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

WS 2015/16
9. Dez. 2015

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 8

Aufgabe 29

Sei t eine natürliche Zahl, so dass die drei Zahlen

$$p_1 := 6t + 1, \quad p_2 := 12t + 1, \quad p_3 := 18t + 1$$

prim sind. Man beweise, dass dann $N := p_1 p_2 p_3$ eine Carmichael-Zahl ist.

Aufgabe 30

Man beweise oder widerlege: Für jede Carmichael-Zahl N gilt $N \equiv 1 \bmod 4$.

Aufgabe 31

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 32

a) Man beweise: Eine ungerade Zahl $N \geqslant 3$ ist genau dann prim, wenn folgende zwei Bedingungen erfüllt sind:

(i) Für alle zu N teilerfremden Zahlen a gilt

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

(ii) Es gibt wenigstens eine zu N teilerfremde Zahl a mit

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

Man zeige an einem Gegenbeispiel, dass (i) allein nicht ausreicht.

b) Man beschreibe einen auf a) beruhenden probabilistischen Primzahltest. Welche Vor- und Nachteile hat dieser gegenüber dem Solovay-Strassen-Test ?