Mathematisches Institut 07.05.2002
Prof. Dr. R. Wallisser

Übungen zur Vorlesung

Elementare Zahlentheorie — SS 2002

Blatt 4

Abgabe: Dienstag, 14.05.02, 9.00 Uhr, vor der Vorlesung

Aufgabe 1.
Es sei $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\} c \mathbb{C}$. Man zeige:

a) $\mathbb{Z}[\sqrt{-2}]$ ist ein euklidischer Ring bzgl. der „Größe“ $s, s(a + b\sqrt{-2}) := a^2 + 2b^2$.

b) $a + \sqrt{-2}$ und $a - \sqrt{-2},\ a \in \mathbb{Z}$, sind in $\mathbb{Z}[\sqrt{-2}]$ teilerfremd.

c) Man gebe alle Punkte $(a, b) \in \mathbb{Z}^2$ an, die auf der elliptischen Kurve $y^2 = x^3 - 2$ liegen.

Aufgabe 2.
Es sei K ein Körper und $K[x]$ die Menge der Polynome mit Koeffizienten aus K. Für $f \in K[x]$,

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,\ a_n \neq 0.$$

sei grad $f := n$.

a) Man zeige, daß $(K[x], \text{grad } f)$ ein Euklidischer Ring ist.

b) Bestimme die Einheiten von $K[x]$.

c) Zeige ferner, daß $p(x), q(x) \in K[x]$ genau dann „teilerfremd“ sind, wenn es $s(x)$ und $t(x) \in K[x]$ gibt, so daß

$$s(x)p(x) + t(x)q(x) = 1$$

gilt.

Aufgabe 3.

a) Mit Hilfe der „Division mit Rest“ in $\big(\mathbb{Q}[x], \text{grad } f\big)$ bestimme man

$$d(x) := \text{ggT}(x^3 + 2x^2 + 2x + 4,\ x^2 + x - 2).$$

b) Man schreibe das Polynom $d(x) = \text{ggT}\big(p(x), q(x)\big)$ aus Teil a) mit Polynomen $s(x), t(x)$ aus $\mathbb{Q}[x]$ in der Form

$$s(x)\, p(x) + t(x)\, q(x).$$

(Bitte wenden)

Aufgabe 4.

a) Es sei $\mathbb{F}_2$ der Körper mit den zwei Elementen 0 und 1. Man zerlege die folgenden Polynome aus $\mathbb{F}_2[x]$ in irreduzible Faktoren:

i) $x^2 + 1$

ii) $x^3 + x + 1$

iii) $x^4 + x^2 + x + 1$

b) Es sei $r(x) = \dfrac{p(x)}{q(x)}$, $p, q \in \mathbb{C}[x]$ eine rationale Funktion in $\mathbb{C}(x)$. Man benutze die „Primfaktorzerlegung" von $q(x)$ zur Herleitung der „Partialbruchzerlegung" von $r(x)$ d.h. $r(x)$ läßt sich als Linearkombination von einem Polynom und rationalen Funktionen der Form $(x - a)^{-i}, a \in \mathbb{C}, i \in \mathbb{N}$, schreiben.