

Übungen zur Angewandten Diskreten Mathematik

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

Gesamtpunktzahl: 24 Punkte

Abgabe: Freitag, 16. Januar 2015, vor den Übungen

1. Es sei $G = ((\mathbb{Z}/32\mathbb{Z})^*, \cdot)$ und $M = \{-1 \bmod 32, 5 \bmod 32\}$.
 - (a) Zeige $G = \langle M \rangle$.
 - (b) Zeige mittels Bestimmung der Ordnungen aller Elemente von G , dass G nicht zyklisch ist. (5 Punkte)

2. Es ist $341 = 11 \cdot 31$.
 - (a) Zeige:
 - i. $2^{340} \equiv 1 \pmod{11}$
 - ii. $2^{340} \equiv 1 \pmod{31}$
 - (b) Es sei $b, n \in \mathbb{N}$. Ist n zusammengesetzt und gilt $b^{n-1} \equiv 1 \pmod{n}$ für $\text{ggT}(b, n) = 1$, so heißt n eine Pseudoprimumzahl zur Basis b . Zeige, dass $n = 341$ eine Pseudoprimumzahl zur Basis 2 ist. (4 Punkte)

3.
 - (a) Zeige, dass $\text{ord}_{341} a \leq 30$ für alle a mit $\text{ggT}(a, 341) = 1$.
 - (b) Gibt es ein a mit $\text{ord}_{341} a = 30$? (4 Punkte)

4. Es sei $G = ((\mathbb{Z}/338\mathbb{Z})^*, \cdot)$.
 - (a) Bestimme die Anzahl der Elemente von G .
 - (b) Zeige, dass G zyklisch ist.
 - (c) Wieviele Primitivwurzeln besitzt G ?
 - (d) Bestimme eine Primitivwurzel von G .
 - (e) Wieviele Untergruppen besitzt G ?
 - (f) Konstruiere eine Untergruppe der Ordnung 12 und gib ihre Elemente explizit an.
 - (g) Welche Untergruppe erzeugt das Element $57 \bmod 338$? (11 Punkte)