

24. März 2011

6. Übungsblatt Zahlentheorie

Aufgabe 1: (9 Punkte)

- Zeigen Sie: Ist p eine Primzahl, so ist p ein Teiler von $2^{p-1} - 1$.
- Für jede Primzahl p ist $2^{M_p-1} \equiv 1 \pmod{M_p}$.
- Für jede Primzahl p ist $2^{2^{p-1}} \equiv 2 \pmod{M_p}$.
- Ist p prim und q ein Primteiler von M_p , so ist $q \equiv 1 \pmod{2p}$.
- Zeigen Sie, daß $M_{11} = 2047$ und $M_{23} = 8388607$ nicht prim sind und finden Sie (ohne Computerhilfe) deren Primzerlegungen!

Aufgabe 2: (6 Punkte)

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

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

Abgabe bis zum Donnerstag, dem 31. März 2011, um 17.15 Uhr