

13. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)**Abgabe: Freitag 8.7.2011, bis 9.15 Uhr****Gruppen 1 und 2 (Mo): Fach Nr. 3 (orangener Schrank bei D1.348)****Gruppen 3 und 4 (Do): Fach Nr. 11 (orangener Schrank bei D1.348)****Internet:** <http://math-www.uni-paderborn.de/~chris>

Schreibe bitte auf die erste Seite **gut** leserlich Namen, Vornamen, Matrikel-Nr., die Nr. deiner Übungsgruppe und eine **Tabelle** für die Punkte. Hefte bitte die Seiten zusammen!

Es können **Bonuspunkte** für die Leistungsnachweis-Klausur erworben werden.

Es ist nur Einzelabgabe erlaubt. **Es sind immer Begründungen erforderlich!**

35. Aufgabe: Seien $a, b, c, d \in \mathbb{Z}$ und $n \in \mathbb{N}$. Beweise:

a) $a \bmod n = b \bmod n$ und $c \bmod n = d \bmod n \implies (a \cdot c) \bmod n = (b \cdot d) \bmod n$.

b) Aus $a \bmod n = b \bmod n$ folgt $a^2 \bmod n = b^2 \bmod n$ und $a^3 \bmod n = b^3 \bmod n$.

Hinweis zu b): c) darf hier nicht benutzt werden!

c) Aus $a \bmod n = b \bmod n$ folgt $a^k \bmod n = b^k \bmod n$ für alle $k \in \mathbb{N}_0$. (4)

36. Aufgabe: Berechne $1004^{482} \bmod 27$.

Hinweis: Versuche, die Basis und den Exponenten der Potenz zu verkleinern.

Potenzen modulo 27 dürfen **nicht** mit einem Rechner berechnet werden! (3)

37. Aufgabe: Seien $a, b \in \mathbb{Z}$ und $m, n \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$. Beweise:

Aus $a \bmod m = b \bmod m$ und $a \bmod n = b \bmod n$ folgt $a \bmod (m \cdot n) = b \bmod (m \cdot n)$. (2)

38. Aufgabe: Sei $n := p \cdot q$ mit Primzahlen $p = 127$ und $q = 137$ (es muss nicht bewiesen werden, dass p und q prim sind). Ferner sei $e := 25$.

a) Beweise, dass e und $\varphi(n)$ teilerfremd sind.

b) Berechne eine Zahl $d \in \mathcal{R}_n$ mit $(e \cdot d) \bmod \varphi(n) = 1$.

c) Berechne $30^e \bmod n$ (**Hinweis:** Es darf $30^{12} \bmod n = 4229$ benutzt werden!)

d) Berechne $(30^e)^d \bmod n$.

e) Berechne $(127^e)^d \bmod n$.

Hinweis zu e): Berechne $(127^e)^d \bmod 127$ und $(127^e)^d \bmod 137$ und benutze Aufgabe 37. (7)