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

WS 2004/05
Übungsblatt 3
4. November 2004

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 10.11.04

Aufgabe 1

Sei R ein Ring (stets kommutativ mit 1) und sei I ein Ideal von R. Weiterhin sei $\varphi : R \to R/I$, $a \mapsto \bar{a}$ $(= a + I)$ der kanonische Homomorphimsus.

(a) Für jedes Ideal $\mathfrak{J}$ von R/I ist $\varphi^{-1}(\mathfrak{J}) = \{a \in R : \varphi(a) \in \mathfrak{J}\}$ ein Ideal von R.

(b) Die Abbildung $\mathfrak{J} \mapsto \varphi^{-1}(\mathfrak{J})$ (aus (a)) ist eine Bijektion von der Menge aller Ideale $\mathfrak{J}$ von R/I auf die Menge aller Ideale J von R mit $J \supseteq I$.

(c) Ist $\mathfrak{P}$ ein Primideal von R/I, so ist $\varphi^{-1}(\mathfrak{P})$ ein Primideal von R.

(d) Wie viele Ideale besitzt der Ring $\mathbb{Z}/(n)$?

Aufgabe 2

Sei R ein Ring.

(a) Ist I ein Ideal von R, so ist auch $\mathrm{Rad}(I) = \sqrt{I} = \{a \in R : a^n \in I \text{ für ein } n \in \mathbb{N}\}$ ein Ideal von R – es heißt das *Radikal* von I.

(b) Für welche Ideale I von $\mathbb{Z}$ gilt $I = \mathrm{Rad}(I)$?

Aufgabe 3

Sei R ein Integritätsring. Für ein Polynom $0 \neq f = \sum_{i=0}^{n} a_i X^i \in R[X]$ mit $a_n \neq 0$ bezeichnet man (wie üblich) mit $\deg(f) = n$ den *Grad* des Polynoms ($\deg(0) = -\infty$).

(a) Für $f, g \in R[X]$ gilt $\deg(fg) = \deg(f) + \deg(g)$ und $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.

(b) Gilt (a) i.a. auch dann noch, wenn R nicht integer ist?

Aufgabe 4

Im Polynomring $\mathbb{Q}[X, Y]$ ist das von X und Y erzeugte Ideal $I = (X, Y)$ kein Hauptideal; insbesondere ist $\mathbb{Q}[X, Y]$ kein Hauptidealring. (Hinweis: Benutze Aufgabe 3).