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

WS 2004/05
Übungsblatt 11
20. Januar 2005

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 26.01.05

Aufgabe 1

Sei $V \subset \mathbb{A}^n (= U_0 \subset \mathbb{P}^n)$ eine affine Varietät, $P \in V$ und $W = \overline{V}$ der projektive Abschluß von V. Zeigen Sie, dass

$$\overline{K}[W] \to \overline{K}[V],\ F \mapsto F^a$$

ein wohldefinierter Ringhomomorphismus ist, der einen Isomorphismus

$$\phi : \overline{K}(W) \to \overline{K}(V),\ F/G \mapsto F^a/G^a$$

induziert. Desweiteren gilt für die lokalen Ringe $\phi(O_p(W)) = O_p(V)$. Geben Sie explizit die Umkehrabbildung von ϕ an.

Aufgabe 2

Sei $C = \{(x, y) \mid y^2 = x^3 - x\} \subset \mathbb{A}^2 (= U_0 \subset \mathbb{P}^2)$ und $\overline{C}$ der projektive Abschluß von C. Zeigen Sie, dass $\overline{C} = C \cup \{P\}$ gilt mit einem $P \in \mathbb{P}^2$; bestimmen Sie homogene Koordinaten für P. Weiterhin sei die rationale Funktion $\varphi = x/y \in \overline{K}(C) = \overline{K}(\overline{C})$ gegeben. Ist φ im unendlich fernen Punkt P definiert? Wenn ja, so bestimmen Sie $\varphi(P)$.

Aufgabe 3

Sei $f \in \overline{K}[X_0, X_1, X_2]$ ein nicht-konstantes, irreduzibles, homogenes Polynom und $C = \{P \in \mathbb{P}^2 : f(P) = 0\}$. Zeigen Sie:

(a) Ein Punkt $P \in C$ ist genau dann singulär, wenn

$$\frac{\partial f}{\partial X_0}(P) = \frac{\partial f}{\partial X_1}(P) = \frac{\partial f}{\partial X_2}(P) = 0$$

gilt.

(b) Ist $P \in C$ ein nicht-singulärer Punkt, so ist

$$\{(x_0 : x_1 : x_2) \in \mathbb{P}^2 \mid \frac{\partial f}{\partial X_0}(P)x_0 + \frac{\partial f}{\partial X_1}(P)x_1 + \frac{\partial f}{\partial X_2}(P)x_2 = 0\}$$

der projektive Abschluß der Tangente an C durch P.

Aufgabe 4

Sei $C = \{(x, y) \mid y^2 - f(x) = 0\} \subset \mathbb{A}^2$, wobei $f \in \overline{K}[X]$ ein nicht-konstantes Polynom ist, $\mathrm{char}(K) \neq 2$. Zeigen Sie, dass C genau dann glatt ist, wenn f keine mehrfachen Nullstellen hat.