

Mathematik und Logik

5. Übungsaufgaben

2010-01-12

1. Überlegen Sie sich, warum eine Zahl genau dann durch 3 teilbar ist, wenn ihre Ziffernsumme durch 3 teilbar ist.
2. Bestimmen Sie den Rest von 17, 345 und 234582930937420981 bei Division durch 7. Dazu ist keine Taschenrechner erforderlich.
3. Testen Sie (mit dem in der Vorlesung vorgestellten probabilistischen Verfahren) für verschiedene Zahlen, ob sie prim sind, unter anderem: 15, 341, 2701. Testen Sie mit mehreren Basen, insbesondere bei 15 auch mit 11.
4. Sei $m = 29 \cdot 37$. Bestimmen Sie $\varphi(m)$ und das kleinste $e \geq 3$, welches modulo $\varphi(m)$ invertierbar ist.
5. Wählen Sie ein paar Zahlen $a < m$ und berechnen Sie $b := a^e \pmod{m}$.
6. Bestimmen Sie das Inverse d zu e (modulo $\varphi(m)$).
7. Berechnen Sie $b^d \pmod{m}$.
8. Berechnen Sie a^e modulo 29 und auch modulo 37 (möglichst mit a und e aus den obigen Beispielen). Bestimmen Sie daraus a^e modulo $29 \cdot 37$.