W.Knapp Tübingen, den 1. Mai 2007

8. Im Folgenden schreiben wir $\mathrm{Pr}(n) := (\mathbb{Z}/n\mathbb{Z})^*$ 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 $\mathrm{Pr}(p^m)$ isomorph zu $Z_{p-1} \times Z_{p^{m-1}}$ und somit zyklisch ist.
Hinweis: Behandeln Sie zuerst den Fall $m = 1$ und zeigen Sie dann, dass die Restklasse $1 + p + p^m\mathbb{Z}$ den Kern des natürlichen Epimorphismus $\mathrm{Pr}(p^m) \to \mathrm{Pr}(p) = {\mathbb{F}_p}^*$ erzeugt. Verwenden Sie dann den Satz von Sylow (oder entsprechende Sätze über abelsche Gruppen) und den chinesischen Reste-Satz.

(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.

9. Es sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik p mit genau $q = p^m$ Elementen. Beweisen Sie:
   (a) In $\mathbb{F}_q$ ist jedes Element Summe von 2 Quadraten.
   (b) Die Gleichung $x^2 + y^2 = 0$ hat in ${\mathbb{F}_q}^2$ genau dann eine von $(0, 0)$ verschiedene Lösung, wenn $p = 2$ oder $q \equiv 1 \pmod 4$ gilt. (7 Punkte)

10. Sei p eine Primzahl.
   (a) Klären Sie, in welchen Fällen die diophantische Gleichung
   $$x^2 + y^2 = pz^2$$
   eine nichttriviale Lösung $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ besitzt.
   (b) Klären Sie, in welchen Fällen die diophantische Gleichung
   $$x^2 + y^2 = pz$$
   eine nichttriviale Lösung $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ besitzt. (7 Punkte)

11. Beweisen Sie:
   (a) Ist p eine Primzahl und gilt $4x^2 + 1 \equiv 0 \pmod p$ für ein $x \in \mathbb{Z}$, so ist $p \equiv 1 \pmod 4$.
   (b) Beweisen Sie, dass es jeweils unendlich viele Primzahlen p gibt, für welche $p \equiv 3 \pmod 4$ bzw. $p \equiv 1 \pmod 4$ gilt.

   Hinweis: Beachten Sie das Resultat von Übungsaufgabe 9. Verwenden Sie das Argument des Beweises von Euklid, dass es unendlich viele Primzahlen gibt, in Verbindung mit der Betrachtung von Zahlen der Art $4\prod_{i\in m} p_i - 1$ bzw. $(2\prod_{i\in m} p_i)^2 + 1$. (6 Punkte)

Die Übungsaufgaben 9, 10 und 11 sind schriftlich zu bearbeiten und vor der Vorlesung am Mittwoch, dem 9. Mai 2007, abzugeben.