Wolfgang K. Seiler — A5, C201
Tel. 2515

25. März 2014

7. Übungsblatt Zahlentheorie

Aufgabe 1: *(9 Punkte)*

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

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) Zeigen Sie, daß $M_{11} = 2\,047$ und $M_{23} = 8\,388\,607$ nicht prim sind und finden Sie (ohne Computerhilfe) deren Primzerlegungen!

Aufgabe 2: *(6 Punkte)*

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

b) Für welche Zahlen a mit $2 \le a \le 14$ 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)*

Zeigen Sie: Eine natürliche Zahl $n > 1$ ist genau dann prim, wenn für alle Polynome $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$ mit Koeffizienten $a_i \in \mathbb{Z}/n$ gilt: $f(X^n) = f(X)^n$ in $(\mathbb{Z}/n)[X]$.

Abgabe bis zum Dienstag, dem 1. April 2014, um 11.55 Uhr