RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

**Hausübungen zur Vorlesung**

# Zahlentheorie

**SS 2013**

Blatt 2 / 12. April 2013 / Abgabe bis spätestens 22. April 2013, 12:00 Uhr in dem Kasten auf NA 02 oder am Anfang der Vorlesung

Geben Sie bitte die Aufgaben zur Vereinfachung der Korrektur folgendermassen nach Aufgaben getrennt ab:

- Aufgaben 1 und 3 in Kasten A
- Aufgabe 2 in Kasten B
- Aufgabe 4 in Kasten C

Die Kästen auf NA 02 sind entsprechend beschriftet. Wenn Sie in der Vorlesung abgeben, machen sie einfach 3 getrennte Stapel. Schreiben Sie auf alle 3 Abgaben jeweils Ihre(n) Namen und/oder Matrikelnummer(n).

**AUFGABE 1** (2 Punkte)**:**
Zeigen Sie, dass der Polynomring $\mathbb{Q}[X]$ ein euklidischer Ring ist.
Bemerkung: Verwenden sie den Grad eines Polynoms als Bewertungsfunktion. Sie dürfen voraussetzen, dass $\mathbb{Q}[X]$ ein Integritätsbereich ist.

**AUFGABE 2** (6 Punkte)**:**
Sei $K = \mathbb{Q}[\sqrt{-3}] = \{a+b\sqrt{-3} \mid a,b \in \mathbb{Q}\} \subset \mathbb{C}$ und $N : K \to \mathbb{Q}$ mit $N(a+b\sqrt{-3}) = a^2+3b^2$ die Normfunktion.
Wir betrachten $R \subset K$, gegeben durch $R = \{a + b\sqrt{-3} \mid a,b \in \mathbb{Z} \text{ oder } a-\frac{1}{2}, b-\frac{1}{2} \in \mathbb{Z}\}$. (d.h. $a,b$ sind entweder beide ganzzahlig oder beide halbzahlig, d.h. $a,b$ sind von der Form $a = \frac{a'}{2}, b = \frac{b'}{2}$, mit entweder $a', b'$ beide gerade oder beide ungerade)
Zeigen Sie:

(a) $R$ ist ein Integritätsbereich. (2 Punkte)

(b) Für $x \in R$ ist $N(x) \in \mathbb{Z}$ (1 Punkt)

(c) $R$ ist euklidisch mit $N$ als Bewertungsfunktion (3 Punkte)

Bemerkung zu (a): Da $R \subset \mathbb{C}$ ist, übertragen sich die entsprechenden Eigenschaften der komplexen Zahlen auf $R$. $0, 1 \in R$ ist ebenfalls klar. Zu zeigen ist hier nur, dass für $a,b \in R$ auch $a+b, a \cdot b \in R$ liegen.

— bitte wenden —

**AUFGABE 3** (6 Punkte)**:**
Sei $R$ ein Integritätsring.

(a) Zeigen Sie, dass folgende Aussagen äquivalent sind (4 Punkte):

(i) Jedes Ideal $J$ von $R$ ist endlich erzeugt, d.h. von der Gestalt $J = (b_1, \ldots, b_n) = \{\sum_i a_i b_i \mid a_i \in R\}$

(ii) Jede aufsteigende Kette von Idealen $I_1 \subset I_2 \subset I_3 \subset \cdots$ wird stationär, d.h. es gibt ein $m > 0$ mit $I_m = I_n$ für alle $n \geq m$.

(b) Zeigen Sie, dass in jedem Integritätsbereich $R$, in dem die Eigenschaft aus (a) gilt (solche Ringe heißen Noethersch), jedes $0 \neq x \in R \setminus R^*$ eine Zerlegung in irreduzible Elemente besitzt. (2 Punkte)

Hinweis zu (a): Für (i) $\Longrightarrow$ (ii) sollten sie Aufgabe 4 von Präsenzblatt 2 nutzen: $\bigcup I_i$ ist ebenfalls ein Ideal.

**AUFGABE 4** (6 Punkte)**:**
Wir nennen eine Primzahl $p \in \mathbb{Z}$ vom Typ A, wenn es $x, y \in \mathbb{Z}$ gibt mit $x^2 + y^2 = p$, ansonsten nennen wir $p$ vom Typ B. Zeigen Sie:

(a) Jedes $0 \neq x \in \mathbb{Z}[i]$ besitzt eine (bis auf Reihenfolge) eindeutige Zerlegung der Form $x = u \cdot \pi_1 \cdot \pi_2 \cdots \pi_n$, wobei $u \in \{\pm 1, \pm i\}$ und die $\pi_i$ Primelemente in $\mathbb{Z}[i]$ mit $\mathrm{Re}(\pi_i) > 0$ und $\mathrm{Im}(\pi_i) \geq 0$ sind. (2 Punkte)

(b) Eine natürliche Zahl $n > 0$ lässt sich genau dann als Summe von 2 Quadraten $n = x^2 + y^2, x, y \in \mathbb{Z}$ schreiben, wenn in der Primfaktorzerlegung (über $\mathbb{Z}$, nicht über $\mathbb{Z}[i]$) von $n$ jede Primzahl vom Typ B geradzahlig oft vorkommt. (4 Punkte)

Hinweis: Beachten Sie für (b), dass $x^2 + y^2 = (x + iy)(x - iy)$ gilt. Vergleichen Sie die Primelementzerlegung von $n$ über $\mathbb{Z}$ mit der Zerlegung von $n$ über $\mathbb{Z}[i]$. Benutzen Sie, dass wenn $z = u \cdot \pi_1 \cdot \pi_2 \cdots \pi_n$ eindeutige Primfaktorzerlegung ist, dass dann auch $\overline{z} = \overline{u} \cdot \overline{\pi}_1 \cdot \overline{\pi}_2 \cdots \overline{\pi}_n$ die Primfaktorzerlegung der komplex konjugierten ist.
Bemerkung: Wir werden später sehen, dass Primzahlen vom Typ B genau die Primzahlen der Form $p = 4k + 3$ mit $k \in \mathbb{Z}$ sind.