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

WS 2004/05
Übungsblatt 4
11. November 2004

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 17.11.04

Aufgabe 1
Zeigen Sie, dass jeder Körper nullteilerfrei ist.

Aufgabe 2
Sei $i = \sqrt{-1} \in \mathbb{C}$. Zeigen Sie:

$$\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\}.$$

Aufgabe 3
Sei K ein Körper. Zeigen Sie:

1. Ist I ein Ideal von K, so gilt $I = (0)$ oder $I = (1)$.
2. Ist $\varphi : K \to R$ ein Ringhomomorphismus in einen Ring $R \neq \{0\}$ (Beachte: Wg. $\varphi(1) = 1 \neq 0$ ist dann φ nicht konstant), so ist φ injektiv.
3. Ist $\varphi : K \to E$ ein Ringhomomorphismus, E ein Körper, so ist $\mathrm{im}(\varphi)$ ein Teilkörper von E.

Aufgabe 4
Sei K ein Körper der Charakteristik $p < \infty$. Zeigen Sie, dass der Frobenius-Endomorphismus

$$\Phi_p : K \to K,\ a \mapsto a^p$$

ein Ringhomomorphismus ist.