W.Knapp Tübingen, den 1. Juli 2010

45. Bestimmen Sie die Menge aller Primelemente π des Rings $R = \mathbb{Z}[i]$ mit $|\pi| \leq 7$ und stellen Sie das Ergebnis zeichnerisch in der komplexen Zahlenebene $\mathbb{C}$ dar.

46. Berechnen Sie mit Hilfe des Quadratischen Reziprozitätsgesetzes bzw. der zugehörigen Ergänzungsformeln die Legendre-Symbole bzw. Jacobi-Symbole $\left(\frac{46}{53}\right)$, $\left(\frac{128}{759}\right)$, $\left(\frac{759}{843}\right)$, $\left(\frac{720}{3333}\right)$. (4 Punkte)

47. Im Folgenden schreiben wir $\mathrm{Pr}(n) := (\mathbb{Z}/n)^*$ für die Prime-Restklassen-Gruppe zum Modul $1 \leq n \in \mathbb{N}$. Sei p eine ungerade Primzahl und $1 \leq m \in \mathbb{N}$.

(a) Beweisen Sie, dass $\mathrm{Pr}(p^m)$ zyklisch ist.

Hinweis: Behandeln Sie zuerst den Fall $m = 1$ und zeigen Sie dann, dass die Restklasse $1 + p + p^m\mathbb{Z}$ die Ordnung p^{m-1} in $\mathrm{Pr}(p^m)$ besitzt (mit Übungsaufgabe 35) und deshalb den Kern des natürlichen Epimorphismus $\mathrm{Pr}(p^m) \to \mathrm{Pr}(p) = {\mathbb{F}_p}^* : x + p^m\mathbb{Z} \mapsto x + p\mathbb{Z}$ erzeugt. Betrachten Sie dann eine geeignete Restklasse $a^{p^\ell}(1 + p) + p^m\mathbb{Z}$, wobei a eine Primitivwurzel modulo p ist und $0 \leq \ell \leq m - 1$.

(b) Beweisen Sie, dass $\mathrm{Pr}(2) \cong \{1\} \cong Z_1$ und $\mathrm{Pr}(4) = \langle 3 + 4\mathbb{Z}\rangle \cong Z_2$ gilt, hingegen für $3 \leq m \in \mathbb{N}$ die Isomorphie $\mathrm{Pr}(2^m) \cong Z_2 \times Z_{2^{m-2}}$ vorliegt, die Prime-Restklassen-Gruppe also nicht zyklisch ist.

Hinweis: Zeigen Sie, dass für $m \geq 3$ der Kern C des natürlichen Epimorphismus $\mathrm{Pr}(2^m) \to \mathrm{Pr}(4)$ von der Restklasse $5 + 2^m\mathbb{Z}$ erzeugt wird und dass $-1 + 2^m\mathbb{Z} \notin C$ gilt.

(c) Bestimmen Sie alle positiven natürlichen Zahlen n, für welche die Prime-Restklassen-Gruppe $\mathrm{Pr}(n)$ zyklisch ist. (6 Punkte)

48. (a) Beweisen Sie das folgende *Kriterium von Artjuhov-Selfridge* :
Sei p eine ungerade Primzahl, $p - 1 = 2^r q$ mit ungeradem q. Dann gilt für jedes $x \in \mathbb{Z} \setminus p\mathbb{Z}$ folgendes:
(i) $x^q \equiv 1 \pmod{p}$ oder
(ii) $x^{q2^\ell} \equiv -1 \pmod{p}$ für genau ein $\ell \in \{0, \ldots, r - 1\}$.

(b) Bestimmen Sie die relative Häufigkeit („Wahrscheinlichkeit“), mit welcher der Fall (i) und mit welcher der Fall (ii) auftritt.
(Warum ist es dabei kein wirkliches Problem, dass die Menge $\mathbb{Z}\setminus p\mathbb{Z}$ unendlich ist ?) (2 Punkte)

Hinweis: Vgl. Übungsaufgabe 36. Das Kriterium von Artjuhov-Selfridge bildet eine Grundlage für den Primzahltest von Miller und Rabin.

Die Übungsaufgaben 46, 47 und 48 sind schriftlich zu bearbeiten und in der Vorlesungspause am Dienstag, dem 6. Juli 2010, abzugeben.