kanonische Lift von $E$ (bzw. einer zu $E$ isomorphen Kurve). Wie berechnet man daraus die Spur des (gelifteten) Frobenius?

Der letzte Schritt in Satohs Algorithmus ist theoretisch recht anspruchsvoll. Zunächst werden Isogenien formale Potenzreihen zugeordnet.

Mit $\left(\widehat{\phi_p^{\uparrow}} : \ E^{\uparrow} \to E^{(n-1)\uparrow}\right) \mapsto \sum_{\nu=0}^{\infty} c_\nu X^\nu \in \overline{\mathbb{Q}}_q[\![X]\!]$ gilt dann $c_1 \in \mathbb{Z}_q$ und für $N \leq n$

$$\mathrm{Tr}(\phi_q) \equiv \mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(c_1) \pmod{p^N}.$$

Wie berechnet man $c_1$ und dessen (algebraische) Norm?

*Harley*: Norm = Resultante (Determinante der Sylvester-Matrix)
Die $(2n-1)^2$ Einträge hängen nur von $c_1$ und $F(X)$ ab!

# Wie berechnet man $c_1$?

$$E^{\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{(1)\uparrow} \longrightarrow \dots \longrightarrow E^{(n-1)\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{\uparrow}$$

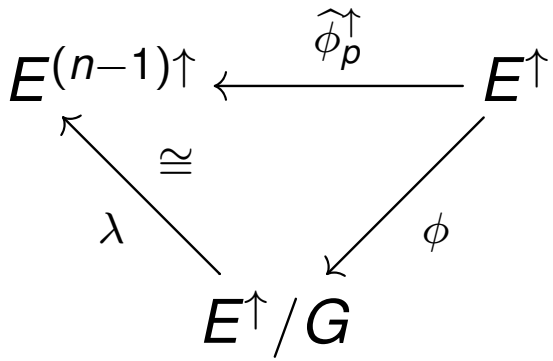
Man faktorisiert $\widehat{\phi_p^{\uparrow}} : E^{\uparrow} \to E^{(n-1)\uparrow}$ mit Hilfe der $p$-elementigen Untergruppe $G := \ker \widehat{\phi_p^{\uparrow}} \subset E^{\uparrow}$. Es gilt $E^{\uparrow}/G \cong E^{(n-1)\uparrow}$.

# Wie berechnet man $c_1$?

$$E^{\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{(1)\uparrow} \longrightarrow \dots \longrightarrow E^{(n-1)\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{\uparrow}$$

Man faktorisiert $\widehat{\phi_p^{\uparrow}} : E^{\uparrow} \to E^{(n-1)\uparrow}$ mit Hilfe der $p$-elementigen Untergruppe $G := \ker \widehat{\phi_p^{\uparrow}} \subset E^{\uparrow}$. Es gilt $E^{\uparrow}/G \cong E^{(n-1)\uparrow}$.

Die Isogenien $\lambda$ und $\phi$ mit $\widehat{\phi_p^{\uparrow}} = \lambda \circ \phi$ sind eindeutig bestimmt.



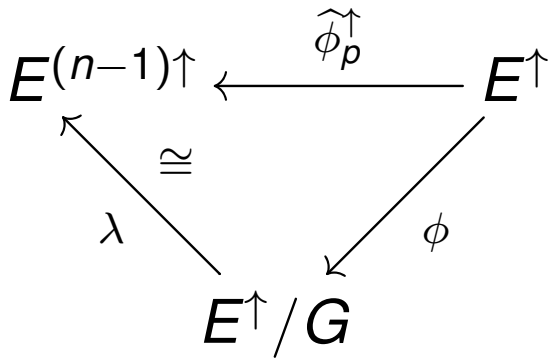
# Wie berechnet man $c_1$?

$$E^{\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{(1)\uparrow} \longrightarrow \dots \longrightarrow E^{(n-1)\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{\uparrow}$$

Man faktorisiert $\widehat{\phi_p^{\uparrow}} : E^{\uparrow} \to E^{(n-1)\uparrow}$ mit Hilfe der $p$-elementigen Untergruppe $G := \ker \widehat{\phi_p^{\uparrow}} \subset E^{\uparrow}$. Es gilt $E^{\uparrow}/G \cong E^{(n-1)\uparrow}$.

Die Isogenien $\lambda$ und $\phi$ mit $\widehat{\phi_p^{\uparrow}} = \lambda \circ \phi$ sind eindeutig bestimmt.

Die obige Formel impliziert (*Vélu*), dass $c_1 = d_1 \cdot 1 = d_1$, wobei $d_1 \in \mathbb{Z}_q$ der erste Koeffizient der von $\lambda$ induzierten Potenzreihe ist ($\lambda \mapsto \sum_{\nu=0}^{\infty} d_\nu X^\nu$).



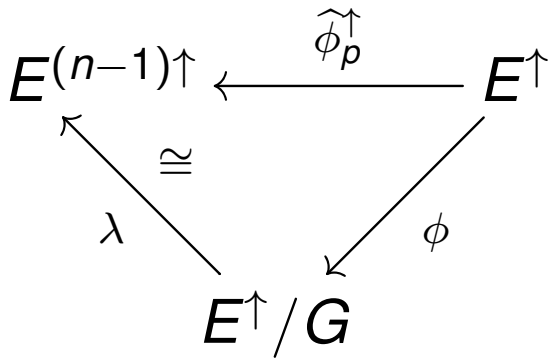
# Wie berechnet man $c_1$?

$$E^{\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{(1)\uparrow} \longrightarrow \dots \longrightarrow E^{(n-1)\uparrow} \xrightarrow{\phi_p^{\uparrow}} E^{\uparrow}$$

Man faktorisiert $\widehat{\phi_p^{\uparrow}} : E^{\uparrow} \to E^{(n-1)\uparrow}$ mit Hilfe der $p$-elementigen Untergruppe $G := \ker \widehat{\phi_p^{\uparrow}} \subset E^{\uparrow}$. Es gilt $E^{\uparrow}/G \cong E^{(n-1)\uparrow}$.

Die Isogenien $\lambda$ und $\phi$ mit $\widehat{\phi_p^{\uparrow}} = \lambda \circ \phi$ sind eindeutig bestimmt.

Die obige Formel impliziert (*Vélu*), dass $c_1 = d_1 \cdot 1 = d_1$, wobei $d_1 \in \mathbb{Z}_q$ der erste Koeffizient der von $\lambda$ induzierten Potenzreihe ist ($\lambda \mapsto \sum_{\nu=0}^{\infty} d_\nu X^\nu$).




## Lemma

*Mit* $E^{\uparrow}/G : \; y^2 = x^3 + \mathcal{A}x + \mathcal{B}$ *gilt* $(d_1)^2 = 3\mathcal{B} \cdot (2\mathcal{A})^{-1}$, *d. h.*

$$\mathrm{Tr}(\phi_q)^2 \equiv \left(\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(d_1)\right)^2 \equiv \mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1}) \pmod{p^N}.$$

# Der letzte Schritt in Satohs Algorithmus

- Wir benötigen also nur noch $\mathcal{A}$ und $\mathcal{B}$. Die gesuchte Spur ist dann eine Quadratwurzel von $\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1})$.
- Da wir (mittels einer expliziten Formel) $\mathrm{Tr}(\phi_q)$ mod $p$ kennen, können wir die Wurzelberechnung korrekt initialisieren.
- $\mathcal{A}$ und $\mathcal{B}$ lassen sich direkt (*Vélu*, *Satoh*) aus den Koeffizienten eines gewissen Teilers $H(X)$ des $p$-ten Divisionspolynoms $P(X) \in \mathbb{Z}_q[X]$ von $E^{\uparrow}$ berechnen. Obwohl $\deg(H) = (p-1)/2$ ist dieser Teil im Allgemeinen am aufwändigsten. *Iterationsvorschrift*:

$$H(X) \leftarrow H(X) + \left( \frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X) \right)$$

  Die Startnäherung gewinnt man aus dem $p$-ten Divisionspolynom von $E^{(n-1)}$.

# Der letzte Schritt in Satohs Algorithmus

- Wir benötigen also nur noch $\mathcal{A}$ und $\mathcal{B}$. Die gesuchte Spur ist dann eine Quadratwurzel von $\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1})$.
- Da wir (mittels einer expliziten Formel) $\mathrm{Tr}(\phi_q)$ mod $p$ kennen, können wir die Wurzelberechnung korrekt initialisieren.
- $\mathcal{A}$ und $\mathcal{B}$ lassen sich direkt (*Vélu*, *Satoh*) aus den Koeffizienten eines gewissen Teilers $H(X)$ des $p$-ten Divisionspolynoms $P(X) \in \mathbb{Z}_q[X]$ von $E^{\uparrow}$ berechnen. Obwohl $\deg(H) = (p-1)/2$ ist dieser Teil im Allgemeinen am aufwändigsten. *Iterationsvorschrift*:

$$H(X) \leftarrow H(X) + \left( \frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X) \right)$$

  Die Startnäherung gewinnt man aus dem $p$-ten Divisionspolynom von $E^{(n-1)}$.

# Der letzte Schritt in Satohs Algorithmus

- Wir benötigen also nur noch $\mathcal{A}$ und $\mathcal{B}$. Die gesuchte Spur ist dann eine Quadratwurzel von $\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1})$.
- Da wir (mittels einer expliziten Formel) $\mathrm{Tr}(\phi_q)$ mod $p$ kennen, können wir die Wurzelberechnung korrekt initialisieren.
- $\mathcal{A}$ und $\mathcal{B}$ lassen sich direkt (*Vélu*, *Satoh*) aus den Koeffizienten eines gewissen Teilers $H(X)$ des $p$-ten Divisionspolynoms $P(X) \in \mathbb{Z}_q[X]$ von $E^{\uparrow}$ berechnen. Obwohl $\deg(H) = (p-1)/2$ ist dieser Teil im Allgemeinen am aufwändigsten. *Iterationsvorschrift*:

$$H(X) \leftarrow H(X) + \left( \frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X) \right)$$

  Die Startnäherung gewinnt man aus dem $p$-ten Divisionspolynom von $E^{(n-1)}$.

# Und was ist mit $N$?

Nach der Abschätzung von *Hasse* gilt: $|\mathrm{Tr}(\phi_q)| \leq 2\sqrt{q}$

# Und was ist mit $N$?

Nach der Abschätzung von *Hasse* gilt: $|\mathrm{Tr}(\phi_q)| \leq 2\sqrt{q}$

Mit dem Ansatz $p^x = 2 \cdot 2\sqrt{q}$ erhält man ($q = p^n$)

$$x \cdot \ln(p) = \ln(4\sqrt{q}) = \ln(4) + \ln(p^{n/2})$$
$$x = \log_p 4 + n/2.$$

# Und was ist mit $N$?

Nach der Abschätzung von *Hasse* gilt: $|\mathrm{Tr}(\phi_q)| \leq 2\sqrt{q}$

Mit dem Ansatz $p^x = 2 \cdot 2\sqrt{q}$ erhält man ($q = p^n$)

$$x \cdot \ln(p) = \ln(4\sqrt{q}) = \ln(4) + \ln(p^{n/2})$$
$$x = \log_p 4 + n/2.$$

Bei der Berechnung von $H(X)$ „verliert man eine Stelle“, d. h.

$$N := \lceil \log_p 4 + n/2 \rceil + 1.$$

# Und was ist mit $N$?

Nach der Abschätzung von *Hasse* gilt: $|\mathrm{Tr}(\phi_q)| \leq 2\sqrt{q}$

Mit dem Ansatz $p^x = 2 \cdot 2\sqrt{q}$ erhält man ($q = p^n$)

$$\begin{aligned} x \cdot \ln(p) &= \ln(4\sqrt{q}) = \ln(4) + \ln(p^{n/2}) \\ x &= \log_p 4 + n/2. \end{aligned}$$

Bei der Berechnung von $H(X)$ „verliert man eine Stelle“, d. h.

$$N := \lceil \log_p 4 + n/2 \rceil + 1.$$

Mit $T := \mathrm{Tr}(\phi_q) \bmod p^{N-1}$ gilt dann

$$\mathrm{Tr}(\phi_q) = \begin{cases} T & \text{falls } T \leq 2\sqrt{q}, \\ T - p^{N-1} & \text{falls } T > 2\sqrt{q}. \end{cases}$$

# Zusammenfassung

## Satohs Algorithmus ($E/\mathbb{F}_{p^n}: \; y^2 = x^3 + ax + b, \; j(E) \notin \mathbb{F}_{p^2}$)

1. $N := \lceil \log_p 4 + n/2 \rceil + 1$
2. $J \equiv j(E^{\uparrow}) \pmod{p^N}$ (*Vercauteren*)
3. $E^{\uparrow}: \; y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right)$
4. $H(X) \leftarrow H(X) + \left(\frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X)\right)$
   - $p$-te Divisionspolynom von $E^{(n-1)}$ (*McKee*)
   - $p$-te Divisionspolynom von $E^{\uparrow}$ (rekursiv oder *McKee*)
5. $H(X) \rightsquigarrow \mathcal{A}, \mathcal{B}$
6. $\mathrm{N}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1}) \equiv \mathrm{Tr}(\phi_{p^n})^2 \pmod{p^{N-1}}$
7. $\#E(\mathbb{F}_{p^n}) = p^n + 1 - \mathrm{Tr}(\phi_{p^n})$

# Zusammenfassung

## Satohs Algorithmus ($E/\mathbb{F}_{p^n}: \; y^2 = x^3 + ax + b, \; j(E) \notin \mathbb{F}_{p^2}$)

1. $N := \lceil \log_p 4 + n/2 \rceil + 1$
2. $J \equiv j(E^{\uparrow}) \pmod{p^N}$ (*Vercauteren*)
3. $E^{\uparrow}: \; y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right)$
4. $H(X) \leftarrow H(X) + \left(\frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X)\right)$
   - $p$-te Divisionspolynom von $E^{(n-1)}$ (*McKee*)
   - $p$-te Divisionspolynom von $E^{\uparrow}$ (rekursiv oder *McKee*)
5. $H(X) \rightsquigarrow \mathcal{A}, \mathcal{B}$
6. $\mathrm{N}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1}) \equiv \mathrm{Tr}(\phi_{p^n})^2 \pmod{p^{N-1}}$
7. $\#E(\mathbb{F}_{p^n}) = p^n + 1 - \mathrm{Tr}(\phi_{p^n})$

# Zusammenfassung

## Satohs Algorithmus ($E/\mathbb{F}_{p^n}: \; y^2 = x^3 + ax + b, \; j(E) \notin \mathbb{F}_{p^2}$)

1. $N := \lceil \log_p 4 + n/2 \rceil + 1$
2. $J \equiv j(E^{\uparrow}) \pmod{p^N}$ (*Vercauteren*)
3. $E^{\uparrow}: \; y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right)$
4. $H(X) \leftarrow H(X) + \left(\frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X)\right)$
   - $p$-te Divisionspolynom von $E^{(n-1)}$ (*McKee*)
   - $p$-te Divisionspolynom von $E^{\uparrow}$ (rekursiv oder *McKee*)
5. $H(X) \rightsquigarrow \mathcal{A}, \mathcal{B}$
6. $\mathrm{N}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1}) \equiv \mathrm{Tr}(\phi_{p^n})^2 \pmod{p^{N-1}}$
7. $\#E(\mathbb{F}_{p^n}) = p^n + 1 - \mathrm{Tr}(\phi_{p^n})$

# Zusammenfassung

## Satohs Algorithmus ($E/\mathbb{F}_{p^n}: \; y^2 = x^3 + ax + b, \; j(E) \notin \mathbb{F}_{p^2}$)

1. $N := \lceil \log_p 4 + n/2 \rceil + 1$
2. $J \equiv j(E^{\uparrow}) \pmod{p^N}$ (*Vercauteren*)
3. $E^{\uparrow}: \; y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right)$
4. $H(X) \leftarrow H(X) + \left(\frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X)\right)$
   - $p$-te Divisionspolynom von $E^{(n-1)}$ (*McKee*)
   - $p$-te Divisionspolynom von $E^{\uparrow}$ (rekursiv oder *McKee*)
5. $H(X) \rightsquigarrow \mathcal{A}, \mathcal{B}$
6. $\mathrm{N}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1}) \equiv \mathrm{Tr}(\phi_{p^n})^2 \pmod{p^{N-1}}$
7. $\#E(\mathbb{F}_{p^n}) = p^n + 1 - \mathrm{Tr}(\phi_{p^n})$

# Zusammenfassung

## Satohs Algorithmus ($E/\mathbb{F}_{p^n}: \; y^2 = x^3 + ax + b, \; j(E) \notin \mathbb{F}_{p^2}$)

1. $N := \lceil \log_p 4 + n/2 \rceil + 1$
2. $J \equiv j(E^{\uparrow}) \pmod{p^N}$ (*Vercauteren*)
3. $E^{\uparrow}: \; y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right)$
4. $H(X) \leftarrow H(X) + \left(\frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X)\right)$
   - $p$-te Divisionspolynom von $E^{(n-1)}$ (*McKee*)
   - $p$-te Divisionspolynom von $E^{\uparrow}$ (rekursiv oder *McKee*)
5. $H(X) \rightsquigarrow \mathcal{A}, \mathcal{B}$
6. $\mathrm{N}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1}) \equiv \mathrm{Tr}(\phi_{p^n})^2 \pmod{p^{N-1}}$
7. $\#E(\mathbb{F}_{p^n}) = p^n + 1 - \mathrm{Tr}(\phi_{p^n})$

# Zusammenfassung

## Satohs Algorithmus ($E/\mathbb{F}_{p^n}: \; y^2 = x^3 + ax + b, \; j(E) \notin \mathbb{F}_{p^2}$)

1. $N := \lceil \log_p 4 + n/2 \rceil + 1$
2. $J \equiv j(E^{\uparrow}) \pmod{p^N}$ (*Vercauteren*)
3. $E^{\uparrow}: \; y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right)$
4. $H(X) \leftarrow H(X) + \left(\frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X)\right)$
   - $p$-te Divisionspolynom von $E^{(n-1)}$ (*McKee*)
   - $p$-te Divisionspolynom von $E^{\uparrow}$ (rekursiv oder *McKee*)
5. $H(X) \rightsquigarrow \mathcal{A}, \mathcal{B}$
6. $\mathrm{N}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1}) \equiv \mathrm{Tr}(\phi_{p^n})^2 \pmod{p^{N-1}}$
7. $\#E(\mathbb{F}_{p^n}) = p^n + 1 - \mathrm{Tr}(\phi_{p^n})$

# Zusammenfassung

## Satohs Algorithmus ($E/\mathbb{F}_{p^n}: \; y^2 = x^3 + ax + b, \; j(E) \notin \mathbb{F}_{p^2}$)

1. $N := \lceil \log_p 4 + n/2 \rceil + 1$
2. $J \equiv j(E^{\uparrow}) \pmod{p^N}$ (*Vercauteren*)
3. $E^{\uparrow}: \; y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right)$
4. $H(X) \leftarrow H(X) + \left(\frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X)\right)$
   - $p$-te Divisionspolynom von $E^{(n-1)}$ (*McKee*)
   - $p$-te Divisionspolynom von $E^{\uparrow}$ (rekursiv oder *McKee*)
5. $H(X) \rightsquigarrow \mathcal{A}, \mathcal{B}$
6. $\mathrm{N}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1}) \equiv \mathrm{Tr}(\phi_{p^n})^2 \pmod{p^{N-1}}$
7. $\#E(\mathbb{F}_{p^n}) = p^n + 1 - \mathrm{Tr}(\phi_{p^n})$

# Zusammenfassung

## Satohs Algorithmus ($E/\mathbb{F}_{p^n}: \; y^2 = x^3 + ax + b, \; j(E) \notin \mathbb{F}_{p^2}$)

1. $N := \lceil \log_p 4 + n/2 \rceil + 1$
2. $J \equiv j(E^{\uparrow}) \pmod{p^N}$ (*Vercauteren*)
3. $E^{\uparrow}: \; y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right)$
4. $H(X) \leftarrow H(X) + \left(\frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X)\right)$
   - $p$-te Divisionspolynom von $E^{(n-1)}$ (*McKee*)
   - $p$-te Divisionspolynom von $E^{\uparrow}$ (rekursiv oder *McKee*)
5. $H(X) \rightsquigarrow \mathcal{A}, \mathcal{B}$
6. $\mathrm{N}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1}) \equiv \mathrm{Tr}(\phi_{p^n})^2 \pmod{p^{N-1}}$
7. $\#E(\mathbb{F}_{p^n}) = p^n + 1 - \mathrm{Tr}(\phi_{p^n})$

# Zusammenfassung

## Satohs Algorithmus ($E/\mathbb{F}_{p^n}: \; y^2 = x^3 + ax + b, \; j(E) \notin \mathbb{F}_{p^2}$)

1. $N := \lceil \log_p 4 + n/2 \rceil + 1$
2. $J \equiv j(E^{\uparrow}) \pmod{p^N}$ (*Vercauteren*)
3. $E^{\uparrow}: \; y^2 = x^3 + \left(\frac{3J}{1728-J}\right) x + \left(\frac{2J}{1728-J}\right)$
4. $H(X) \leftarrow H(X) + \left(\frac{P(X) \cdot H'(X)}{P'(X)} \bmod H(X)\right)$
   - $p$-te Divisionspolynom von $E^{(n-1)}$ (*McKee*)
   - $p$-te Divisionspolynom von $E^{\uparrow}$ (rekursiv oder *McKee*)
5. $H(X) \rightsquigarrow \mathcal{A}, \mathcal{B}$
6. $\mathrm{N}_{\mathbb{Q}_{p^n}/\mathbb{Q}_p}(3\mathcal{B} \cdot (2\mathcal{A})^{-1}) \equiv \mathrm{Tr}(\phi_{p^n})^2 \pmod{p^{N-1}}$
7. $\#E(\mathbb{F}_{p^n}) = p^n + 1 - \mathrm{Tr}(\phi_{p^n})$

# Anmerkungen zur Implementierung

- Satohs Algorithmus wurde in `C++` implementiert (unter Verwendung von `NTL` und `GMP`)
- Theoretisch keine obere Grenze für $p$ (Daten für $\Phi_p(X, Y)$ nur bis $p = 353$ vorhanden)
- Tests im Bereich $5 \leq p \leq 317$
- Sonderfall $j(E) \in \mathbb{F}_{p^2}$ wurde berücksichtigt
- Anwendung ab $p^n > 2^{160}$, $p \geq 127$

# Anmerkungen zur Implementierung

- Satohs Algorithmus wurde in `C++` implementiert (unter Verwendung von `NTL` und `GMP`)
- Theoretisch keine obere Grenze für $p$ (Daten für $\Phi_p(X, Y)$ nur bis $p = 353$ vorhanden)
- Tests im Bereich $5 \leq p \leq 317$
- Sonderfall $j(E) \in \mathbb{F}_{p^2}$ wurde berücksichtigt
- Anwendung ab $p^n > 2^{160}$, $p \geq 127$

# Anmerkungen zur Implementierung

- Satohs Algorithmus wurde in `C++` implementiert (unter Verwendung von `NTL` und `GMP`)
- Theoretisch keine obere Grenze für $p$ (Daten für $\Phi_p(X, Y)$ nur bis $p = 353$ vorhanden)
- Tests im Bereich $5 \leq p \leq 317$
- Sonderfall $j(E) \in \mathbb{F}_{p^2}$ wurde berücksichtigt
- Anwendung ab $p^n > 2^{160}$, $p \geq 127$

# Anmerkungen zur Implementierung

- Satohs Algorithmus wurde in `C++` implementiert (unter Verwendung von `NTL` und `GMP`)
- Theoretisch keine obere Grenze für $p$ (Daten für $\Phi_p(X, Y)$ nur bis $p = 353$ vorhanden)
- Tests im Bereich $5 \leq p \leq 317$
- Sonderfall $j(E) \in \mathbb{F}_{p^2}$ wurde berücksichtigt
- Anwendung ab $p^n > 2^{160}$, $p \geq 127$

# Anmerkungen zur Implementierung

- Satohs Algorithmus wurde in `C++` implementiert (unter Verwendung von `NTL` und `GMP`)
- Theoretisch keine obere Grenze für $p$ (Daten für $\Phi_p(X, Y)$ nur bis $p = 353$ vorhanden)
- Tests im Bereich $5 \leq p \leq 317$
- Sonderfall $j(E) \in \mathbb{F}_{p^2}$ wurde berücksichtigt
- Anwendung ab $p^n > 2^{160}$, $p \geq 127$

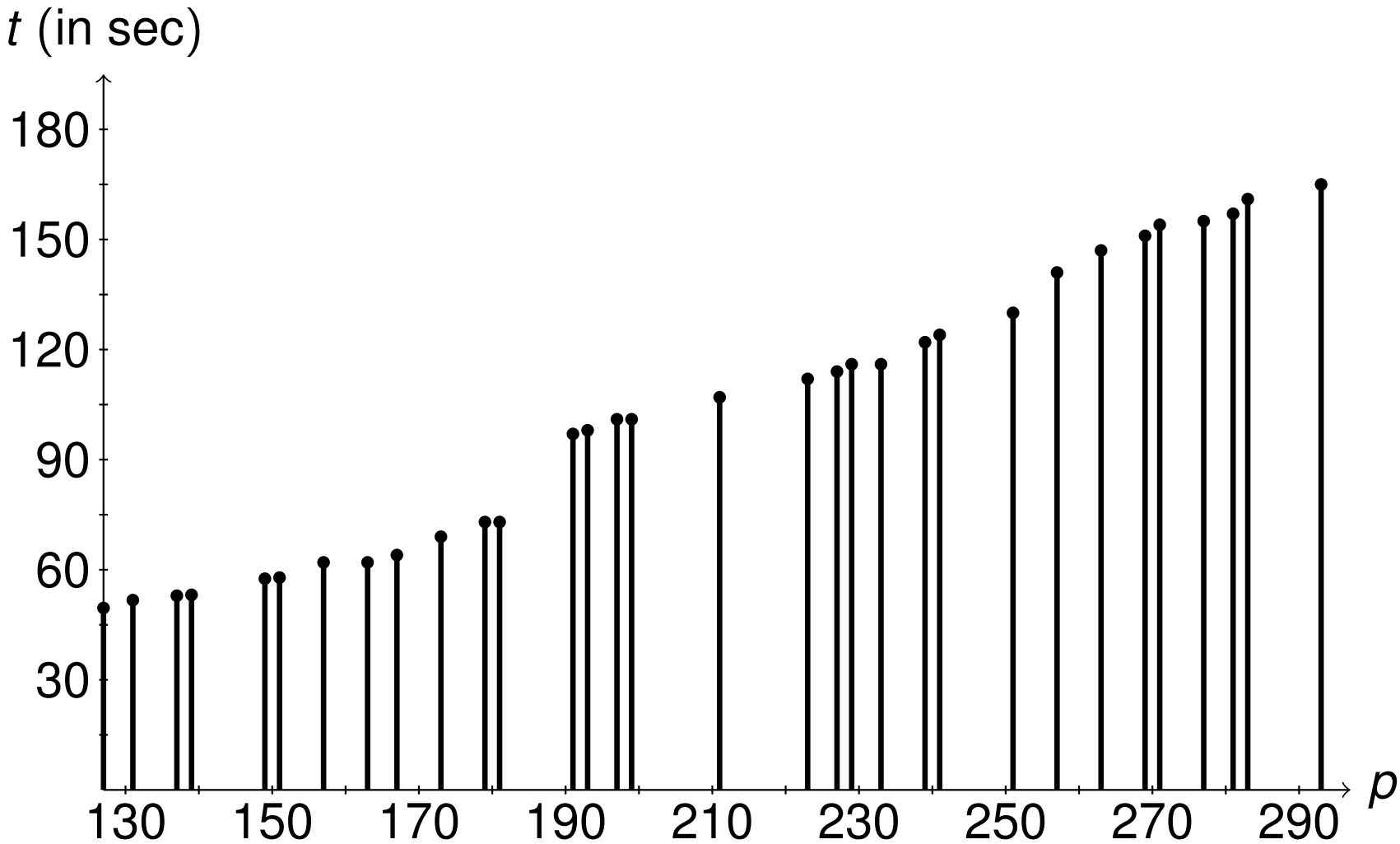
# Anmerkungen zur Implementierung

- Satohs Algorithmus wurde in `C++` implementiert (unter Verwendung von `NTL` und `GMP`)
- Theoretisch keine obere Grenze für $p$ (Daten für $\Phi_p(X, Y)$ nur bis $p = 353$ vorhanden)
- Tests im Bereich $5 \leq p \leq 317$
- Sonderfall $j(E) \in \mathbb{F}_{p^2}$ wurde berücksichtigt
- Anwendung ab $p^n > 2^{160}$, $p \geq 127$

Tabelle : Laufzeiten `satoh`, $p^n \approx 2^{160}$

| $p$ | $n$ | $t$ | $t_{\text{j\_invariant}}/t$ | $t_{\text{kernel}}/t$ |
|---|---|---|---|---|
| 7 | 59 | 2,0 sec | 66 % | 32 % |
| 89 | 29 | 39,2 sec | 9 % | 91 % |

# Laufzeiten `satoh`, $p \in [127, 293],\ n = 23$ ($p^n > 2^{160}$)



# Suche nach kryptographisch starken Kurven

*Gesucht*: $E/\mathbb{F}_q$, so dass $\#E(\mathbb{F}_q)$ eine (große) Primzahl ist

*Trial-and-Error Ansatz*: Man erzeugt so lange Zufallskurven, bis die gewünschte Eigenschaft auftritt.

# Suche nach kryptographisch starken Kurven

*Gesucht*: $E/\mathbb{F}_q$, so dass $\#E(\mathbb{F}_q)$ eine (große) Primzahl ist

*Trial-and-Error Ansatz*: Man erzeugt so lange Zufallskurven, bis die gewünschte Eigenschaft auftritt.

*Early-Abort Strategie*: Mit Hilfe von Divisionspolynomen kann man schnell entscheiden, ob $\#E(\mathbb{F}_q)$ kleine Primteiler hat (in diesem Fall wird die Ordnung erst gar nicht berechnet).

# Suche nach kryptographisch starken Kurven

*Gesucht*: $E/\mathbb{F}_q$, so dass $\#E(\mathbb{F}_q)$ eine (große) Primzahl ist

*Trial-and-Error Ansatz*: Man erzeugt so lange Zufallskurven, bis die gewünschte Eigenschaft auftritt.

*Early-Abort Strategie*: Mit Hilfe von Divisionspolynomen kann man schnell entscheiden, ob $\#E(\mathbb{F}_q)$ kleine Primteiler hat (in diesem Fall wird die Ordnung erst gar nicht berechnet).

Sei $r$ eine Primzahl. Besitzt das $r$-te Divisionspolynom eine Nullstelle $x \in \mathbb{F}_q$ *und* existiert $y \in \mathbb{F}_q$ mit $y^2 = x^3 + ax + b$, so ist $\#E(\mathbb{F}_q)$ durch $r$ teilbar!

# Suche nach kryptographisch starken Kurven

*Gesucht*: $E/\mathbb{F}_q$, so dass $\#E(\mathbb{F}_q)$ eine (große) Primzahl ist

*Trial-and-Error Ansatz*: Man erzeugt so lange Zufallskurven, bis die gewünschte Eigenschaft auftritt.

*Early-Abort Strategie*: Mit Hilfe von Divisionspolynomen kann man schnell entscheiden, ob $\#E(\mathbb{F}_q)$ kleine Primteiler hat (in diesem Fall wird die Ordnung erst gar nicht berechnet).

Sei $r$ eine Primzahl. Besitzt das $r$-te Divisionspolynom eine Nullstelle $x \in \mathbb{F}_q$ *und* existiert $y \in \mathbb{F}_q$ mit $y^2 = x^3 + ax + b$, so ist $\#E(\mathbb{F}_q)$ durch $r$ teilbar!

$r = 2, 3, 5, 7$ reicht bereits aus um ca. 77 Prozent aller Zufallskurven auszusieben.

# Suche nach kryptographisch starken Kurven

*Gesucht*: $E/\mathbb{F}_q$, so dass $\#E(\mathbb{F}_q)$ eine (große) Primzahl ist

*Trial-and-Error Ansatz*: Man erzeugt so lange Zufallskurven, bis die gewünschte Eigenschaft auftritt.

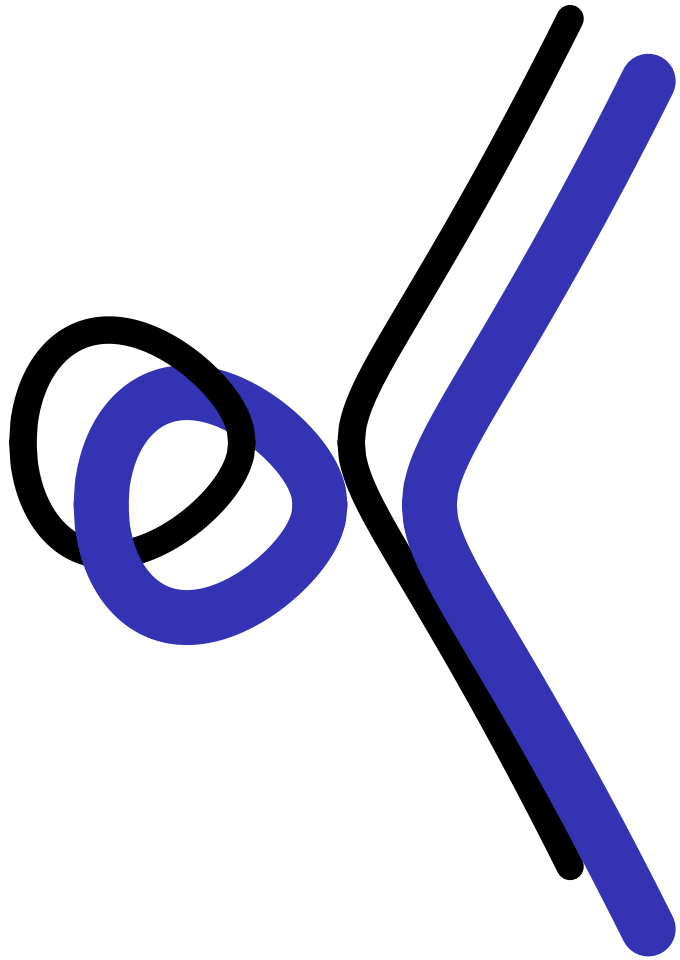
*Early-Abort Strategie*: Mit Hilfe von Divisionspolynomen kann man schnell entscheiden, ob $\#E(\mathbb{F}_q)$ kleine Primteiler hat (in diesem Fall wird die Ordnung erst gar nicht berechnet).

Sei $r$ eine Primzahl. Besitzt das $r$-te Divisionspolynom eine Nullstelle $x \in \mathbb{F}_q$ *und* existiert $y \in \mathbb{F}_q$ mit $y^2 = x^3 + ax + b$, so ist $\#E(\mathbb{F}_q)$ durch $r$ teilbar!

$r = 2, 3, 5, 7$ reicht bereits aus um ca. 77 Prozent aller Zufallskurven auszusieben.

Mit `search` konnte ich für alle $p \in [5, 293]$ elliptische Kurven finden, so dass $\#E(\mathbb{F}_q) \approx 2^{256}$ prim ist.

# *Vielen Dank für Ihre Aufmerksamkeit!*



Diplomarbeit, Vortrag & Kurven:
`http://niske.net/`