

Einführung in die Zahlentheorie, Übungsblatt 8

Aufgabe 29

- a) Man zeige, dass kein Vielfaches von 21, 39 oder 55 eine Carmichael-Zahl ist.
- b)* Man formuliere und beweise einen allgemeinen Satz, aus dem Teil a) als Spezialfall folgt.

Aufgabe 30

- a) Sei N eine Carmichael-Zahl. Man zeige: Es gibt eine natürliche Zahl a mit

$$\gcd(a, N) = 1 \quad \text{und} \quad a^{(N-1)/2} \not\equiv \pm 1 \pmod{N}. \quad (*)$$

- b) Sei N eine ungerade natürliche Zahl. Es gebe eine natürliche Zahl a mit (*). Man zeige: N ist nicht prim.

Aufgabe 31

Man führe das Fermatsche Faktorisierungs-Verfahren für die Zahl $N = 38911$ durch.

Aufgabe 32

Die ungerade natürliche Zahl N besitze eine Faktorzerlegung $N = p \cdot q$ mit

$$|p - q| \leq \alpha N^{1/4}.$$

Man schätze in Abhängigkeit von α die Anzahl der Schritte ab, die das Fermatsche Faktorisierungs-Verfahren braucht, um diese Faktorzerlegung zu finden.

Abgabe: Freitag, 18. Juni 2004, 11 Uhr, Übungskasten vor der Bibliothek

Um Kosten für Korrekturen zu sparen, bitte in Gruppen zu 2 oder 3 Teilnehmern bearbeiten und abgeben!

Klausurtermin: Mittwoch, 21. Juli 2004, 16 – 18 Uhr.