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

WS 2004/05
Übungsblatt 8
16. Dezember 2004

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 22.12.04

Aufgabe 1

Programmieren Sie eine LiDIA-Prozedur zur Berechnung des Jacobi-Symbols.

Aufgabe 2

Sei $N = p_1 \cdots p_r$ mit paarweise verschiedenen Primzahlen p_i und sei φ die Eulersche φ-Funktion (siehe Blatt 7). Zeigen Sie:

(a) Für $x, y \in \mathbb{Z}$ gilt $x \equiv y \mod N$ genau dann, wenn $x \equiv y \mod p_i$ für jedes $i = 1, \ldots, r$ gilt.

(b) Für alle $x, k \in \mathbb{Z}$, $k \geq 0$, gilt

$$x^{1+k\varphi(N)} \equiv x \mod N.$$

(c) Für jedes $x \in \mathbb{Z}$ mit $\mathrm{ggT}(x, N) = 1$ ist

$$x^{\varphi(N)} \equiv 1 \mod N.$$

Aufgabe 3

Zeigen Sie: Ist K ein endlicher Körper, so ist jede Teilmenge M von $\mathbb{A}^n(K)$ von der Form $M = V \cap \mathbb{A}^n(K)$ mit einer algebraischen Menge $V \subset \mathbb{A}^n$.

Aufgabe 4

(a) Sei $X \subset \mathbb{A}^2$ gegeben durch $X = V(f, g)$ mit $f(x, y) = x^2 + y^2 - 1$ und $g(x, y) = x - 1$. Bestimme das Verschwindungsideal $I(X)$. Gilt $I(X) = (f, g)$?

(b) Für jede Teilmenge $M \subset \mathbb{A}^n$ ist das Verschwindungsideal $I(M)$ ein Radikalideal, d.h. $I(M) = \sqrt{I(M)}$.