ulm university universität ulm

Übungen zur Elementaren Zahlentheorie

Prof. Dr. Helmut Maier, Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte
Abgabe: Dienstag, 5. Juli 2016, vor den Übungen

1. Im Gegensatz zu zyklischen Gruppen bestehen Erzeugendensysteme nichtzyklischer Gruppen aus mehr als nur einem Element. Wir wollen ein Erzeugendensystem für die Gruppe $G = ((\mathbb{Z}/2016\mathbb{Z})^*, \cdot)$ bestimmen. Dazu benützen wir die Konzepte der vergangenen Abschnitte.

   (a) Zeige, dass G nicht zyklisch ist.

   (b) Die Mindestgröße eines Erzeugendensystems der Gruppe $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ mit $n = 2^\epsilon \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ mit $n > 2$ ist durch
   $$g(\epsilon, k) = \begin{cases} k, & \text{falls } \epsilon < 2 \\ k+1, & \text{falls } \epsilon = 2 \\ k+2, & \text{falls } \epsilon > 2 \end{cases}$$
   gegeben. Bestimme die Mindestgröße eines Erzeugendensystems von G.

   (c) Der "Hauptsatz über endliche abelsche Gruppen" besagt, dass jede endliche abelsche Gruppe zu einem direkten Produkt zyklischer Gruppen isomorph ist. Dabei existiert eine eindeutig bestimmte Darstellung mit $g(\epsilon, k)$ Faktoren, wobei für die Gruppenordnung m_i der jeweiligen Faktoren
   $$|G| = \prod_{i=1}^{g(\epsilon,k)} m_i$$
   sowie $m_{i+1} | m_i$ mit $m_1 := kgV(f, \varphi(p_1^{\alpha_1}), \ldots, \varphi(p_k^{\alpha_k}))$ mit
   $$f := \begin{cases} 1, & \text{falls } \epsilon < 2 \\ 2, & \text{falls } \epsilon = 2 \\ 2^{\epsilon-2}, & \text{falls } \epsilon > 2 \end{cases}$$
   und $m_{g(\epsilon,k)} \geq 2$ gilt. Bestimme daraus $m_1, \ldots, m_{g(\epsilon,k)}$ und die Zerlegung von G.

   (d) Bestimme für alle $1 \leq j \leq k$ Primitivwurzeln modulo $p_j^{\alpha_j}$.

   (e) Gib ein Erzeugendensystem von $((\mathbb{Z}/2^\epsilon\mathbb{Z})^*, \cdot)$ an.

   Für die in Teilaufgabe b) gefundene Struktur von G als Produkt zyklischer Gruppen verwenden wir nun Untergruppen von G. Dazu benötigen wir Elemente $a_i \in G$ mit $\operatorname{ord} a_i = m_i$ für $1 \leq i \leq g(\epsilon, k)$.

   (f) Zeige $\operatorname{ord}_{2016} 101 \leq 24$.

   (g) Bestimme $g(\epsilon, k)$ Elemente $y_i \in G$, deren Ordnung der Gruppenordnung m_i entspricht.

   Hinweis:
   Für Kongruenzen $x \equiv a_t \bmod q_t$ mit $\operatorname{ord}_{q_t} a_t = o_t$ für $1 \leq t \leq r$ gilt $\operatorname{ord}_q a = kgV(o_1, \ldots, o_r)$ für das nach dem Chinesischen Restsatz modulo $q = q_1 \cdots q_r$ eindeutig bestimmte $x \equiv a \bmod q$.

   (h) Prüfe, ob $\langle y_{i_1} \rangle \cap \langle y_{i_2} \rangle = \{1\}$ mit $1 \leq i_1 < i_2 \leq g(\epsilon, k)$ gilt.
   Andernfalls bestimme neue Werte y_i und wiederhole das Vorgehen.

   (i) Gib ein Erzeugendensystem von G an. (12 Punkte)

2. Es gilt $10007 \in \mathbb{P}$, $F_3 = 257$, $F_4 = 65537$ und $10001 = 137 \cdot 73$.

   (a) Berechne folgende Legendre- Symbole:

   i. $\left(\frac{7837}{10007}\right)$

   ii. $\left(\frac{10001}{65537}\right)$

   (b) Überprüfe die Lösbarkeit folgender Kongruenzen:

   i. $x^2 \equiv 17 \bmod 10007$

   ii. $x^2 \equiv 27 \bmod 257$

   (c) Zeige, dass $x^3 \equiv 11 \bmod 23$ lösbar ist und gib die Lösungsgesamtheit an. (8 Punkte)

3. Es sei $p \in \mathbb{P}$.

   (a) Für welche p ist 5 ein quadratischer Rest modulo p?

   (b) Es sei $x \in \mathbb{Z}$ und $p|(20x^2 - 1)$. Zeige, dass $p \equiv 1 \bmod 5$ oder $p \equiv 4 \bmod 5$ gilt.

   (c) Folgere aus den Teilaufgaben a) und b), dass unendlich viele Primzahlen existieren, deren Darstellung im gewöhnlichen Dezimalsystem auf die Ziffer 9 endet. (4 Punkte)