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

WS 2004/05
Übungsblatt 10
13. Januar 2005

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 19.01.05

Aufgabe 1

Seien $f, g \in \overline{K}[X_1, \ldots, X_n] \setminus 0$ und $F, G \in \overline{K}[X_0, \ldots, X_n] \setminus 0$; F, G seien homogen. Zeigen Sie:

(a) $(fg)^h = f^h g^h$ und $(FG)^a = F^a G^a$.

(b) $(f^h)^a = f$; und ist e maximal mit $x_0^e | F$, so ist $x_0^e (F^a)^h = F$.

(c) $(F+G)^a = F^a + G^a$; und ist $r = \deg(g)$, $s = \deg(f)$, $t = r + s - \deg(f+g)$, so gilt $x_0^t (f+g)^h = x_0^r f^h + x_0^s g^h$.

Aufgabe 2

Sei $f \in \overline{K}[X_1, \ldots, X_n] \setminus 0$ und $f = \sum_j f_j$ die Zerlegung von f in homogene Komponenten. Sei $P \in \mathbb{P}^n$ und $a = (a_0, \ldots, a_n) \in \overline{K}^{n+1}$ mit $P = (a_0 : \cdots : a_n)$. Dann gilt

$$f(P) = 0 \qquad \Longleftrightarrow \qquad f_j(a) = 0 \quad \text{für alle } j.$$

Aufgabe 3

Sei $V \subset \mathbb{A}^n$ eine affine algebraische Menge, $\overline{V}$ der projektive Abschluß von V und $H_\infty = \mathbb{P}^n \setminus \mathbb{A}^n$ die Hyperebene im Unendlichen. Zeigen Sie:

(a) $\overline{V} \cap \mathbb{A}^n = V$.

(b) V ist irreduzibel $\Longleftrightarrow$ $\overline{V}$ ist irreduzibel.

(c) Ist $V = V_1 \cup \cdots \cup V_r$ die Zerlegung von V in irreduzible Komponenten, so ist $\overline{V} = \overline{V_1} \cup \cdots \cup \overline{V_r}$ die Zerlegung von $\overline{V}$ in irreduzible Komponenten.

(d) Keine irreduzible Komponente von $\overline{V}$ liegt ganz in H_∞.

(e) Die Abbildung $V \mapsto W := \overline{V}$ vermittelt eine Bijektion von der Menge aller affinen algebraischen Mengen $V \subset \mathbb{A}^n$ auf die Menge aller projektiven algebraischen Mengen $W \subset \mathbb{P}^n$, für die keine irreduzible Komponente ganz in H_∞ liegt.

Aufgabe 4

Bestimmen Sie $V_\infty = \overline{V} \cap H_\infty$, sowie $\overline{V} \cap U_i$ $(i = 1, 2)$ für $V = \{y - x^2 = 0\}$ und $V = \{y^2 - x^3 + 1 = 0\}$ (H_∞ Hyperebene im Unendlichen, $U_i = \{(x_0 : x_1 : x_2) | x_i \neq 0\}$, $\overline{V}$ proj. Abschluß von V).