ulm university universität
uulm

Prof. Dr. Irene Bouw
Christian Steck
Sommersemester 2014

Übungsblatt 8

Elliptische Kurven

Die Besprechung erfolgt am Mittwoch, dem 9.7.2014,
um 12:00 Uhr in He18 - E60.

Aufgabe 1 (1+3+3)

Sei p eine ungerade Primzahl und $q = p^n$ für ein $n \in \mathbb{N}$. Wir betrachten die elliptische Kurve

$$E : y^2 = x^3 + ax + b, \quad \text{mit } a, b \in \mathbb{F}_q.$$

Sei ferner $\varphi_p : E \to E^{(p)}$, $(x, y) \mapsto (x^p, y^p)$ der p-Frobeniusmorphismus.

(a) Zeigen Sie, dass φ_p eine Isogenie ist.

(b) Sei $K = \mathbb{F}_q(E^{(p)}) = \mathbb{F}_q(x^p, y^p)/((y^p)^2 - (x^p)^3 - a^p x^p - b^p)$. Zeigen Sie, dass eine Funktion $h \in \mathbb{F}_q(E)$ genau dann in K liegt, wenn es ein $g \in \mathbb{F}_q(E)$ gibt, mit $g^p = h$.

Bemerkung: Verwenden Sie, dass $\mathbb{F}_q$ perfekt ist. Dies impliziert insbesondere, dass die Abbildung $\mathbb{F}_q \to \mathbb{F}_q$, $a \mapsto a^p$ surjektiv ist.

(c) Zeigen Sie Grad $\varphi_p = p$, indem Sie das folgende Diagramm betrachten:

$$\begin{array}{ccc} \mathbb{F}_q(E) & \hookleftarrow & \mathbb{F}_q(x) \\ \uparrow & & \uparrow \\ \mathbb{F}_q(E^{(p)}) & \hookleftarrow & \mathbb{F}_q(x^p) \end{array}$$

Aufgabe 2 (2+2+2+3)

Sei p eine Primzahl mit $p \equiv 1 \pmod 4$, insbesondere gibt es also ein Element $i \in \mathbb{F}_p$ mit $\operatorname{ord}(i) = 4$. Ferner sei $E : y^2 = f(x)$, mit $f(x) = x^3 + x$.

(a) Zeigen Sie, dass f genau 3 Nullstellen in $\mathbb{F}_p$ besitzt. Folgern Sie $\#E(\mathbb{F}_p) \equiv 0 \pmod 4$.

Bemerkung: Vergessen Sie nicht den Punkt O im Unendlichen.

(b) In dieser Aufgabe dürfen Sie ohne Beweis benutzen, dass $\operatorname{End}(E) = \mathbb{Z}[i]$. Machen Sie sich klar, dass $E \cong E^{(p)}$ gilt. Sei $\varphi_p = A + Bi : E \to E$ der p-Frobeniusmorphismus. Zeigen Sie die Gleichung $A^2 + B^2 = p$.

Bemerkung: Es wirkt i auf Punkten von E durch $i \cdot (x, y) = (-x, iy)$.

(c) Wir betrachten die Menge

$$L = \{(A, B) \in \mathbb{Z} \; ; \; A^2 + B^2 = p\}.$$

Nach Aufgabenteil (b) ist diese Menge nicht leer. Zeigen Sie, dass es genau ein Paar $(a, b) \in L$ gibt, so dass a, b positiv sind und a ungerade ist. Schließen Sie, dass $N_p = p + 1 \pm 2a$ ist.

(d) Berechnen Sie N_p für $p \in \{5, 13, 17\}$ und überprüfen Sie, dass

$$N_p = \begin{cases} p + 1 + 2A & \text{falls } A \equiv 3 \pmod 4, \\ p + 1 - 2A & \text{falls } A \equiv 1 \pmod 4. \end{cases}$$