Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Dr. Peter Ullrich

WS 2004/05
Übungsblatt 13
3. Februar 2005

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 09.02.05

Aufgabe 1

Sei $p > 3$ eine Primzahl und C eine projektive, ebene Kurve gegeben durch $y^2 = x^3 + ax + b$ mit $a, b \in \mathbb{F}_p$. Zeigen Sie, dass C genau dann singulär ist, wenn $4a^3 + 27b^2 = 0$ gilt.

Aufgabe 2

Sei $O = (0 : 0 : 1) \in \mathbb{P}^2$, ein unendlich ferner Punkt und $P = (x_0, y_0) \in \mathbb{A}^2 (= U_0 \subset \mathbb{P}^2)$ ein Punkt im Affinen. Sei $L \subset \mathbb{P}^2$ die eindeutige Gerade durch P und O. Zeigen Sie, dass

$$L \cap \mathbb{A}^2 = \{(x, y) \in \mathbb{A}^2 \mid x - x_0 = 0\}$$

gilt.

Aufgabe 3

Sei $p > 3$ eine Primzahl und C eine projektive, eben, glatte Kurve gegeben durch $y^2 = x^3 + ax + b$ mit $a, b \in \mathbb{F}_p$. Implementieren Sie in LiDIA eine Funktion, die bei Eingabe von $k \geq 0$ und $P \in C[\mathbb{F}_p]$ den Punkt $[k]P$ mit Hilfe des iterierten Verdoppelns berechnet und ausgibt. Testen Sie Ihre Funktion an Hand des Beispiels aus Aufgabe 4, Blatt 12.

Aufgabe 4

Sei $C \subset \mathbb{P}^2$ eine ebene Kubik, gegeben in Weierstraßscher Normalform. Zeigen Sie, dass $O = (0 : 0 : 1)$ stets ein nicht-singulärer Punkt von C ist.