Übungen zur Angewandten Diskreten Mathematik

Dr. Hartmut Lanzinger, Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte

Abgabe: Freitag, 25. Januar 2013, vor den Übungen

1. Es seien $m \in \mathbb{N}$ und $p \in \mathbb{P}$ und $p > 3$.

   (a) Es seien $2p-1$ und $3p-2$ ebenfalls prim.
   Zeige, dass $m = p \cdot (2p-1) \cdot (3p-2)$ eine Carmichael- Zahl ist.

   (b) Auf Übungsblatt 11 haben wir in Aufgabe 2 gesehen, dass $n = (6m+1) \cdot (12m+1) \cdot (18m+1)$ eine Carmichael-Zahl ist, sofern $6m+1, 12m+1, 18m+1 \in \mathbb{P}$ erfüllt ist.
   Zeige, dass die Aussage in Teilaufgabe a) dazu äquivalent ist. (6 Punkte)

2. (a) Es gelte $a^n \equiv a \bmod n^2$. Zeige, dass dann n^2 pseudoprim ist.

   (b) Zeige, dass 121 zur Basis 3 pesudoprim ist. (4 Punkte)

3. Es sei M_n eine Mersenne- Zahl und F_k die k- te Fermatzahl.
   Zeige: Gilt $n = 2^m$, so ist M_n das Produkt der ersten m Fermatzahlen, es gilt also

$$M_n = \prod_{k=0}^{m-1} F_k.$$

   (5 Punkte)

4. Bestimme die Faktorisierung der gegebenen Zahlen n mittels des Pollard- Rho- Verfahrens.

   (a) $n = 1751$

   (b) $n = 119$ (8 Punkte)