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

SS 2009
27. Mai 2009

Algorithmische Zahlentheorie

Übungsblatt 6

Aufgabe 21

a) Für die Fermat-Zahlen $F_n = 2^{2^n} + 1$ beweise man die Formel

$$F_{n+1} = F_0 F_1 \cdot \ldots \cdot F_n + 2.$$

b) Man zeige für $n \neq m$

$$\gcd(F_n, F_m) = 1.$$

Aufgabe 22

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 23

Man zeige: Keine Carmichael-Zahl ist durch 21, 39, 55 oder 57 teilbar.

Aufgabe 24

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 ?

Abgabetermin: Freitag, 5. Juni 2009, 14 Uhr, Übungskasten im 1. Stock