Übungen zur Angewandten Diskreten Mathematik

Dr. Hartmut Lanzinger, Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte

Abgabe: Freitag, 30. November 2012, vor den Übungen

1. (a) Berechne $\varphi(167)$ und $\varphi(169)$.

   (b) Bestimme $5^{1280} \bmod 167$ und $5^{1280} \bmod 169$. (8 Punkte)

2. Es sei p eine Primzahl.

   (a) Zeige: $(p-2)! \equiv 1 \bmod p$.

   (b) Zeige: $(p-1)! \equiv p-1 \bmod (1+2+3+\ldots+(p-1))$

   (c) Es sei $a \in \mathbb{Z}$. Zeige: $p|(a^p + a \cdot (p-1)!)$ und $p|(a + a^p \cdot (p-1)!)$ (8 Punkte)

3. Es sei das Produkt

$$V := \prod_{1 \leq m \leq \frac{p-1}{2}} m$$

   mit einer Primzahl $p \equiv 1 \bmod 4$ gegeben. Wie im Beweis zum Satz von Wilson folgt $V^2 \equiv -1 \bmod p$. Weiter sei $\mathcal{M} = \{(x,y) \in \mathbb{Z}^2 \colon 0 \leq x, y < \sqrt{p}\}$. Zeige:

   (a) Es gibt Paare $(x_1, y_1) \neq (x_2, y_2) \in \mathcal{M}$ mit $x_1 + Vy_1 \equiv x_2 + Vy_2 \bmod p$.

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

   (c) Eine Primzahl $p \equiv 3 \bmod 4$ ist niemals die Summe zweier Quadratzahlen. (8 Punkte)