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

WS 2004/05
Übungsblatt 7
9. Dezember 2004

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 15.12.04

Aufgabe 1

Sei $q = p^d$ eine Primzahlpotenz und $f = X^q - X \in \mathbb{F}_p[X]$. Es sei E ein algebraischer Abschluß von $\mathbb{F}_p$ und $K = \{a \in E : f(a) = 0\}$. Zeigen Sie, dass K ein Körper mit q Elementen ist.

Aufgabe 2

Entscheide, ob 7411 ein quadratischer Rest modulo der Primzahl 9283 ist.

Aufgabe 3

Für $n \in \mathbb{N}$ bezeichne $(\mathbb{Z}/n\mathbb{Z})^*$ die Gruppe der Einheiten von $\mathbb{Z}/n\mathbb{Z}$. Die Eulersche φ-Funktion ist definiert durch $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$. Zeigen Sie:

(a) $m \in \mathbb{N}$ ist genau dann eine Einheit in $\mathbb{Z}/n\mathbb{Z}$, wenn m und n teilerfremd sind.

(b) Sind $n, m \in \mathbb{N}$ teilerfremd, so gilt $\varphi(nm) = \varphi(n)\varphi(m)$.

(c) Ist p eine Primzahl und $e \in \mathbb{N}$, so ist $\varphi(p^e) = (p-1)p^{e-1}$.

(d) Ist $n = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung von $n > 1$, so gilt

$$\varphi(n) = \prod_{k=1}^{r} (p_k - 1) p_k^{e_k - 1}.$$

Aufgabe 4

Sei p eine ungerade Primzahl. Zeigen Sie:

(a) Es gilt $p^2 \equiv 1 \mod 8$.

(b) $(-1)^{(p^2-1)/8} = 1$, falls $p \equiv \pm 1 \mod 8$ und $(-1)^{(p^2-1)/8} = -1$, falls $p \equiv \pm 3 \mod 8$.