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

WS 2004/05
Übungsblatt 9
23. Dezember 2004

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 12.01.05

Aufgabe 1

Sei $V \subset \mathbb{A}^n$ eine algebraische Menge. Zeigen Sie, dass V genau dann irreduzibel ist, wenn $I(V)$ ein Primideal ist.

Aufgabe 2

Sei $F \in \overline{K}[X_1, \ldots, X_n]$ ein nicht-konstantes Polynom und $V = V(F) \subset \mathbb{A}^n$. Sei F_{red} die Reduktion von F (siehe Vorlesung). Zeigen Sie:

(a) Das Verschwindungsideal $I(V)$ ist ein Hauptideal und wird von F_{red} erzeugt.

(b) V ist irreduzibel $\iff$ F_{red} ist irreduzibel.

(c) Sei nun speziell F von der Form $F(x, y) = y^2 - f(x) \in \overline{K}[x, y]$, wobei $f(x) \in \overline{K}[x]$ ein (nicht-konstantes) Polynom von ungeradem Grad ist. Dann ist $V(F) \subset \mathbb{A}^2$ irreduzibel.

Aufgabe 3

Sei $V = V(f) \subset \mathbb{A}^2$ mit $f(x, y) = y^2 - x^3 \in \overline{K}[x, y]$. Weiterhin seien die rationalen Funktionen $\varphi = \frac{y}{x} \in \overline{K}(V)$ und $\psi = \frac{y^2}{x^2} \in \overline{K}(V)$ gegeben. Zeigen Sie, dass ψ im Punkt $P = (0, 0) \in V$ definiert ist, φ hingegen nicht.

Aufgabe 4

Sei $f(x_0, x_1) \in \overline{K}[x_0, x_1]$ ein homogenes Polynom vom Grad $d \geq 1$. Zeigen Sie, dass es dann $a_0, \ldots, a_d, b_0, \ldots, b_d \in \overline{K}$ gibt, so dass

$$f(x_0, x_1) = \prod_{i=1}^{d} (a_i x_0 + b_i x_1)$$

gilt. (Hinweis: Dehomogenisiere zunächst f).