Übungen zur Vorlesung Elementare Zahlentheorie (SS 18)

PD Dr. Jürgen Müller, Dr. Martin Bender

(7.1) Aufgabe: Isomorphiesätze. Sei R ein kommutativer Ring und $I \trianglelefteq R$.

a) Sei $J \trianglelefteq R$ wobei $J \subseteq I$. Dann ist $(R/J)/(I/J) \cong R/I$.

b) Sei $S \subseteq R$ ein Unterring. Dann ist $S/(S \cap I) \cong (S+I)/I$.

Hinweis: Wenden Sie den Homomorphiesatz auf geeignete natürliche Abbildungen an.

(7.2) Aufgabe: Arithmetik in $\mathbb{Z}[\sqrt{-5}]$. Wir betrachten die Ideale

$$I_1 = \langle 2, 1+\sqrt{-5}\rangle, I_2 = \langle 3, 1+\sqrt{-5}\rangle, I_3 = \langle 3, 1-\sqrt{-5}\rangle \trianglelefteq \mathbb{Z}[\sqrt{-5}].$$

a) Zeigen Sie, daß $I_1 \cdot I_2 = (1+\sqrt{-5})$ und $I_1 \cdot I_3 = (1-\sqrt{-5})$, sowie $I_1^2 = \langle 2\rangle$ und $I_2 \cdot I_3 = \langle 3\rangle$. Folgern Sie, daß $I_1^2 \cdot I_2 \cdot I_3 = \langle 6\rangle$.

b) Zeigen Sie, daß die Ideale I_i keine Hauptideale sind, und bestimmen Sie jeweils die Anzahl der Restklassen modulo I_i.

c) Zeigen Sie, daß die Erzeugerpaare der Ideale I_i jeweils einen größten gemeinsamen Teiler d_i besitzen. Wie verhalten sich $\langle d_i\rangle$ und I_i zueinander?

(7.3) Aufgabe: Primzahlen mit vorgegebener Restklasse. Zeigen Sie, daß es unendlich viele Primzahlen gibt, die kongruent -1 modulo 3 sind.

(7.4) Aufgabe: Polynomkongruenzen.
Für einen kommutativen Ring R bezeichne $R[X]$ den **Polynomring** über R in der Unbestimmten X.

a) Es sei $n \in \mathbb{N}$. Zeigen Sie: Die natürliche Abbildung $\nu_n\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\colon a \mapsto \overline{a}$ kann eindeutig zu einem Ringhomomorphismus $\nu_n\colon \mathbb{Z}[X] \to (\mathbb{Z}/n\mathbb{Z})[X]$ mit $\nu_n(X) = X$ fortgesetzt werden. Dieser induziert dann einen Isomorphismus $\mathbb{Z}[X]/\langle n\rangle \cong (\mathbb{Z}/n\mathbb{Z})[X]$. Wie sehen die Elemente des Ideals $\langle n\rangle \trianglelefteq \mathbb{Z}[X]$ aus?

Für $f, g \in \mathbb{Z}[X]$ schreiben wir $\overline{f} := \nu_n(f)$; und $f \equiv g \pmod{n}$, falls $\overline{f} = \overline{g}$.

b) Eine Zahl $a \in \mathbb{Z}$ heißt eine **Nullstelle** von f **modulo** n, falls $\overline{f(a)} = \overline{0}$ ist. Zeigen Sie: Dies ist genau dann der Fall, wenn $\overline{a}$ eine Nullstelle von $\overline{f}$ ist. Weiter zeige man: Dies ist genau dann der Fall, wenn es $g \in \mathbb{Z}[X]$ gibt mit $f \equiv g \cdot (X-a) \pmod{n}$.

c) Bekanntlich hat ein Polynom $0 \neq f \in \mathbb{Z}[X]$ vom Grad d höchstens d paarweise verschiedene Nullstellen in $\mathbb{Z}$. Gilt eine analoge Aussage auch für Polynome in $(\mathbb{Z}/n\mathbb{Z})[X]$ und ihre Nullstellen in $\mathbb{Z}/n\mathbb{Z}$?

Abgabe: 07.06.2018 (Donnerstag), bis 10:00 Uhr.