Wolfgang K. Seiler
Tel. 2515

A5, C201

19. April 2018

8. Übungsblatt Zahlentheorie

Aufgabe 1: *(9 Punkte)*

a) Zeigen Sie: Ist $p > 2$ eine Primzahl, so ist p ein Teiler von $M_{p-1} = 2^{p-1} - 1$.

b) Für jede Primzahl $p > 2$ ist $2^{M_p - 1} \equiv 1 \bmod M_p$.

c) Für jede Primzahl $p > 2$ ist $2^{2^{p-1}} \equiv 2 \bmod M_p$.

d) Ist $p > 2$ prim und q ein Primteiler von M_p, so ist $q \equiv 1 \bmod 2p$.

e) Wenden Sie dies an, um ohne Computerhilfe die Primzerlegungen von $M_{11} = 2047$ und $M_{23} = 8388607$ zu finden!

Aufgabe 2: *(6 Punkte)*

a) Für welche Zahlen a mit $2 \leq a \leq 14$ zeigt der gewöhnliche Primzahltest nach Fermat, daß 15 keine Primzahl ist?

b) Für welche Zahlen a mit $2 \leq a \leq 14$ zeigt der Primzahltest nach Miller und Rabin, daß 15 keine Primzahl ist?
Hinweis: Mit dem chinesischen Restesatz können Sie hier viel Rechenzeit sparen! Weder Computer noch Taschenrechner werden benötigt.

Aufgabe 3: *(5 Punkte)*

Faktorisieren Sie die Zahl $N = 72263$ nach Pollards $(p-1)$-Methode mit Suchgrenze $B = 10!$

Abgabe bis zum Donnerstag, dem 26. April 2018, um 10.10 Uhr