Universität Mannheim, Lehrstuhl für Mathematik VI
Christian Sevenheck

Übungsaufgaben zur Algebra

1. *(2 Punkte)* Führen Sie den erweiterten Euklidischen Algorithmus für die Zahlen $r_0 = 14372$ und $r_1 = 1236$ durch, mit den gleichen Notationen und analogen Ergebnissen wie im Beispiel 7.6 der Vorlesung.

   Geben Sie die Ergebnisse (die Anzahl n der Schritte und alle r_i, q_i, x_i, y_i für $i = 0, ..., n+1$, außer q_0 und q_{n+1} (die existieren nicht)) in einer Tabelle wie im Beispiel 7.6 an.

2. *(2 Punkte)* Führen Sie den erweiterten Euklidischen Algorithmus mit den Polynomen $r_0 = x^4 + x^3 + x + 1$ und $r_1 = x^3 + x^2 - x \in \mathbb{Q}[x]$ durch. Geben Sie die Ergebnisse (die Anzahl n der Schritte und alle r_i, q_i, x_i, y_i) in einer Tabelle wie in den Beispielen 7.6 und 7.7 der Vorlesung an.

3. *(2+1+1 Punkte)*

   (a) Aus dem erweiterten Euklidischen Algorithmus folgt, daß für zwei Zahlen $a, b \in \mathbb{Z}$ gilt:

   $$\exists\, c, d \in \mathbb{Z} \quad \text{mit} \quad \mathrm{ggT}(a, b) = ca + db.$$

   Folgern Sie daraus

   $$(\mathbb{Z}/m\mathbb{Z})^* = \{[a] \mid 0 < a < m, \mathrm{ggT}(a, m) = 1\}.$$

   (b) Listen Sie in den beiden Fällen $m = 15$ und $m = 28$ jeweils die Elemente von $(\mathbb{Z}/m\mathbb{Z})^*$ und ihre Inversen auf (am besten in Tabellen mit den Inversen der Elemente unter den Elementen).

4. *(2 Punkte)* Zeigen Sie, daß der Ring $\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ mit der Gradfunktion

   $$w : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}, \quad a + ib \mapsto |a + ib|^2 = a^2 + b^2,$$

   ein Euklidischer Ring ist.

5. *(4 Punkte)* Nach Aufgabe 4 ist der Ring $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z} \cdot i \subset \mathbb{C}$ ein Euklidischer Ring, also (Satz 7.14 der Vorlesung) auch ein Hauptidealring. Daher sind die folgenden 6 Ideale Hauptideale. Finden Sie je ein Erzeugendes (mit Beweis).

   $$(3, i), \quad (4 + 4i, 8i), \quad (2 - i, 2 + i), \quad (1 + i, 1 - i), \quad (5, 3 + 4i), \quad (10, 7 + i).$$

6. *(2 Punkte)* Die Eulersche phi-Funktion $\varphi : \mathbb{N} - \{1\} \to \mathbb{N}$ ist definiert durch

   $$\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|.$$

   (a) Zeigen Sie folgende Verallgemeinerung des kleinen Satzes von Fermat:

   Seien $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann ist

   $$a^{\varphi(m)} \equiv 1 \mod m.$$

   Hinweise: Benutzen Sie Aufgabe 3 (a) und den Satz von Lagrange oder eine Folgerung davon.

   (b) Folgern Sie: *Es seien p und q zwei verschiedene Primzahlen, $a \in \mathbb{Z}$ und $r \in \mathbb{N} \cup \{0\}$. Dann gilt*

   $$a^{1+r(p-1)(q-1)} \equiv a \mod pq.$$

Alle Informationen zur Vorlesung (Termine, Übungsblätter etc.) sind unter

`http://hilbert.math.uni-mannheim.de/~sevenhec/Algebra13.html`

zu finden.

Abgabe bis Montag, den 21. Oktober, in der Vorlesung.