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

WS 2004/05
Übungsblatt 2
28. Oktober 2004

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 03.11.04

Aufgabe 1

Sei R ein Ring. Bezeichne mit $\widetilde{R}$ die Menge aller Folgen $(a_i)_{i\in\mathbb{N}_0}$, so dass nur endlich viele Folgenglieder von 0 verschieden sind, d.h. es existiere eine endliche Menge $I \subset \mathbb{N}_0$ mit $a_i = 0$ für alle $i \in \mathbb{N}_0 \setminus I$. Auf $\widetilde{R}$ seien wie folgt Verknüpfungen gegeben:

$$(a_i)_{i\in\mathbb{N}_0} + (b_i)_{i\in\mathbb{N}_0} = (a_i + b_i)_{i\in\mathbb{N}_0}$$

$$(a_i)_{i\in\mathbb{N}_0} \cdot (b_i)_{i\in\mathbb{N}_0} = (c_i)_{i\in\mathbb{N}_0}, \text{ wobei } c_i = \sum_{k=0}^{i} a_k b_{i-k}$$

Zeigen Sie:

1. $(\widetilde{R}, +, \cdot)$ is ein kommutativer Ring mit 1.
2. Sei $X = (x_i)$, wobei $x_1 = 1$ und $x_i = 0$ für alle $i \neq 1$. Dann hat jedes $f \in \widetilde{R}$ eine eindeutige Darstellung der Form $f = \sum_i a_i X^i$ mit $a_i \in R$, wobei $a(b_i) := (ab_i)$ für $a \in R$ und $(b_i) \in \widetilde{R}$ definiert ist. (Beachte: Die Summe ist hier nicht formal, sondern die Addition in $\widetilde{R}$).
3. Der Ring $(\widetilde{R}, +, \cdot)$ mit $X \in \widetilde{R}$ aus 2. besitzt die universelle Eigenschaft des Polynomrings (siehe Lemma 1.2.1 der Vorlesung).

Aufgabe 2

Zeigen Sie:

1. Seien $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$. Dann gilt: $d = \mathrm{ggT}(a_1, \ldots, a_n) \iff (d) = (a_1, \ldots, a_n)$.
2. Für ein $a \in \mathbb{Z} \setminus 0$ gilt: (a) ist ein Primideal genau dann, wenn a eine Primzahl ist. Ist das Nullideal $(0) = \{0\}$ auch ein Primideal?