Übungen zur Angewandten Diskreten Mathematik

Prof. Dr. Helmut Maier, Dr. Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte

Abgabe: Freitag, 30. Januar 2015, vor den Übungen

1. (a) Bestimme die Anzahl der 77sten Potenzreste modulo 242.
   (b) Gib diese 77sten Potenzreste explizit an.
   (c) Wieviele Lösungen besitzen die Kongruenzen $x^{77} \equiv 161 \bmod 242$ bzw. $x^{77} \equiv 181 \bmod 242$?
   (d) Untersuche Teilaufgabe a) für den Modul 239.
   (e) Zeige, dass 10 ein quadratischer Rest modulo 239 ist.
   (f) Gib zwei Lösungen der Kongruenz $x^2 \equiv 10 \bmod 239$ an. (12 Punkte)

2. Es sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann setzen wir

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{falls } a \text{ ein quadratischer Rest modulo } p \text{ ist} \\ -1, & \text{falls } a \text{ ein quadratischer Nichtrest modulo } p \text{ ist} \\ 0, & \text{falls } p|a. \end{cases}$$

   Dabei heißt $\left(\frac{a}{p}\right)$ das Legendre- Symbol.

   (a) Es sei $b \in \mathbb{Z}$. Zeige:
      i. Das Legendre- Symbol ist multiplikativ: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.
      ii. Es gilt $\left(\frac{a^2}{p}\right) = 1$.
      iii. Aus $a \equiv b \bmod p$ folgt $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

   Es gilt das quadratische Reziprozitätsgesetz (dies braucht nicht gezeigt werden):
   Es seien p und q ungerade Primzahlen. Dann gilt

   - $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

   Weiter gelten sogenannte Ergänzungssätze:

   - $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
   - $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

   (b) i. Bestimme die Legendre- Symbole

$$\left(\frac{10}{239}\right) \quad \text{und} \quad \left(\frac{61}{211}\right).$$

      ii. Es gilt $1201, 2017 \in \mathbb{P}$. Welche Potenz ist nach den Verfahren in Abschnitt 1.18 zu berechnen, um entscheiden zu können, ob die Kongruenz $x^2 \equiv 1201 \bmod 2017$ lösbar ist?
      iii. Untersuche die Lösbarkeit der Kongruenz aus ii) mit dem Legendre- Symbol. (12 Punkte)