

Übungen zur Vorlesung Angewandte Diskrete Mathematik

Institut für Reine Mathematik

WS 08/09 – Blatt 05

Abgabetermin: Freitag, 21.11.2008 um 14:15 Uhr vor Beginn der Übung

1. Berechnen Sie die Exponenten modulo 35 der Zahlen 8, 17 und 31. (6 P)
2. (a) Berechnen Sie $3^{97} \pmod{101}$ mit dem schnellen Potenzier-Algorithmus (siehe Satz 2.4.2 auf Seite 41). (4 P)
(b) Sei n von der Größenordnung 10^{150} . Geben Sie eine Abschätzung für die benötigten Operationen zur Berechnung von 3^n an. (2 P)
3. Berechnen Sie $5^{133} \pmod{737}$ mit dem Chinesischen Restsatz. (4 P)
4. Sei n eine zusammengesetzte Zahl, und $a \in \mathbb{N}$ mit $\text{ggT}(a, n) = 1$. Die Zahl n heißt *Pseudoprimzahl zur Basis a*, falls (4 P)

$$a^{n-1} \equiv 1 \pmod{n}$$

gilt. Zeigen Sie: 645 ist eine Pseudoprimzahl zur Basis 2.