Übungen zur Algebra I

Prof. Dr. S. Bosch/C. Löh — Blatt 5 vom 15. November 2007

Aufgabe 1 (Gaußsche Primzahlen**).** Sei $\mathbb{Z}[i]$ der Ring der ganzen Gaußschen Zahlen; zur Erinnerung: $\mathbb{Z}[i] = \{x + i \cdot y \mid x,\ y \in \mathbb{Z}\} \subset \mathbb{C}$.

1. Sei $N\colon \mathbb{Z}[i] \longrightarrow \mathbb{N}, z \longmapsto |z|^2$ die *Normabbildung.* Zeigen Sie für alle Gaußschen Zahlen $z \in \mathbb{Z}[i]$: Ist $N(z)$ prim in $\mathbb{Z}$, so ist z prim in $\mathbb{Z}[i]$.
2. Geben Sie sowohl ein Beispiel für eine Primzahl in $\mathbb{Z}$, die prim in $\mathbb{Z}[i]$ ist als auch ein Beispiel für eine Primzahl in $\mathbb{Z}$, die nicht prim in $\mathbb{Z}[i]$ ist.

Aufgabe 2 (Bosch „Algebra“ 2.4.8**).** Bestimmen Sie alle irreduziblen Polynome vom Grad höchstens 3 im Polynomring $\mathbb{F}_2[X]$.

Aufgabe 3 (Bosch „Algebra“ 2.4.9**).** Sei $p \in \mathbb{N}$ prim. Die Menge

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \;\middle|\; a,\, b \in \mathbb{Z} \text{ und } p \text{ teilt nicht } b \right\}$$

bildet einen Unterring von $\mathbb{Q}$.

1. Bestimmen Sie alle Ideale von $\mathbb{Z}_{(p)}$ und zeigen Sie, dass $\mathbb{Z}_{(p)}$ ein Hauptidealring ist.
2. Bestimmen Sie (bis auf Assoziiertheit) alle Primelemente von $\mathbb{Z}_{(p)}$.

Aufgabe 4 (RSA-Verschlüsselung**).** Seien p und $q \in \mathbb{N}$ zwei (große) verschiedene Primzahlen und $n := p \cdot q$. Seien d, $e \in \mathbb{N}$ (große, verschiedene) Zahlen mit

$$\operatorname{ggT}\big(d, (p-1)(q-1)\big) = 1 \quad \text{und} \quad d \cdot e \ \equiv 1 \ \big(\mathrm{mod}\ (p-1)(q-1)\big).$$

Das Paar (e, n) ist der sogenannte *öffentliche Schlüssel,* das Paar (d, n) der *private Schlüssel.* Wir betrachten nun die Abbildungen (Ver- und Entschlüsselung)

$$\begin{aligned} \mathrm{encrypt}\colon \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ \overline{m} &\longmapsto \overline{m^e} \end{aligned} \qquad \text{und} \qquad \begin{aligned} \mathrm{decrypt}\colon \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ \overline{m} &\longmapsto \overline{m^d}. \end{aligned}$$

Zeigen Sie, dass der private Schlüssel Nachrichten (aus $\mathbb{Z}/n\mathbb{Z}$), die mit dem öffentlichen Schlüssel verschlüsselt wurden, entschlüsseln kann:

1. Beweisen Sie zunächst Folgendes: Sei $p \in \mathbb{N}$ eine Primzahl. Zeigen Sie, dass $m^{p-1} \equiv 1 \pmod{p}$ für alle $m \in \mathbb{Z} - p\mathbb{Z}$ gilt.
2. Folgern Sie nun, dass $\mathrm{decrypt} \circ \mathrm{encrypt} = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$.

Bemerkung. Dieses Verfahren ist *asymmetrisch,* d.h. Nachrichten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, können nicht mit dem öffentlichen Schlüssel entschlüsselt werden, sondern nur mit dem privaten.

Die Sicherheit des obigen Verfahrens beruht darauf, dass bislang keine effiziente Methode bekannt ist, die es erlaubt, das Paar (d, n) aus (e, n) zu rekonstruieren.

Aufgabe 5*. Zeigen Sie, dass es zu jedem $n \in \mathbb{N}$ einen Ring gibt, der (modulo Assoziiertheit) genau n Primelemente enthält.
Hinweis. Betrachten Sie eine Variation der Konstruktion aus Aufgabe 3.

Abgabe bis zum 22. November 2007, 8:00 Uhr