Elliptische Kurven und Kryptographie

Inhalt

1. Hintergrund
2. Einführung in die Grundlagen
3. Spezifische Eigenschaften von elliptischen Kurven
4. Additions-Operation auf elliptischen Kurven
5. Kryptographie auf elliptischen Kurven (später)

Hintergrund

- seit über 100 Jahren in der Mathematik ein Thema
- seit ca. 30 Jahren: Anwendungen für verschiedene Gebiete entdeckt
  - **Bsp 1:** Faktorisierung von Zahlen mit Hilfe elliptischer Kurven (Lenstra, '87)
  - **Bsp 2:** Krypto-System basierend auf elliptischen Kurven (Miller, Koblitz, '86)

Hintergrund

Repetition

- El Gamal Verfahren (Kapitel 4): basiert auf diskretem Logarithmus.
- ”Schwäche” dieses Systems: In primen Restklassengruppen gibt es verschiedene Ansätze, um diskrete Logarithmen zu bestimmen.
  $\rightarrow$ erfordert relative grosse Schlüssel-Längen.

Grund-Idee des Krypto-Systems von Miller und Koblitz

- **Verbesserung:** neue Gruppe = Punkte auf einer elliptischen Kurve
- Das diskrete Logarithmus-Problem ist für solche Gruppen schwieriger zu knacken (gemäss heutigem Stand).
- **Vorteil:** Schlüssel-Längen können nun viel kleiner gewählt werden, um die entsprechende Sicherheitsanforderung zu erfüllen
  (im Vergleich zu El Gamal mit primen Restklassengruppen).

Definition (unvollständige Version)

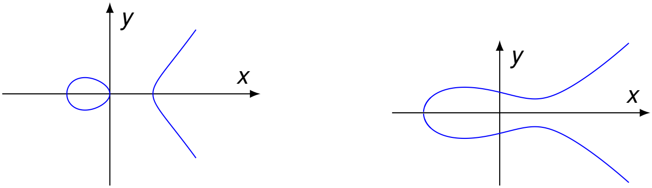
Eine elliptische Kurve ist gegeben durch eine Gleichung der Form

$$y^2 = x^3 + ax + b$$

Beispiel: $y^2 = x^3 - 2x$

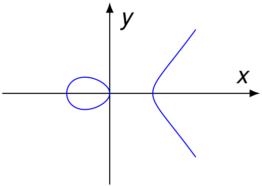
Aufgabe: Skizziere die Kurve der Gleichung im obigen Beispiel.

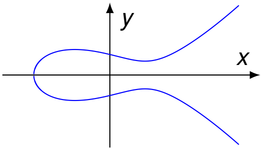
- Elliptische Kurven haben die Form ”Küste mit Insel” oder ”Kleiderbügel”



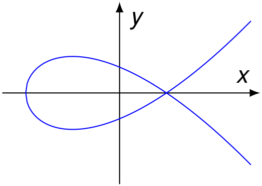
Einführung in die Grundlagen

- Elliptische Kurven haben die Form ”Küste mit Insel” oder ”Kleiderbügel”



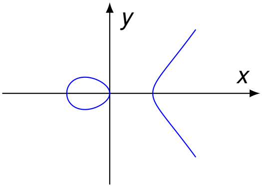


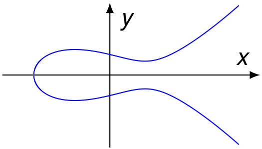
- Grenzfall: ”Küste und Insel treffen sich”



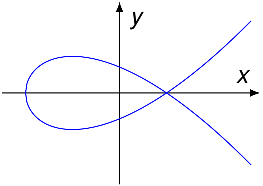
Einführung in die Grundlagen

- Elliptische Kurven haben die Form "Küste mit Insel" oder "Kleiderbügel"



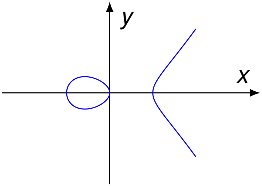


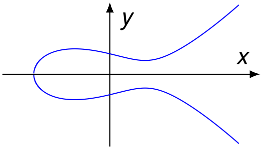
- Grenzfall: "Küste und Insel treffen sich"
  - problematisch für gewisse Konstruktionen



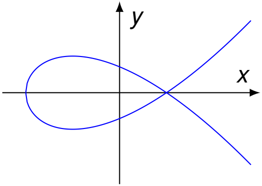
Einführung in die Grundlagen

- Elliptische Kurven haben die Form ”Küste mit Insel” oder ”Kleiderbügel”

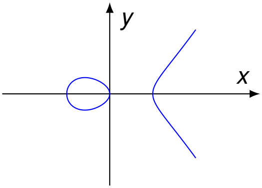


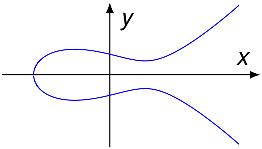


- Grenzfall: ”Küste und Insel treffen sich”
  - problematisch für gewisse Konstruktionen
  - wollen diesen Fall ausschliessen!

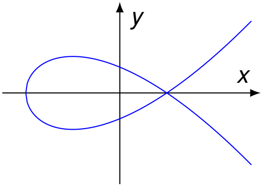


- Elliptische Kurven haben die Form ”Küste mit Insel” oder ”Kleiderbügel”



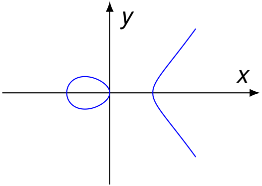


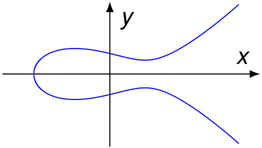
- Grenzfall: ”Küste und Insel treffen sich”
  - problematisch für gewisse Konstruktionen
  - wollen diesen Fall ausschliessen!
  - Charakterisierung: Nullstelle und lokales Minimum (des oberen Teils) treffen zusammen



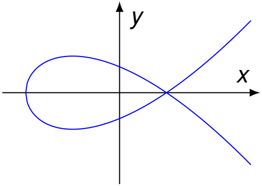
Einführung in die Grundlagen

- Elliptische Kurven haben die Form ”Küste mit Insel” oder ”Kleiderbügel”





- Grenzfall: ”Küste und Insel treffen sich”
  - problematisch für gewisse Konstruktionen
  - wollen diesen Fall ausschliessen!
  - Charakterisierung: Nullstelle und lokales Minimum (des oberen Teils) treffen zusammen
  - Analyse via Differentialrechnung ergibt: Dies passiert, wenn $4a^3 + 27b^2 = 0$.



Erweiterung der Definition, um Problemfall auszuschliessen

Definition (unvollständige Version)

Eine elliptische Kurve ist gegeben durch eine Gleichung der Form

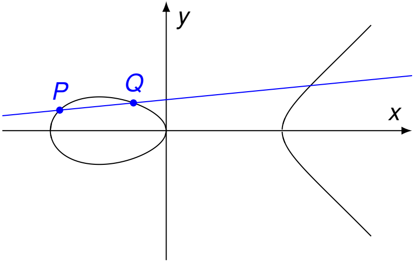
$$y^2 = x^3 + ax + b$$

mit $4a^3 + 27b^2 \neq 0$

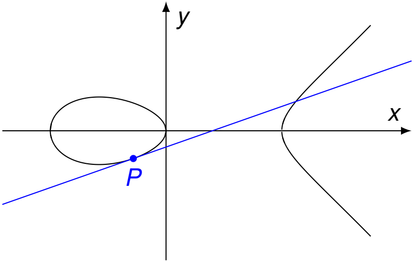
Spezifische Eigenschaften von Elliptischen Kurven

1. Verbindet man zwei Punkte, die
   - beide auf der Kurve liegen, und
   - versch. x-Koordinaten haben

   dann gibt es einen weiteren Schnittpunkt.



2. Legt man die Tangente an einen Punkt auf der Kurve, dann gibt es einen weiteren Schnittpunkt.



Bem: Der "Problemfall" (s. letzte Folie) erfüllt diese beiden Bed. nicht.

Spezifische Eigenschaften von Elliptischen Kurven

Bem: Um eine Addition von Punkten zu definieren, wird ein Zusatzkonstrukt benötigt:
Der "unendlich ferne Punkt" (Bezeichnung: O).

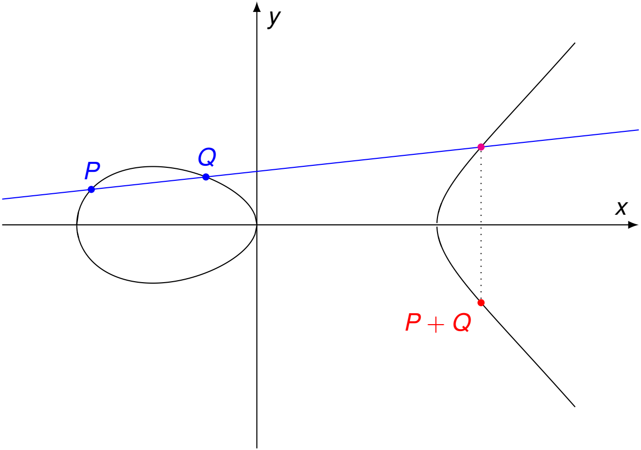
Definition

Für gegebene a, b mit $4a^3 + 27b^2 \neq 0$ beinhaltet die entsprechende elliptische Kurve alle Punkte (x, y) mit der Eigenschaft

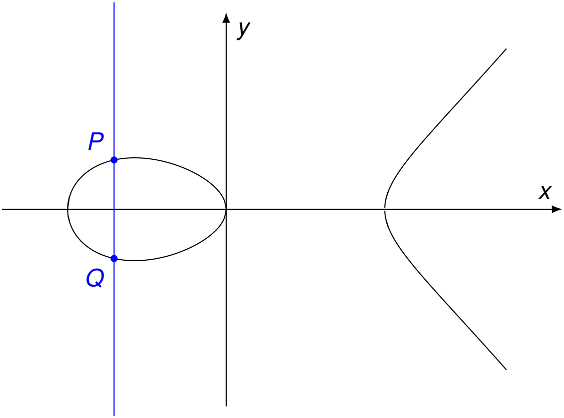
$$y^2 = x^3 + ax + b$$

sowie einen Zusatzpunkt O.

Standard-Fall



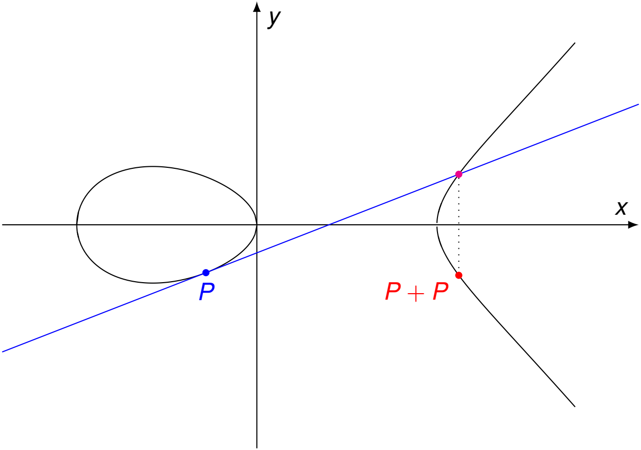
Sonderfall 1: P und Q haben die gleiche x-Koordinate.



$P + Q = O$

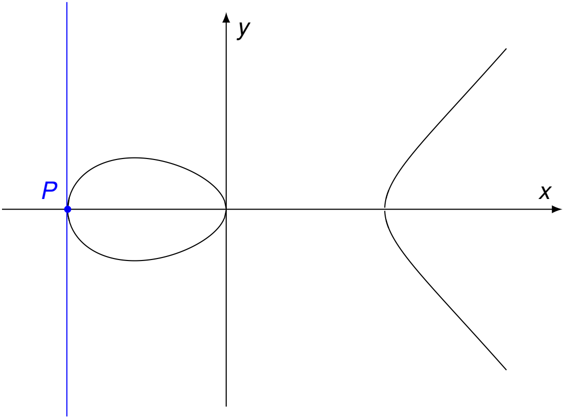
Additions-Operation – Illustration

Sonderfall 2: $P = Q$, $\quad y$-Koord ist $\neq 0$



Additions-Operation – Illustration

Sonder-Fall 3: $P = Q, \quad y\text{-Koord ist} = 0$



$$P + P = O$$

Additions-Operation – Illustration

Applet: https://www.desmos.com/calculator/ialhd71we3

Additions-Operation – Rechnung

Herleitungs-Idee: s. Wandtafel

Resultierende Formeln

Für Punkte $P = (x_1; y_1)$ und $Q = (x_2; y_2)$ auf der Kurve gilt:

a) Falls $x_1 \neq x_2$:

$m := \frac{y_2 - y_1}{x_2 - x_1}, \quad x_3 := m^2 - x_1 - x_2, \quad y_3 := -m(x_3 - x_1) - y_1$ und

$P + Q := (x_3; y_3)$

b) Falls $x_1 = x_2$ und $y_1 = y_2 \neq 0$:

$m := \frac{3x_1^2 + a}{2y_1}, \quad x_3 := m^2 - 2x_1, \quad y_3 := -m(x_3 - x_1) - y_1$ und

$P + Q := (x_3; y_3)$

c) Falls $x_1 = x_2$ und $y_1 = -y_2$ setzen wir $P + Q := O$.

d) $P + O = O + P = P$.

Bem: $2P = P + P$

Ausblick

- **Bem:** Elliptische Kurven lassen sich über (fast) allen Körpern K definieren.
- Bisherige Betrachtung: für $K = \mathbb{R}$
- Für kryptographische Anwendungen: geeigneter sind elliptische Kurven über **endliche Körper**, z.B. $\mathbb{Z}_p$.
- Anpassung der Definition

Definition

Für gegebene a, b mit $4a^3 + 27b^2 \neq 0$ beinhaltet die entsprechende elliptische Kurve alle Punkte (x, y) mit $x, y \in K$ und der Eigenschaft

$$y^2 = x^3 + ax + b$$

sowie einen Zusatzpunkt O.