



Übungsblatt 3

Elliptische Kurven

Die Besprechung erfolgt am Mittwoch, dem 21.5.2014,
um 12:00 Uhr in He18 - E60.

Aufgabe 1

(2+4+4)

Sei K ein Körper und C die ebene projektive Kurve gegeben durch die affine Gleichung $y^2 = x^3$. Sei ferner $C_{ns}(K) := C(K) \setminus \{(0,0)\}$. Wir wollen auf $C_{ns}(K)$ eine Gruppenstruktur definieren und gehen dabei wie folgt vor: Das Lemma von Bezout gilt auch für C , darum kann man die Verknüpfung $* : C(K) \times C(K) \rightarrow C(K)$ wie üblich definieren.

- (a) Zeigen Sie, dass sich $*$ zu einer Abbildung $C_{ns}(K) \times C_{ns}(K) \rightarrow C_{ns}(K)$ einschränkt, d.h. für zwei Punkte $P, Q \in C_{ns}(K)$ gilt auch $P * Q \in C_{ns}(K)$.

Bemerkung: An welcher Stelle verwendet man, dass $(0,0)$ ein singulärer Punkt ist?

- (b) Zeigen Sie, dass $(C_{ns}(K), +)$ eine Gruppe ist und die Verknüpfung für zwei Punkte $(x_1, y_1), (x_2, y_2)$ mit $x_1 \neq x_2$ gegeben ist durch

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{\mu^2}{x_1 x_2}, \frac{-\mu^3}{y_1 y_2} \right), \quad \text{mit } \mu = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}.$$

Bemerkung: Die Assoziativität müssen Sie nicht zeigen.

- (c) Zeigen Sie, dass die Abbildung

$$\Phi : C_{ns}(K) \rightarrow K, \quad P \mapsto \begin{cases} \frac{x}{y} & \text{falls } P = (x, y), \\ 0 & \text{falls } P = O, \end{cases}$$

ein Gruppenisomorphismus ist.

Bemerkung: Obige singuläre Kurve ist ungeeignet für Anwendungen in der Kryptographie, da ihre Gruppe $C_{ns}(K)$ der nicht-singulären K -rationalen Punkte isomorph zu $(K, +)$ ist und man daher das diskrete Logarithmus Problem auf $C_{ns}(K)$ sehr leicht lösen kann.

Aufgabe 2

(2+2+3+3)

Sei $p \equiv 3 \pmod{4}$ eine Primzahl, $a \in \mathbb{F}_p^*$ und E die projektive Kurve gegeben durch die affine Gleichung $y^2 = x^3 + ax$.

- (a) Zeigen Sie, dass E glatt ist.
(b) Zeigen Sie, dass $-1 \in \mathbb{F}_p^*$ kein Quadrat ist.

Hinweis: Benutzen Sie $p \equiv 3 \pmod{4}$.

Bitte wenden!

- (c) Zeigen Sie, dass für alle $x \in \mathbb{F}_p$ mit $f(x) := x^3 + ax \neq 0$ gilt:

$$\left(\frac{f(x)}{p}\right) = 1 \quad \Leftrightarrow \quad \left(\frac{f(-x)}{p}\right) = -1$$

Hier bezeichnen wir mit $\left(\frac{\cdot}{p}\right)$ wieder das Legendre-Symbol.

- (d) Benutzen Sie die vorherigen Aufgabenteile, um die Anzahl der Elemente in $E(\mathbb{F}_p)$ zu zählen.