UNIVERSITÄT ULM
Institut für Zahlentheorie und Wahrscheinlichkeitstheorie

Übungen zur Elementaren Zahlentheorie

Prof. Dr. Helmut Maier, Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte

Übungsblatt 7

Abgabe: Mittwoch, 1. Juni 2011, vor den Übungen

1. Bestimme mittels des Chinesischen Restsatzes die Lösungen von
   (a) $x^6 - 11x^4 + 36x^2 - 36 \equiv 0 \bmod 135$
   (b) $x^3 - 3x + 27 \equiv 0 \bmod 45$. (5 Punkte)

2. Es sei $p \in \mathbb{P}$ und $a, b \in \mathbb{Z}/p\mathbb{Z}$. Zeige:
   (a) $(a+b)^p \equiv a^p + b^p \bmod p$.
   (b) Ist $\alpha \in \mathbb{N}$ und $m \equiv 1 \bmod p^\alpha$, so gilt $m^p \equiv 1 \bmod p^{\alpha+1}$. (4 Punkte)

3. Es sei $p \in \mathbb{P}$ mit $p > 3$. Weiter sei mit $a, b \in \mathbb{N}$
   $$S(p) := 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} = \frac{a}{b}.$$
   Wir wollen in dieser Aufgabe $a \equiv 0 \bmod p^2$ zeigen, der Zähler soll also durch p^2 teilbar sein.
   (a) Betrachte die Funktion $f\colon \mathbb{Z} \to \mathbb{Z}$ mit
   $$f(x) := \prod_{n=1}^{p-1} (x-n) = \sum_{k=0}^{p-1} s_k(p) x^k.$$
   Bestimme die Koeffizienten $s_0(p)$, $s_1(p)$ und $s_{p-1}(p)$.
   (b) Beweise: es genügt nun $s_1(p) \equiv 0 \bmod p^2$ zu zeigen.
   (c) Zeige: Für alle $k = 1, \ldots, p-2$ gilt $s_k(p) \equiv 0 \bmod p$.

   Hinweis:
   Multipliziere $f(x)$ mit x, substituiere $x = y - 1$ und vergleiche dann die Koeffizienten.
   (d) Folgere nun die Aussage $s_1(p) \equiv 0 \bmod p^2$.

   Hinweis:
   Bestimme dazu $f(p)$.
   (e) Zeige: $\binom{2p-1}{p-1} \equiv 1 \bmod p^3$. (15 Punkte)