Die Punktegruppe-Operation

Elliptische Kurven Kryptographie Seminar

Richard Lindner

Institut für Theoretische Informatik
Technische Universität Darmstadt

28.04.2005 / Seminarvortrag Nr. 2

Gliederung

Gliederung

Gliederung

Gliederung

Die Punktegrupppen-Menge.

Definition

Menge der Punktegruppe $(\mathcal{E}(\mathbb{K}), +)$

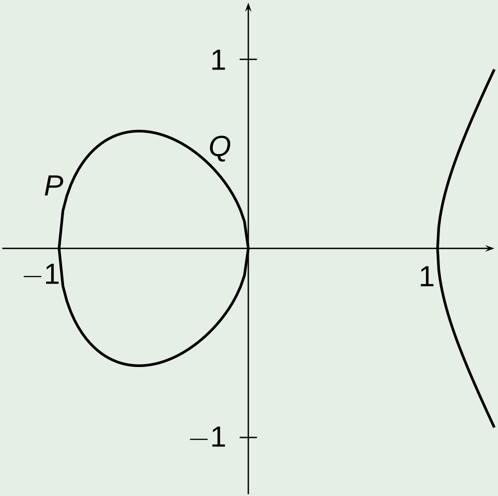
Die Punktegruppe einer elliptischen Kurve $\mathcal{E}$ über $\mathbb{K}$ ist die Menge der Punkte, die auf der Kurve liegen und der Fernpunkt $\mathcal{O} := (\infty, \infty)$.

$$\mathcal{E}(\mathbb{K}) := \left\{ P = (x, y) \in \mathbb{K}^2 : y^2 = x^3 + ax^2 + bx + c \right\} \cup \{\mathcal{O}\}$$

Gliederung

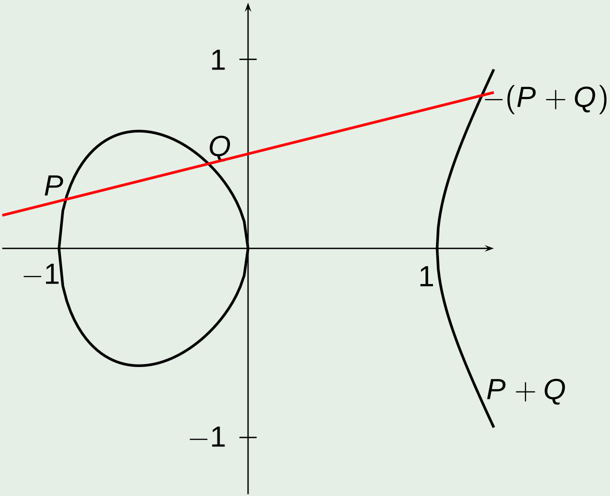
Example

$$\mathcal{E} : y^2 = x^3 - x$$



Example

$$\mathcal{E} : y^2 = x^3 - x$$



Gliederung

Axiome

Ist $(\mathcal{E}(\mathbb{K}), +)$ eine kommutative Gruppe?

- *Abgeschlossenheit* $+ : \mathcal{E}(\mathbb{K})^2 \to \mathcal{E}(\mathbb{K})$
- *Assoziativität* $P + (Q + R) = (P + Q) + R$
- *Neutrales Element* $P + 0 = P$
- *Inverse Elemente* $-P$
- *Kommutativität* $P + Q = Q + P$

Axiome

Ist $(\mathcal{E}(\mathbb{K}), +)$ eine kommutative Gruppe?

- *Abgeschlossenheit* $+ : \mathcal{E}(\mathbb{K})^2 \to \mathcal{E}(\mathbb{K})$
- *Assoziativität* $P + (Q + R) = (P + Q) + R$
- *Neutrales Element* $P + 0 = P$
- *Inverse Elemente* $-P$
- *Kommutativität* $P + Q = Q + P$

Axiome

Ist $(\mathcal{E}(\mathbb{K}), +)$ eine kommutative Gruppe?

- *Abgeschlossenheit* $+ : \mathcal{E}(\mathbb{K})^2 \to \mathcal{E}(\mathbb{K})$
- *Assoziativität* $P + (Q + R) = (P + Q) + R$
- *Neutrales Element* $P + 0 = P$
- *Inverse Elemente* $-P$
- *Kommutativität* $P + Q = Q + P$

Axiome

Ist $(\mathcal{E}(\mathbb{K}), +)$ eine kommutative Gruppe?

- *Abgeschlossenheit* $+ : \mathcal{E}(\mathbb{K})^2 \to \mathcal{E}(\mathbb{K})$
- *Assoziativität* $P + (Q + R) = (P + Q) + R$
- *Neutrales Element* $P + 0 = P$
- *Inverse Elemente* $-P$
- *Kommutativität* $P + Q = Q + P$

Axiome

Ist $(\mathcal{E}(\mathbb{K}), +)$ eine kommutative Gruppe?

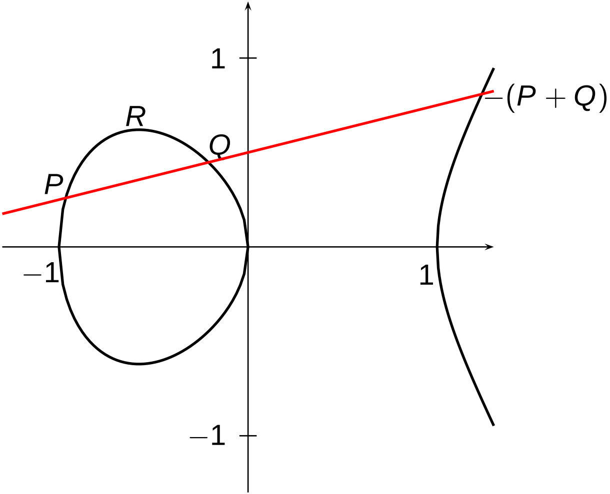
- *Abgeschlossenheit* $+ : \mathcal{E}(\mathbb{K})^2 \to \mathcal{E}(\mathbb{K})$
- *Assoziativität* $P + (Q + R) = (P + Q) + R$
- *Neutrales Element* $P + 0 = P$
- *Inverse Elemente* $-P$
- *Kommutativität* $P + Q = Q + P$

Axiome

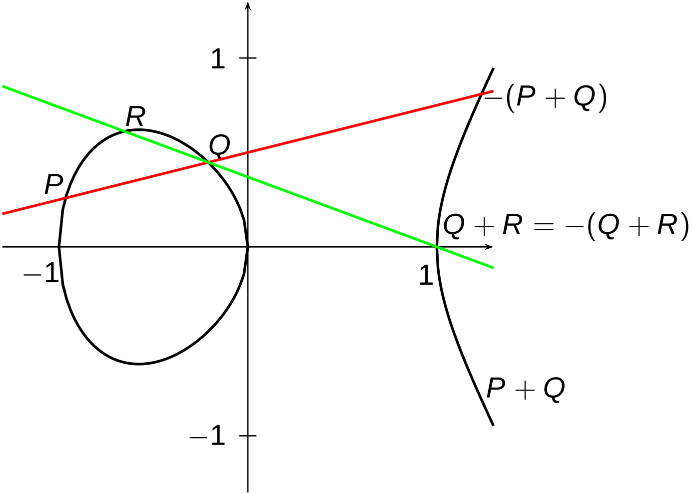
Ist $(\mathcal{E}(\mathbb{K}), +)$ eine kommutative Gruppe?

- *Abgeschlossenheit* $+ : \mathcal{E}(\mathbb{K})^2 \to \mathcal{E}(\mathbb{K})$
- *Assoziativität* $P + (Q + R) = (P + Q) + R$
- *Neutrales Element* $P + 0 = P$
- *Inverse Elemente* $-P$
- *Kommutativität* $P + Q = Q + P$

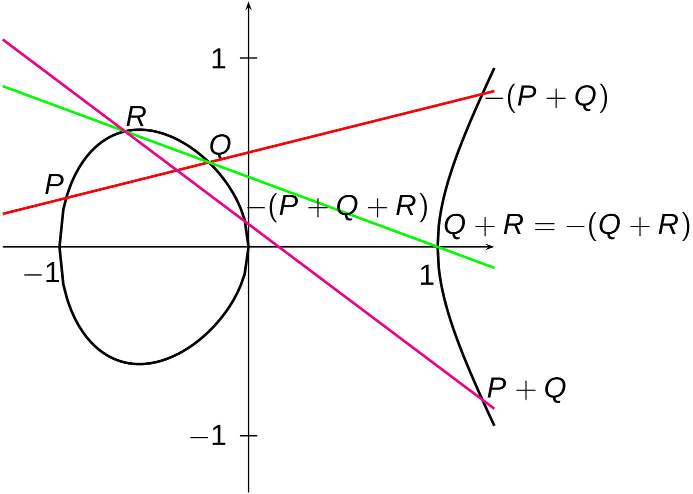
Assoziativität



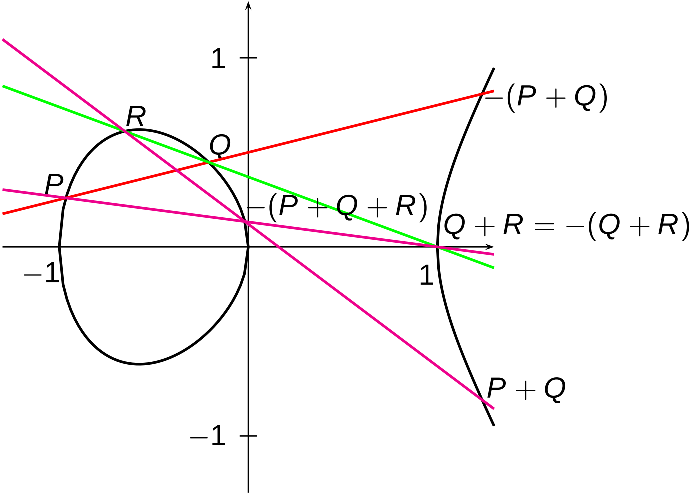
Assoziativität



Assoziativität



Assoziativität



Additionsformeln

Formeln für Charakteristik$(\mathbb{K}) > 3$

$$\mathcal{E} : y^2 = x^3 + ax + b$$

Gliederung

Die **Inversen** Elemente findet man mit einer Spiegelung an der X-Achse:

$$-P = -(x_P, y_P) = (x_P, -y_P)$$

Gliederung

Addieren **verschiedener** Punkte:
Seien $P = (x_P, y_P), Q = (x_Q, y_Q), R = (x_R, y_R)$, so daß

$$P + Q = R$$

Ist $x_P \neq x_Q$ können wir die Steigung der Gerade $\overline{PQ}$ berechnen:

$$s = \frac{y_Q - y_P}{x_Q - x_P}$$

R berechnet sich dann aus dieser Steigung s:

$$x_R = s^2 - x_P - x_Q$$

$$y_R = s \cdot (x_P - x_R) - y_P$$

Gliederung

Addieren von 2 **gleichen** Punkte, also eine Punkt-Verdoppelung.

$$2 \cdot P = R$$

Steigung der Tangente an $\mathcal{E}$ in P:

$$s = \frac{3x_P^2 + a}{2y_P}$$

Für $y_P \neq 0$ kann man aus der Steigung *wie zuvor* R berechnen:

$$x_R = s^2 - 2x_P$$

$$y_R = s \cdot (x_P - x_R) - y_P$$

Spezielle Formeln

Formeln für Charakteristik$(\mathbb{K}) = 2$

$$\mathcal{E} : y^2 + yx = x^3 + ax^2 + b$$

Durchs lösen eines Gleichungsystems ergibt sich:

- *Inverse* $-P = (x_P, y_P + x_P)$
- *„Steigung"* $s := \frac{y_Q + y_P}{x_Q + x_P}$
- *Addieren*

$$x_R = s^2 + s + x_P + x_Q + a$$

$$y_R = s \cdot (x_P + x_R) + x_R + y_P$$

- *Verdoppeln*

$$x_R = s^2 + s + a$$

$$y_R = x_P^2 + s \cdot x_R + x_R$$

Charakteristik 2

Durchs lösen eines Gleichungsystems ergibt sich:

- *Inverse* $-P = (x_P, y_P + x_P)$
- *„Steigung"* $s := \frac{y_Q + y_P}{x_Q + x_P}$
- *Addieren*

$$x_R = s^2 + s + x_P + x_Q + a$$

$$y_R = s \cdot (x_P + x_R) + x_R + y_P$$

- *Verdoppeln*

$$x_R = s^2 + s + a$$

$$y_R = x_P^2 + s \cdot x_R + x_R$$

Durchs lösen eines Gleichungsystems ergibt sich:

- *Inverse* $-P = (x_P, y_P + x_P)$
- *„Steigung“* $s := \frac{y_Q + y_P}{x_Q + x_P}$
- *Addieren*

$$x_R = s^2 + s + x_P + x_Q + a$$

$$y_R = s \cdot (x_P + x_R) + x_R + y_P$$

- *Verdoppeln*

$$x_R = s^2 + s + a$$

$$y_R = x_P^2 + s \cdot x_R + x_R$$

Durchs lösen eines Gleichungssystems ergibt sich:

- *Inverse* $-P = (x_P, y_P + x_P)$
- *„Steigung“* $s := \frac{y_Q + y_P}{x_Q + x_P}$
- *Addieren*

$$x_R = s^2 + s + x_P + x_Q + a$$

$$y_R = s \cdot (x_P + x_R) + x_R + y_P$$

- *Verdoppeln*

$$x_R = s^2 + s + a$$

$$y_R = x_P^2 + s \cdot x_R + x_R$$

The End

Vielen Dank für Ihre Aufmerksamkeit.