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

SS 2009
10. Juni 2009

Algorithmische Zahlentheorie

Übungsblatt 8

Aufgabe 29

Man beweise oder widerlege folgende Aussage: Für jede Carmichael-Zahl N gilt

$$N \equiv 1 \bmod 4.$$

Aufgabe 30

Man beweise: Zu jeder geraden Zahl $N \geqslant 4$ gibt es eine zu N teilerfremde Zahl a mit

$$a^{N-1} \not\equiv 1 \bmod N.$$

Aufgabe 31

a) Die ungerade natürliche Zahl N sei ein Produkt $N = uv$ mit $|u - v| \leqslant \alpha N^{1/4}$. Dabei sei α eine reelle Zahl, die klein gegenüber $\sqrt{N}$ sei (d.h. Terme der Gestalt $\alpha/\sqrt{N}$ sind vernachlässigbar.) Man gebe als Funktion von α eine Abschätzung für die Anzahl der Schritte, die das Fermatsche Faktorisierungs-Verfahren zur Auffindung der Faktoren u, v braucht.

b) Man zerlege die Zahl $N = 998953$ mit dem Fermatschen Faktorisierungs-Verfahren.

Aufgabe 32

a) Man zeige: Es gibt genau 22 Möglichkeiten für die letzten beiden Ziffern einer Quadratzahl im Dezimalsystem.

b) Sei Q_N die Anzahl der Quadrate im Ring $\mathbb{Z}/N$ (nach a) ist also z.B. $Q_{100} = 22$). Man beweise

$$\limsup_{N\to\infty} \frac{Q_N}{N} = \frac{1}{2}, \qquad \liminf_{N\to\infty} \frac{Q_N}{N} = 0.$$

c) Man bestimme diejenige Zahl $N \leqslant 2^{16}$, für die der Quotient Q_N/N möglichst klein wird.

Abgabetermin: Freitag, 19. Juni 2009, 14 Uhr, Übungskasten im 1. Stock