

Elliptische Kurven

Kevin Kappelman, Lukas Stevens

15. April 2016

Inhaltsverzeichnis

1	Motivation und Geschichte	3
2	Grundbegriffe	3
2.1	Affine Ebenen	3
2.2	Projektive Ebenen	3
2.2.1	Die projektive Ebene $\text{PG}(2, \mathbb{F})$	3
2.2.2	Konstruktion affiner Ebenen aus projektiven Ebenen	3
3	Elliptische Kurven E	3
3.1	Definiton elliptischer Kurven	3
3.2	Die unendliche Gerade über $\text{PG}(2, \mathbb{F})$	4
3.3	Affine Darstellung elliptischer Kurven	4
4	Eine Gruppe über E	4
4.1	Tangenten elliptischer Kurven	4
4.2	Schnittpunkte von Geraden mit elliptischen Kurven	4
4.3	Die Schnittpunkt-Verknüpfung \oplus über E	4
4.4	Die Gruppe $(E, +)$	4
5	Anwendung elliptischer Kurven in der Kryptologie	4
5.1	Elgamal	4
5.2	Noch einen für Signaturen	4

Darstellungsformen nicht vergessen! Edwards Kurven und so
Beispiel zitier [1, Kapitel 5, S. 215]

1 Motivation und Geschichte

Macht Kevin

Einleitung, warum elliptische Kurven, etc. (geschichtliches?)

2 Grundbegriffe

2.1 Affine Ebenen

Definition, Beispiele

2.2 Projektive Ebenen

Definition

2.2.1 Die projektive Ebene $\mathbb{P}G(2, \mathbb{F})$

Konstruktion, Beispiel

2.2.2 Konstruktion affiner Ebenen aus projektiven Ebenen

Beweis, Beispiel

3 Elliptische Kurven E

Macht Lukas

3.1 Definition elliptischer Kurven

Wir haben bereits die projektive Ebene $\mathbb{P}G(2, \mathbb{F})$ über beliebige Körper \mathbb{F} eingeführt.
Diese hat die folgende Punktmenge:

$$P = \{(u : v : w) \mid (u, v, w) \in \mathbb{F}^3 \setminus (0, 0, 0)\} \quad (1)$$

Nun wollen wir die Punktmenge der elliptischen Kurve einführen. Dazu benötigen wir
Polynome in drei Unbestimmten. Der Polynomring mit drei Unbestimmten über \mathbb{F} ist mit

$$\mathbb{F}[X, Y, Z] = \left\{ \sum_{k,l,m \geq 0} a_{k,l,m} X^k Y^l Z^m \mid a_{k,l,m} \in \mathbb{F} \right\} \quad (2)$$

definiert.

3.2 Die unendliche Gerade über $\text{PG}(2, \mathbb{F})$

Isomorphismus von $\mathbb{F}^2 \rightarrow \mathcal{P}_U$

3.3 Affine Darstellung elliptischer Kurven

Erklärung, Beispiel(Graphen)

4 Eine Gruppe über E

Macht Kevin bis 4.3

4.1 Tangenten elliptischer Kurven

4.2 Schnittpunkte von Geraden mit elliptischen Kurven

Unendlich ferne Gerade mit Schnittpunkt \mathcal{O} , Affine Geraden, Parallele zur y-Achse

4.3 Die Schnittpunkt-Verknüpfung \oplus über E

Definition, Beweis der Abgeschlossenheit, graphische Interpretation

4.4 Die Gruppe $(E, +)$

Macht Lukas bis fertig

Gruppe ist abelsch mit neutralem Element \mathcal{O} , Beispiel

5 Anwendung elliptischer Kurven in der Kryptologie

5.1 Elgamal

Welche Charakteristiken für elliptische Kurven, Domänenparameter

5.2 Noch einen für Signaturen

Welche Charakteristiken für elliptische Kurven, Domänenparameter

Literatur

[1] Test author. Elliptic bla bla, 2012.