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

WS 2004/05
Übungsblatt 12
27. Januar 2005

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 02.02.05

Aufgabe 1

Sei C eine glatte, ebene Kubik. Das neutrale Element O der Gruppenstruktur auf C sei ein Wendepunkt von C, d.h. $\varphi(O, O) = O$. Zeigen Sie:

(a) $P \oplus \varphi(P, O) = O$,

(b) $P \oplus Q \oplus R = O \iff$ es gibt eine Gerade L mit $L \cdot C = P + Q + R$,

(c) P ist Wendepunkt von $C \iff P \oplus P \oplus P = O$.

Aufgabe 2

Sei C eine glatte, ebene Kubik, gegeben in Weierstraßscher Normlform. Zeigen Sie, dass C im Unendlichen genau einen Punkt P besitzt, d.h. $C \cap H_\infty = \{P\}$. Bestimmen Sie die homogenen Koordinaten von P. Desweiteren zeigen Sie, dass P ein Wendepunkt von C ist.

Aufgabe 3

Zeigen Sie: Ist C eine glatte, ebene Kubik definiert über K und sind P, Q K-rationale Punkte von C, so ist auch $\varphi(P, Q)$ ein K-rationaler Punkt.

Aufgabe 4

(a) Implementieren Sie die geometrische Addition auf glatten, ebenen Kubiken der Form $y^2 = x^3 + ax + b$ in LiDIA.

(b) Für die Kurve $y^2 = x^3 + x + 1$ über $\mathbb{F}_p$ mit $p = 10^{17} + 19$ und $P_0 = (0, 1)$ berechne man $[2346532]P_0$ (= das 2346532-fache von P_0).