Übungen zur Elementaren Zahlentheorie

Prof. Dr. Helmut Maier, Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte
Abgabe: Dienstag, 28. Juni 2016, vor den Übungen

1. Ein Weg zur Bestimmung einer Liste von Primzahlen ist der folgende Algorithmus:

   Es sei $N \in \mathbb{N}$, und es liege eine Liste aller natürlichen Zahlen von 1 bis N vor.

   - Streiche die 1.
   - Markiere die 2 als Primzahl und streiche alle Vielfachen von 2.
   - Betrachte nun die kleinste nicht gestrichene und nicht markierte Zahl $p > 1$ auf der Liste.
   - Markiere diese Zahl als Primzahl und streiche alle Vielfachen von p.
   - Wiederhole die beiden letzten Schritte, bis alle Zahlen in der Liste entweder gestrichen oder als Primzahl markiert sind.

   (a) Es sei $N = 110$. Führe obiges Verfahren durch und bestimme alle Primzahlen unterhalb 110.

   (b) Führe nun ausgehend von diesem Schema dasselbe Verfahren "rückwärts" durch und lies daraus alle Darstellungen der Zahl 110 als Summe von zwei Primzahlen ab.

   (c) Zwei Primzahlen werden Primzahlzwillinge genannt, wenn für eine Primzahl p die Zahl $p + 2$ ebenfalls wieder eine Primzahl ist.
   Modifiziere dieses Verfahren derart, um eine Liste aller Primzahlzwillinge zu erhalten.

   (d) Bestimme mit Teilaufgabe c) alle Primzahlzwillinge zwischen 1 und 110. (6 Punkte)

2. 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 8, Aufgabe 3).

   (c) Es sei $\mathcal{M} = \{(x, y) \in \mathbb{Z}^2 : 0 \le x, y < \sqrt{p}\}$.
   Zeige, dass Paare $(x_1, y_1) \neq (x_2, y_2) \in \mathcal{M}$ mit $x_1 + Vy_1 \equiv x_2 + Vy_2 \bmod p$ existieren.

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

   (e) Zeige, dass eine Primzahl $p \equiv 3 \bmod 4$ niemals die Summe zweier Quadrate ist. (7 Punkte)

3. Bestimme die Faktorisierung von 7837 mittels des Pollardschen- Rho- Verfahrens. (3 Punkte)

4. (a) Begründe, warum zum Modul 54 eine Primitivwurzel existiert.
   (b) Wieviele teilerfremde Restklassen modulo 54 gibt es?
   (c) Gib diese teilerfremden Restklassen modulo 54 explizit an.
   (d) Welche Ordnung besitzt das Element 7 modulo 54?
   (e) Zeige, dass 5 eine Primitivwurzel modulo 54 ist.
   (f) Wieviele zehnte Potenzreste gibt es modulo 54?
   (g) Überprüfe, ob 19 zehnter Potenzrest modulo 54 ist.
   (h) Wieviele Lösungen besitzt dann die Kongruenz $x^{10} \equiv 19 \bmod 54$? (8 Punkte)