Übungen zur Elementaren Zahlentheorie

Prof. Dr. Helmut Maier, Hans- Peter Reck

Gesamtpunktzahl: 36 Punkte, alles Zusatzpunkte
Abgabe: Dienstag, 12. Juli 2016, vor den Übungen

1. Tabea möchte Marina Nachrichten versenden, ohne dabei abgehört zu werden.
   Marina veröffentlicht ihren öffentlichen Schlüssel $S = (e, n)$ mit $e = 37$ und $n = 11 \cdot 19 = 209$.
   (a) Tabea möchte die Botschaft $B = 17$ verschlüsselt an Marina senden.
   Welchen Wert C schickt sie weiter?
   (b) Aufgrund einer Störung erhält Marina allerdings die Botschaft $C = 17$.
   Was vermutet sie als ursprüngliche Information? (9 Punkte)

2. Es sei $n \in \mathbb{N}$ mit $n = p \cdot q$ mit $p, q \in \mathbb{P}$.
   (a) Es seien die Größen n und $\varphi(n)$ als Zahlenwerte bekannt.
   Ermittle ein Verfahren, daraus die Werte von p und q zu bestimmen.
   (b) Es seien $n = p \cdot q = 292\,937$ und $\varphi(n) = 291\,840$ gegeben. Bestimme p und q. (6 Punkte)

3. (a) Zeige Satz 6.2.1, d.h. dass unendlich viele Pseudoprimzahlen zur Basis 2 existieren.
   (b) Zeige Satz 6.2.2, d.h. dass eine Zahl $n \in \mathbb{N}$ genau dann eine Carmichael- Zahl ist, wenn $n = p_1 \cdot p_2 \cdots p_r$ mit $r \geq 3$ und paarweise verschiedenen ungeraden Primzahlen p_i ist, für die $(p_i - 1) | (n - 1)$ für alle $1 \leq i \leq r$ gilt. (7 Punkte)

4. Es sei $p \in \mathbb{P}$ und M_p die bereits von Übungsblatt 2 bekannten Mersenne- Zahlen.
   (a) Es sei $\omega = 2 + \sqrt{3}$ und $\overline{\omega} = 2 - \sqrt{3}$. Weiter sei die Folge s_i rekursiv über
   $$s_i := \begin{cases} 4 & \text{für } i = 0, \\ s_{i-1}^2 - 2 & \text{für } i > 0 \end{cases}$$
   definiert. Zeige mittels vollständiger Induktion $s_i = \omega^{2^i} + \overline{\omega}^{2^i}$.
   (b) Gilt $s_{p-2} \equiv 0 \bmod M_p$, so ist $\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1$ für ein $k \in \mathbb{Z}$.
   (c) Es sei nun q der kleinste Primfaktor von M_p und $X := \{a + b \cdot \sqrt{3} \colon a, b \in \mathbb{Z}/q\mathbb{Z}\}$, wobei die Multiplikation $\circ$ in X über
   $$(a + b \cdot \sqrt{3}) \circ (c + d \cdot \sqrt{3}) = ((ac + 3bd) \bmod q) + \sqrt{3} \cdot ((ad + bc) \bmod q)$$
   definiert ist.
   Es sei X^* die Menge der Einheiten von X, d.h. $X^* := \{\alpha \in X \colon \exists \beta \in X \text{ mit } \alpha \circ \beta \equiv 1 \bmod q\}$.
   Zeige, dass $(X^*, \circ)$ eine Gruppe darstellt.
   (d) Für $\alpha \in X^*$ sei $\operatorname{ord}_q \alpha := \min\{k \in \mathbb{N} \colon \alpha^k \equiv 1 \bmod q\}$. Zudem gelte $s_{p-2} \equiv 0 \bmod M_p$.
   Zeige: $\operatorname{ord}_q \omega = 2^p$.
   (e) Wir nehmen nun an, es gelte $q < M_p$ und $s_{p-2} \equiv 0 \bmod M_p$. Führe dies zu einem Widerspruch.
   (f) Zeige: Gilt $s_{p-2} \equiv 0 \bmod M_p$, so ist M_p eine Primzahl.
   (g) Zeige mit diesem Verfahren, dass M_7 eine Primzahl ist. (14 Punkte)