**Zahlentheorie (Osnabrück SS 2008)**

**Arbeitsblatt 7**

**Aufgabe 1.** (2 Punkte)

Zu $p = 13$ und $k = 3$ berechne die Vielfachen $ik \mod 13$ für $i = 1, \ldots, 6$ und repräsentiere sie durch Zahlen zwischen $-6$ und 6. Bereche damit die Vorzeichen $\epsilon_i = \epsilon_i(3)$ und bestätige das Gaußsche Vorzeichenlemma an diesem Beispiel.

Die folgende Aufgabe verallgemeinert das Eulersche Kriterium für beliebige Potenzreste.

**Aufgabe 2.** (4 Punkte)

Sei $p$ eine Primzahl und sei $e$ eine natürliche Zahl. Zeige, dass ein Element $k \in (\mathbb{Z}/(p))^\times$ genau dann eine $e$-te Wurzel besitzt, wenn $k^{\frac{p-1}{e}} = 1$ ist.

**Aufgabe 3.** (3 Punkte)

Sei $p$ eine ungerade Primzahl und $a \in \mathbb{Z}/(p)$ primitiv. Zeige, dass von den $p$ Elementen aus $\mathbb{Z}/(p^2)$, die auf $a$ abgebildet werden, genau $p-1$ Stück primitiv in $\mathbb{Z}/(p^2)$ sind. Finde für $p = 7$ und $a = 3$ dasjenige Element $b \in \mathbb{Z}/(49)$ mit $b = a \mod 7$, das nicht primitiv ist.

**Aufgabe 4.** (4 Punkte)

Finde die Lösungen der Kongruenz

$$5x^2 + 5x + 4 = 0 \mod 91\,.$$

**Aufgabe 5.** (2 Punkte)

Die Wikiversity-Seite

`Restklassenringe (Z)/Quadratreste/Gauß Vorzeichenlemma/Fakt Beweis/Gleichungslinks`

enthält einen Beweis für das Gaußsche Vorzeichenlemma. Kopieren Sie den Inhalt der Seite in eine Unterseite Ihrer Benutzerseite (am besten mit subst::). Begründen Sie in den an den roten Gleichheitszeichen verankerten Links, warum die Gleichungen stimmen. Sagen Sie insbesondere, ob die Gleichheit in $\mathbb{Z}$ gilt oder nur $\mod p$.

**Aufgabe 6.** (3 Punkte)

Charakterisiere diejenigen positiven ungeraden Zahlen $n$ mit der Eigenschaft, dass bei dem in Aufgabe 5.13 beschriebenen Algorithmus genau zwei ungerade Zahlen auftreten (nämlich $n$ und 1).

**Aufgabe 7.** (4 Punkte)

Zeige, dass im Restklassenring $\mathbb{Z}/(n)$ die Äquivalenz gilt, dass zwei Elemente $a, b$ genau dann assoziiert sind, wenn $(a) = (b)$ ist.

Finde eine Charakterisierung für diese Äquivalenzrelation, die auf den Primfaktorzerlegungen von $n, a$ und $b$ aufbaut.

Die folgende Aufgabe setzt eine gewisse Routine im Umgang mit kommutativen Ringen voraus.

**Aufgabe 8.** (4 Punkte)

Gebe ein Beispiel von zwei Elementen $a$ und $b$ eines kommutativen Ringes derart, dass $(a) = (b)$ ist, dass aber $a$ und $b$ nicht assoziiert sind.

Dafür ist die folgende Aufgabe für Leute gedacht, die gerne Diagramme am Computer erstellen.

**Aufgabe 9.** (2-4 Punkte)

Erstelle einen Diagrammstammbaum, der für alle Zahlen (oder nur alle ungeraden Zahlen) $\leq 100$ die Wirkungsweise des in Aufgabe 5.13 beschriebenen Algorithmus widergibt. Der Übersichtlichkeit halber könnte es sinnvoll sein, nur die Schritte von einer ungeraden Zahl zur algorithmisch folgenden ungeraden Zahl darzustellen. Die 1 sollte die (Ziel-)Wurzel des Stammbaums sein. Ein solches Diagramm kann direkt in Wikiversity erstellt werden oder aber in einem von Wiki-Commons akzeptierten Format (dort hochladen und hier einbinden).

Die Begriffe teilen, irreduzibel und prim machen in jedem Monoid Sinn (nicht nur im multiplikativen Monoid eines Ringes). In den folgenden Aufgaben werden Teilbarkeitseigenschaften in einigen kommutativen Monoiden besprochen. Da diese Aufgaben sich ähneln, können dafür maximal nur 5 Punkte gut geschrieben werden.

**Aufgabe 10.** (3 Punkte)

Betrachte die Menge $M$ derjenigen positiven Zahlen, die modulo 4 den Rest 1 haben. Zeige, dass $M$ mit der Multiplikation ein kommutatives Monoid ist. Bestimme die irreduziblen Elemente und die Primelemente von $M$. Zeige, dass in $M$ jedes Element Produkt von irreduziblen Elementen ist, aber keine eindeutige Primfaktorzerlegung in $M$ gilt.

**Aufgabe 11.** (3 Punkte)

Betrachte die Menge $G$ der positiven geraden Zahlen zusammen mit 1. Zeige, dass $G$ ein kommutatives Monoid ist. Bestimme die irreduziblen Elemente und die Primelemente von $G$. Zeige, dass in $G$ jedes Element Produkt von irreduziblen Elementen ist, aber keine eindeutige Primfaktorzerlegung in $G$ gilt.

**Aufgabe 12.** (2 Punkte)

Betrachte die natürlichen Zahlen $\mathbb{N}$ als kommutatives Monoid mit der Addition und neutralem Element 0. Bestimme die irreduziblen Elemente und die Primelemente von diesem Monoid. Gilt die eindeutige Primfaktorzerlegung?