Elliptische Kurven Kryptographie

Kevin Kappelmann, Lukas Stevens

Technische Universität München

21. Mai 2016

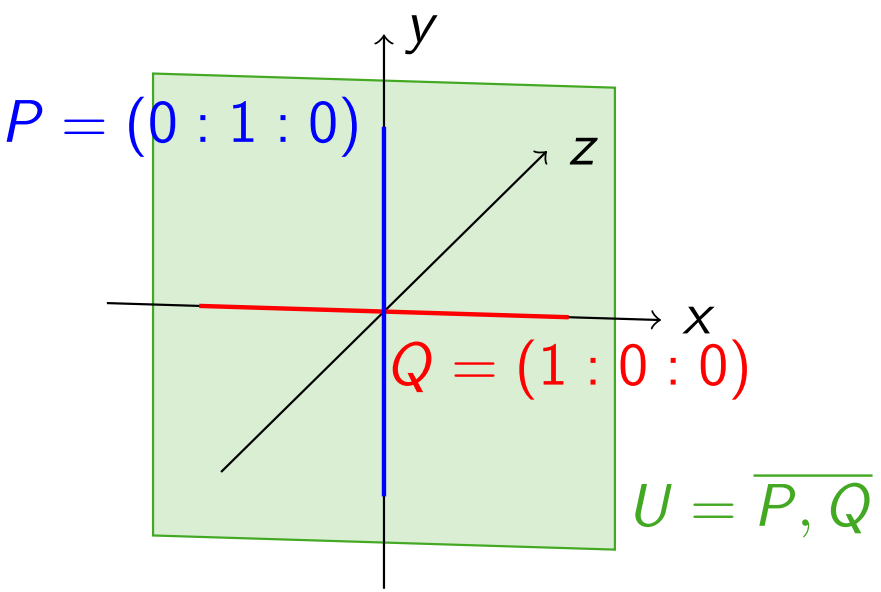
Überblick

Elliptische Kurven – Die unendlich ferne Gerade

- Wähle $U := \overline{P, Q}$ mit $P = (1 : 0 : 0), Q = (0 : 1 : 0)$.

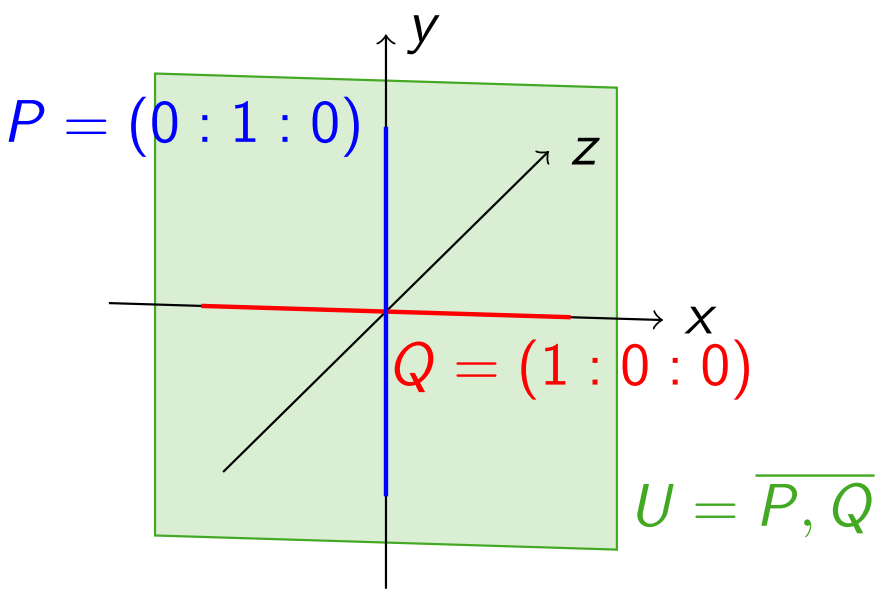
Elliptische Kurven – Die unendlich ferne Gerade

- Wähle $U := \overline{P, Q}$ mit $P = (1 : 0 : 0), Q = (0 : 1 : 0)$.
- U ist im dreidimensionalen Raum genau die x,y-Ebene mit $z = 0$.



Elliptische Kurven – Die unendlich ferne Gerade

- Wähle $U := \overline{P, Q}$ mit $P = (1 : 0 : 0), Q = (0 : 1 : 0)$.
- U ist im dreidimensionalen Raum genau die x,y-Ebene mit $z = 0$.



- Wir bezeichnen U als die **unendlich ferne Gerade**.

Elliptische Kurven – Die unendlich ferne Gerade

Lemma

Gegeben sei die projektive Ebene $(\mathcal{P}, \mathcal{G}) = PG(2, \mathbb{F})$ *und die unendlich ferne Gerade* U*, dann ist die Abbildung*

$$\phi : \mathbb{F}^2 \to \mathcal{P}_U, \ (a, b) \mapsto (a : b : 1)$$

bijektiv und bildet Geraden auf Geraden ab, d.h. ϕ *ist ein Isomorphismus von affinen Ebenen.*

Elliptische Kurven – Weierstraß-Gleichung

Erinnerung: Punktemenge von PG(2, $\mathbb{F}$)

$$P = \{(x : y : z) \mid (x, y, z) \in \mathbb{F}^3 \setminus \{\mathbf{0}\}\}$$

Definition

Eine elliptische Kurve $E \subseteq P$ ist durch die Lösung der **Weierstraß-Gleichung**

$$0 = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

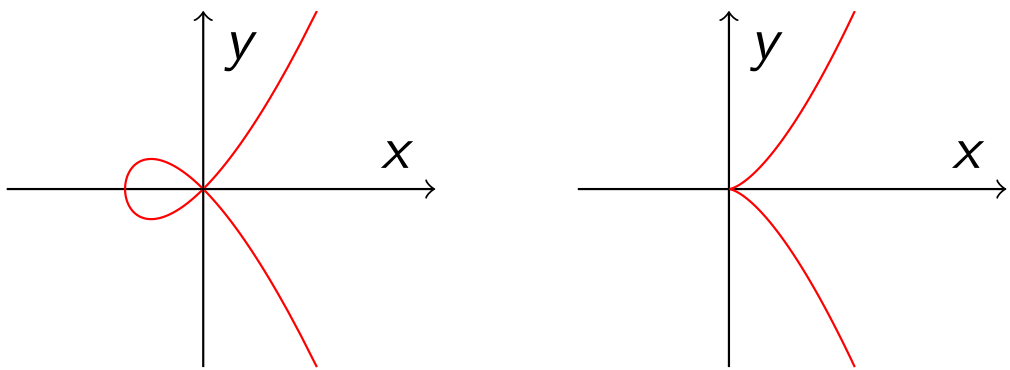
gegeben, wobei $a_i \in \mathbb{F}$ gilt und die Lösung keine Singularitäten besitzen darf.

Elliptische Kurven – Weierstraß-Gleichung

Definition

Eine Kurve E ist **singulär** in einem Punkt $P = (a : b : c) \in E$, wenn gilt:

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$$



(a) $y^2 = x^3 + x^2$ (b) $y^2 = x^3$

Abbildung: Kurven mit Singularitäten (Knoten und Spitze)

Elliptische Kurven – Weierstraß-Gleichung

- Wir schränken ein: Die *Charakteristik* des Körpers $\mathbb{F}$ soll nicht 2 und nicht 3 sein: $char\ \mathbb{F} \neq 2, 3$.

Elliptische Kurven – Weierstraß-Gleichung

- Wir schränken ein: Die *Charakteristik* des Körpers $\mathbb{F}$ soll nicht 2 und nicht 3 sein: $char\ \mathbb{F} \neq 2, 3$.
- Dies bedeutet, dass $1 + 1 \neq 0$ bzw. $1 + 1 + 1 \neq 0$, wobei $0, 1$ die neutralen Elemente der Addition bzw. Multiplikation von $\mathbb{F}$ sind.

Elliptische Kurven – Weierstraß-Gleichung

- Wir schränken ein: Die *Charakteristik* des Körpers $\mathbb{F}$ soll nicht 2 und nicht 3 sein: $char\ \mathbb{F} \neq 2, 3$.
- Dies bedeutet, dass $1 + 1 \neq 0$ bzw. $1 + 1 + 1 \neq 0$, wobei $0, 1$ die neutralen Elemente der Addition bzw. Multiplikation von $\mathbb{F}$ sind.
- Unter diesen Voraussetzungen können wir die Weierstraß-Gleichung vereinfachen zu:

$$0 = Y^2Z - X^3 - aXZ^2 - bZ^3$$

Elliptische Kurven – Weierstraß-Gleichung

- Wir betrachten die elliptische Kurve

$$E = \{(x : y : z) \mid 0 = y^2z - x^3 - axz^2 - bz^3\}$$

Elliptische Kurven – Weierstraß-Gleichung

- Wir betrachten die elliptische Kurve

$$E = \{(x : y : z) \mid 0 = y^2z - x^3 - axz^2 - bz^3\}$$

- Wir erinnern uns an die unendlich fernen Gerade $U = \overline{(0 : 1 : 0), (1 : 0 : 0)}$.

Elliptische Kurven – Weierstraß-Gleichung

- Wir betrachten die elliptische Kurve

$$E = \{(x : y : z) \mid 0 = y^2z - x^3 - axz^2 - bz^3\}$$

- Wir erinnern uns an die unendlich fernen Gerade $U = \overline{(0 : 1 : 0), (1 : 0 : 0)}$.
- Es gilt: $U \cap E = (0 : 1 : 0) =: \mathcal{O}$, d.h. es liegt nur $\mathcal{O}$ auf unserer Kurve E.

Elliptische Kurven – Weierstraß-Gleichung

- Wir betrachten die elliptische Kurve

$$E = \{(x : y : z) \mid 0 = y^2z - x^3 - axz^2 - bz^3\}$$

- Wir erinnern uns an die unendlich fernen Gerade $U = \overline{(0 : 1 : 0), (1 : 0 : 0)}$.
- Es gilt: $U \cap E = (0 : 1 : 0) =: \mathcal{O}$, d.h. es liegt nur $\mathcal{O}$ auf unserer Kurve E.
- Wir bezeichnen $\mathcal{O}$ als den **unendlich fernen Punkt**.

Bullet Points

- Lorem ipsum dolor sit amet, consectetur adipiscing elit
- Aliquam blandit faucibus nisi, sit amet dapibus enim tempus eu
- Nulla commodo, erat quis gravida posuere, elit lacus lobortis est, quis porttitor odio mauris at libero
- Nam cursus est eget velit posuere pellentesque
- Vestibulum faucibus velit a augue condimentum quis convallis nulla gravida

Blocks of Highlighted Text

Block 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Block 2

Pellentesque sed tellus purus. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum quis magna at risus dictum tempor eu vitae velit.

Block 3

Suspendisse tincidunt sagittis gravida. Curabitur condimentum, enim sed venenatis rutrum, ipsum neque consectetur orci, sed blandit justo nisi ac lacus.

Multiple Columns

Heading

1. Statement
2. Explanation
3. Example

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Table

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Tabelle: Table caption

Theorem

Satz (Mass–energy equivalence)

$E = mc^2$

Verbatim

Beispiel (Theorem Slide Code)

```
\begin{frame}
\frametitle{Theorem}
\begin{theorem}[Mass--energy equivalence]
$E = mc^2$
\end{theorem}
\end{frame}
```

Figure

Uncomment the code on this slide to include your own image from the same directory as the template TeX file.

References

John Smith (2012)

Title of the publication

Journal Name 12(3), 45 – 678.

The End