

Einführung in die Zahlentheorie, Übungsblatt 11

Aufgabe 41

Für die Zahlen $N_1 := 551$ und $N_2 := 561$ bestimme man die Anzahl der falschen Zeugen $a \in (\mathbb{Z}/N_k)^*$ bezüglich das Solovay-Strassen und des Miller-Rabin Primzahltests.

Aufgabe 42

Sei q eine ungerade Primzahl, so dass $p := 2q - 1$ ebenfalls prim ist und $N := pq$.
Man zeige: Die Untergruppe

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

hat genau $\varphi(N)/4$ Elemente.

Aufgabe 43

Man beweise, dass die Fermatzahl

$$F_{23} = 2^{2^{23}} + 1 = 2^{8388608} + 1$$

nicht prim ist, indem man einen Faktor von F_{23} bestimme.

Aufgabe 44

Sei $(f_n)_{n \geq 0}$ die Folge der Fibonacci-Zahlen.

a) Für jede Primzahl p gilt $p \mid f_m$, wobei $m := p - \left(\frac{5}{p} \right)$.

b) Sei $p := f_q$ eine Primzahl ≥ 5 . Dann ist bekanntlich auch q prim (vgl. Aufgabe 1). Man zeige:

$$q \mid p - \left(\frac{5}{p} \right).$$

Abgabe: Freitag, 9. Juli 2004, 11 Uhr, Übungskasten vor der Bibliothek
Wegen der Sparmaßnahmen werden nur die Aufgaben 41 und 42 korrigiert.