Elliptische Kurven

Sei K ein Körper (mit $\mathrm{char}(K) \notin \{2,3\}$), z.B. $K = \mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P} \setminus \{2,3\}$.

Definition

Eine *elliptische Kurve* (über K) ist eine ebene Kurve die durch eine Gleichung

$$\mathbf{E}: \quad \mathbf{y^2 = x^3 + ax + b} \qquad \text{(Weierstrass Gleichung)}$$

mit a, $b \in K$ und

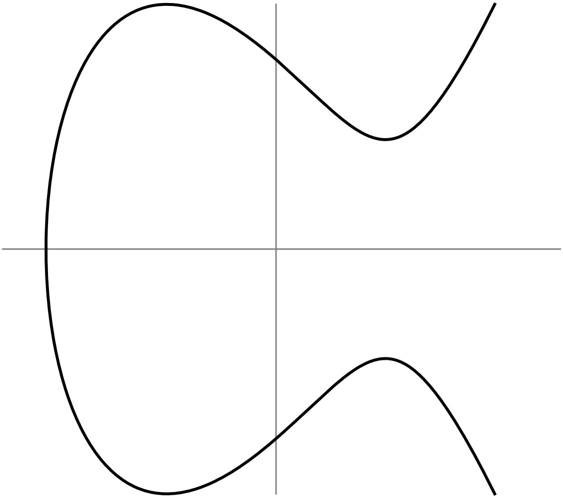
$$\Delta(E) = -16(4a^3 + 27b^2) \neq 0$$

gegeben ist.

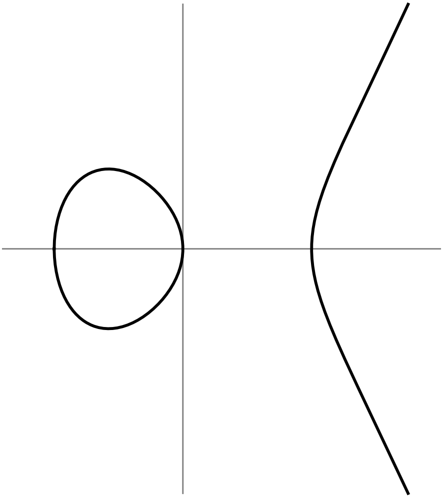
Bemerkung zur Definition

Sei C eine nicht-singuläre, absolut irreduzible, ebene projektive Kurve über K und $C(K) \neq \emptyset$.

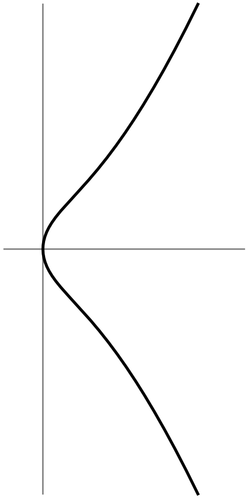
- Ist der Genus $g = 0$, so ist C ein Kegelschnitt (Gerade, Kreis, Ellipse, Parabel, Hyperbel)
- Ist $g = 1$, so ist C ein elliptische Kurve (lässt sich also durch eine Weierstrass Gleichung darstellen).



$$y^2 = x^3 - 3x + 3 \qquad (\Delta(E) = 2160)$$



$$y^2 = x^3 - x \qquad (\Delta(E) = 64)$$

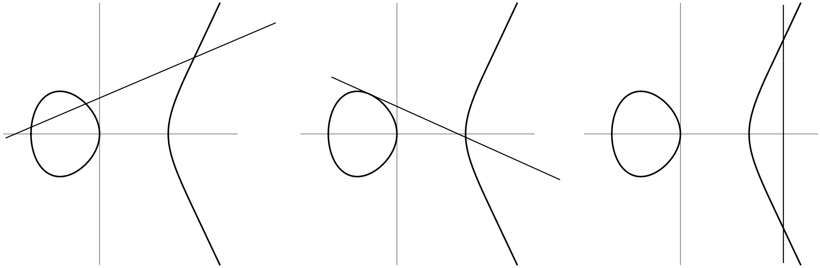


$$y^2 = x^3 + x \qquad (\Delta(E) = -64)$$

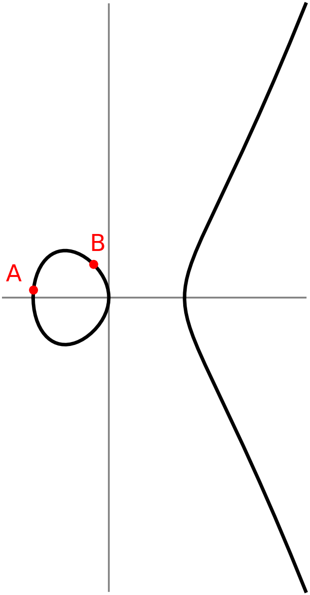
$$E(K) \coloneqq \{\, (x, y) \in K^2 \mid y^2 = x^3 + ax + b \,\} \cup \{O\}.$$

Auf $E(K)$ lässt sich eine Addition definieren, die $E(K)$ zu einer abelschen Gruppe macht!

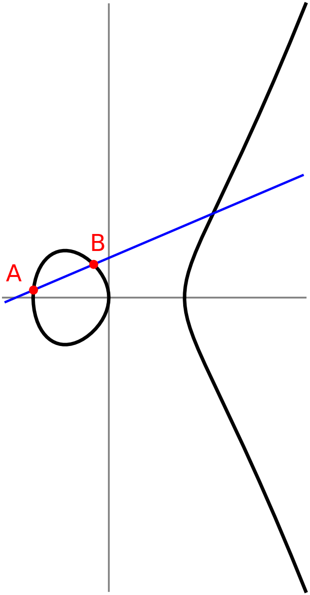
- E besitzt einen *Punkt im Unendlichen* $O = [0 : 1 : 0]$.
  (Formal: Projektiven Abschluss von E betrachten!)
- Eine Gerade g geht durch $O \Leftrightarrow g$ ist parallel zur y-Achse.
- Jede Gerade die $E(K)$ in zwei Punkten schneidet, schneidet $E(K)$ auch in einem dritten Punkt.
  (mit Vielfachheiten; O).



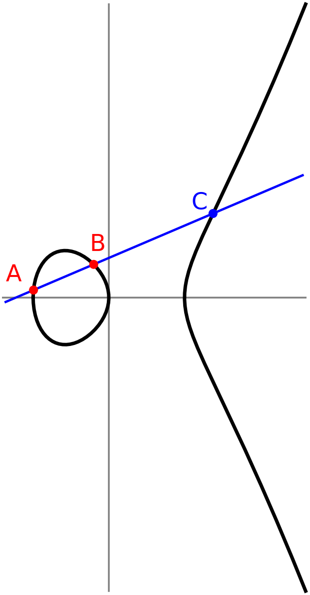
$A \oplus B$



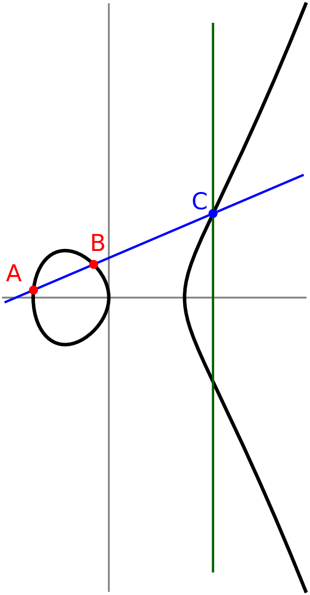
$A \oplus B$



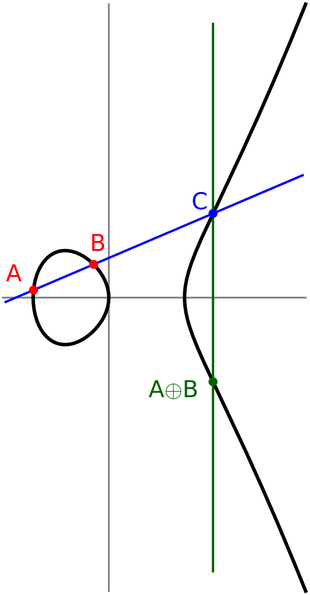
$A \oplus B$



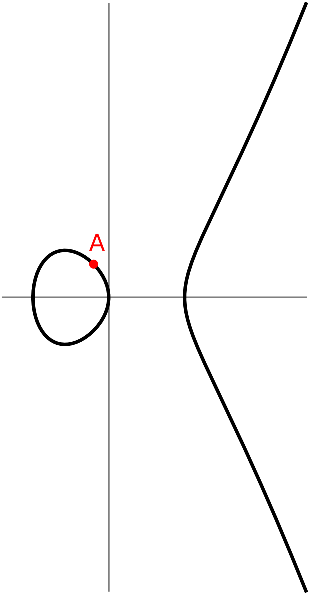
$A \oplus B$



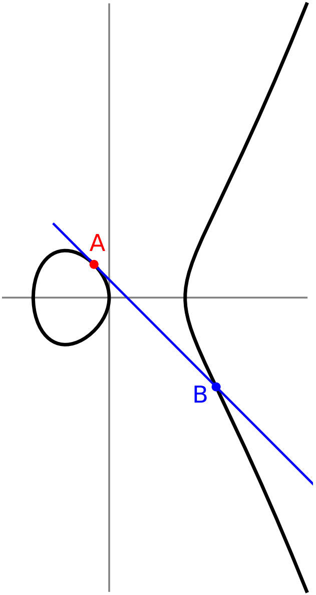
$A \oplus B$



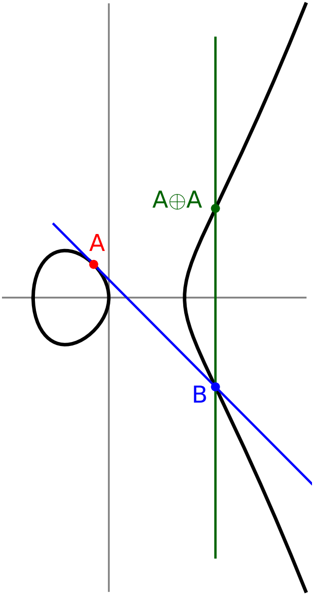
$A \oplus A (= [2]A)$



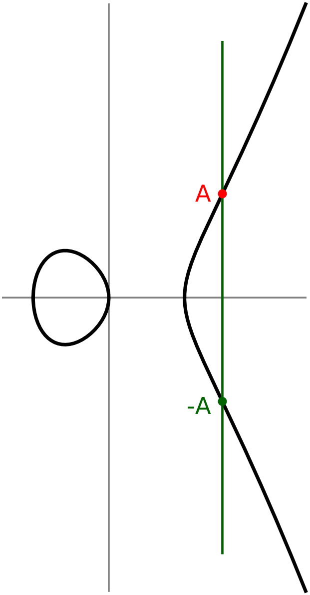
$A \oplus A (= [2]A)$



$A \oplus A (= [2]A)$

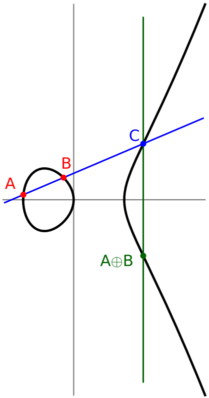


$O \oplus A, -A$



Für A, B, $C \in E(K)$ gilt:

A, B, C liegen auf einer Gerade $\Leftrightarrow A \oplus B \oplus C = O$.



Satz

$(E(K), \oplus, O)$ *ist eine abelsche Gruppe.*

Verknüpfung als Formel:

Für $A = (x_A, y_A)$, $B = (x_B, y_B)$

$$\begin{aligned} -A &= (x_A, -y_A) \\ A \oplus B &= (\lambda^2 - x_A - x_B,\ -\lambda - \nu) \qquad \text{(falls } A \neq -B\text{)} \end{aligned}$$

mit

$$\begin{aligned} \lambda &= \frac{y_B - y_A}{x_B - x_A} \qquad & \nu &= \frac{y_A x_B - y_B x_A}{x_B - x_A} \qquad & &\text{falls } A \neq \pm B, \\ \lambda &= \frac{3x_A^2 + a}{2y_A} \qquad & \nu &= \frac{-x_A^3 + a x_A + 2b}{2y_A} \qquad & &\text{falls } A = B, \end{aligned}$$

$E(\mathbb{Q})$

Satz (Mordell-Weil, 1922)

$E(\mathbb{Q})$ ist endlich erzeugt, d.h., es gibt $P_1, \ldots, P_k \in E(\mathbb{Q})$, so dass sich jeder Punkt $A \in E(\mathbb{Q})$ darstellen lässt als

$$A = [n_1]P_1 \oplus \cdots \oplus [n_k]P_k \qquad \textit{mit } n_1, \ldots, n_k \in \mathbb{Z}.$$

Struktursatz für endlich erzeugte abelsche Gruppen $\Rightarrow$

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}, \qquad \text{wobei}$$

$$E(\mathbb{Q})_{\text{tors}} = \{\, A \in E(\mathbb{Q}) \mid \operatorname{ord}(A) < \infty \,\} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_l\mathbb{Z}.$$

Torsionsgruppe

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}$$

Satz (Mazur, 1978)

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/n\mathbb{Z} \quad \textit{mit } n \in [1, 10] \cup \{12\}$$

oder

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad \textit{mit } n \in [1, 4].$$

Rang

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}$$

r ist eindeutig bestimmt und heißt *Rang* von E (über $\mathbb{Q}$).

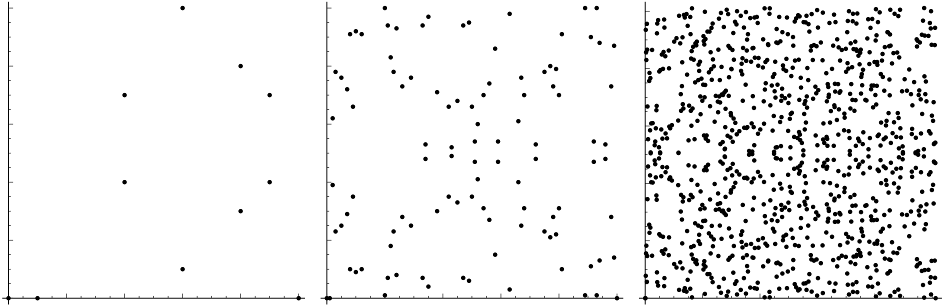
Vermutung

Über $\mathbb{Q}$ gibt es elliptische Kurven von beliebig großem Rang.

- Kurve mit $r \geq 28$ hat derzeit größten bekannten Rang (Elkies, 2006).
- Algorithmus um Erzeuger von $E(\mathbb{Q})$ zu berechnen (*Descent*)?

Endliche Körper

$$E: \quad y^2 = x^3 - x$$



$E(\mathbb{Z}/11\mathbb{Z})$, $E(\mathbb{Z}/101\mathbb{Z})$ und $E(\mathbb{Z}/1013\mathbb{Z})$
(je 12, 104, bzw. 968 Punkte).

Anzahl Rationaler Punkte über $\mathbb{Z}/p\mathbb{Z}$

Triviale Schranke: $|E(\mathbb{Z}/p\mathbb{Z})| \leq 2p + 1$.

Heuristik: $|E(\mathbb{Z}/p\mathbb{Z})| \approx p$.

Theorem (Hasse, 1933)

$$\Big| |E(\mathbb{Z}/p\mathbb{Z})| - (p+1) \Big| \leq 2\sqrt{p}.$$

Pollard-$(p-1)$-Methode zur Faktorisierung

Möchten $N \in \mathbb{N}$ faktorisieren.

1. Wähle $a \in [2, N]$; setze $B \leftarrow A$.
2. Für $i = 1,\ 2,\ \dots,\ L$:
   2.1 $B \leftarrow B^i \mod N$.
   2.2 $d \leftarrow \mathrm{ggT}(B-1, N)$.
      - Falls $1 < d < N$: d ist nicht-trivialer Faktor!
      - Falls $d = N$: Neustart mit anderem Startwert A.

Funktionsweise:

- Sei p Primfaktor von N, mit $p - 1 = q_1^{e_1} \cdots q_r^{e_r}$.
- Berechnen $A^{i!}$ für $i \in [1, L]$.
- Ist $p - 1 \mid i!$, so ist $p \mid A^{i!} - 1$ (Fermat).
- Wenn $L \geq \max_{1 \leq i \leq r} e_i q_i$ ist $p - 1 \mid L!$
- $p - 1$ **muss *glatt* sein!**

Lenstras Faktorisierungsalgorithms

Um $N \in \mathbb{N}$ zu faktorisieren:

1. Wähle elliptische Kurve E mod N und $A \in E(\mathbb{Z}/N\mathbb{Z})$; $B \leftarrow A$.
   (Wähle zuerst a, $A = (x_A, y_A)$ zufällig, dann $b = y_A^2 - x_A^3 - ax_A$).
2. Für $i = 2, 3, \ldots, L$:
   2.1 $B \leftarrow [i]B$ in $E(\mathbb{Z}/N\mathbb{Z})$.
   2.2 Dabei muss man Elemente $\overline{d} \in \mathbb{Z}/N\mathbb{Z}$ invertieren; schlägt dies fehl (also $\mathrm{ggT}(N, d) > 1$), so ist (wahrscheinlich) $\mathrm{ggT}(N, d)$ ein nicht-trivialer Teiler von N.
3. Wähle eine neue Kurve und einen neuen Punkt und beginne von vorn.

Funktionsweise:

- Wir berechnen $B = [i!]A$ für $i = 1, \dots, L$.
- $p \mid N$ und $|E(\mathbb{Z}/p\mathbb{Z})| \mid L!$, so ist $[L!]A = 0$ in $E(\mathbb{Z}/p\mathbb{Z})$
  $\Rightarrow$ Invertieren in $E(\mathbb{Z}/N\mathbb{Z})$ schlägt fehl!
- $|E(\mathbb{Z}/p\mathbb{Z})| = p + 1 + a_p$ mit $|a_p| \leq 2\sqrt{p}$ muss glatt sein.
- $|E(\mathbb{Z}/p\mathbb{Z})|$ lässt sich durch Wahl der Kurve variieren.
- Funktioniert gut, wenn N kleine Primfaktoren besitzt.

$$\text{Pollard-}(p-1) \text{ vs. Lenstra:} \quad (\mathbb{Z}/p\mathbb{Z})^\times \text{ vs. } E(\mathbb{Z}/p\mathbb{Z}).$$

Weiterführende Literatur

Elementar:

Joseph H. Silverman und John T. Tate. *Rational points on elliptic curves*. Second. Undergraduate Texts in Mathematics. Springer, Cham, 2015, S. xxii+332. ISBN: 978-3-319-18587-3; 978-3-319-18588-0. DOI: 10.1007/978-3-319-18588-0.

Mit etwas algebraischer Zahlentheorie/algebraischer Geometrie:

J. W. S. Cassels. *Lectures on elliptic curves*. Bd. 24. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1991, S. vi+137. ISBN: 0-521-41517-9; 0-521-42530-1. DOI: 10.1017/CBO9781139172530.

Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Bd. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, S. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6.