UNIVERSITÄT ULM
Institut für Zahlentheorie und Wahrscheinlichkeitstheorie

Übungen zur Elementaren Zahlentheorie

Prof. Dr. Helmut Maier, Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte

Übungsblatt 6

Abgabe: Mittwoch, 25. Mai 2011, vor den Übungen

1. Es sei $p \equiv 1 \bmod 4$ eine Primzahl.

   (a) Es seien
   $$V := \prod_{1 \le m \le \frac{p-1}{2}} m \quad \text{und} \quad W := \prod_{\frac{p-1}{2} < m \le p-1} m.$$
   Zeige: $V \equiv W \bmod p$.

   (b) Zeige: $V^2 \equiv -1 \bmod p$.

   Hinweis:
   Verwende dazu den Satz von Wilson (Übungsblatt 5, Aufgabe 2).

   (c) Es sei $\mathcal{M} = \{(x, y) \in \mathbb{Z}^2 \colon 0 \le x, y < \sqrt{p}\}$.
   Zeige: Es gibt Paare $(x_1, y_1) \neq (x_2, y_2) \in \mathcal{M}$ mit $x_1 + V y_1 \equiv x_2 + V y_2 \bmod p$.

   (d) Zeige: $p = (x_1 - x_2)^2 + (y_1 - y_2)^2$.
   Jede Primzahl $p \equiv 1 \bmod 4$ ist also Summe zweier Quadratzahlen.

   (e) Zeige: Eine Primzahl $p \equiv 3 \bmod 4$ ist niemals die Summe zweier Quadratzahlen. (14 Punkte)

2. Pierre de Fermats Vermutung, alle Fermatzahlen $F_k := 2^{2^k} + 1$ seien prim, wurde 1732 von Leonhard Euler mit der zusammengesetzten Zahl $F_5 = 2^{32} + 1$ widerlegt. Folgere aus den beiden Gleichungen
   $$641 = 5 \cdot 2^7 + 1 \quad \text{und} \quad 641 = 5^4 + 2^4$$
   die Gültigkeit von $641 \mid (2^{32} + 1)$. (4 Punkte)

3. Bestimme mit Hilfe des Chinesischen Restsatzes die Anzahl der Nullstellen des Polynoms
   $$P(x) = 7x^3 + 5x^2 + 3x$$
   über dem Ring $\mathbb{Z}/210\mathbb{Z}$. Die Lösungen brauchen nicht explizit angegeben werden.

   Hinweis:
   Berechne dazu zunächst die Anzahl der Nullstellen von $P(x)$ über den Ringen $\mathbb{Z}/p\mathbb{Z}$ für die Primzahlen $p \mid 210$.

   (6 Punkte)