Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

SS 2009
3. Juni 2009

Algorithmische Zahlentheorie

Übungsblatt 7

Aufgabe 25

Seien $n \geqslant 2$ und $k \leqslant 2^n$ natürliche Zahlen mit $3 \nmid k$. Man zeige:

$$N := k \cdot 2^n + 1$$

ist genau dann prim, wenn

$$3^{(N-1)/2} \equiv -1 \bmod N.$$

(Ein Beispiel für eine solche Primzahl ist $N := 13 \cdot 2^{1000} + 1$.)

Aufgabe 26

Für eine zusammengesetzte ungerade Zahl $N = 2^t u + 1$, (u ungerade), sei

$$T_{SS}(N) := \left\{ a \in (\mathbb{Z}/N)^* : a^{(N-1)/2} = \left(\frac{a}{N}\right) \right\}$$

die Menge der falschen Zeugen bzgl. des Solovay/Strassen-Tests und

$$T_{MR}(N) := \left\{ a \in (\mathbb{Z}/N)^* : a^u = 1 \text{ oder } \exists k \in \{0, 1 \ldots, t-1\} \text{ mit } a^{2^k u} = -1 \right\}$$

die Menge der falschen Zeugen bzgl. des Miller/Rabin-Tests.

Man berechne die Anzahlen $\varphi(N)$, $\#T_{SS}(N)$, $\#T_{MR}(N)$ für die Carmichael-Zahlen

$$N = 561, 1105, 1729.$$

Aufgabe 27

Seien q, p ungerade Primzahlen mit $p = 2q - 1$. (Beispiele dafür sind $(q, p) = (3, 5)$, $(7, 13)$, $(19, 37)$, $(31, 61)$, $(37, 73), \ldots$). Man zeige: Für $N := pq$ gilt

$$\#T_{SS}(N) = \frac{\varphi(N)}{4}.$$

Aufgabe 28

a) Man beweise: Für eine natürliche Zahl $N \equiv 3 \bmod 4$ gilt

$$T_{SS}(N) = T_{MR}(N).$$

b)* Für jedes ungerade N gilt $T_{MR}(N) \subset T_{SS}(N)$.

Abgabetermin: Freitag, 12. Juni 2009, 14 Uhr, Übungskasten im 1. Stock