

## 12. Aufgabenblatt

**KRYPTOGRAPHIE (für GHRG) (SS 2011)****Abgabe: Freitag 1.7.2011, 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!**

**31. Aufgabe:** Sei  $n \in \mathbb{N}$  eine beliebige Zahl.

a) Beweise, dass  $n - 1$  ein Inverses modulo  $n$  besitzt, und bestimme ein  $x \in \mathcal{R}_n$  mit der Eigenschaft  $((n - 1) \cdot x) \bmod n = 1$ .

b) Kann es Zahlen  $x, y \in \mathcal{R}_n$  geben mit  $x \neq y$  und  $((n - 1) \cdot x) \bmod n = 1$  und  $((n - 1) \cdot y) \bmod n = 1$ ? Begründe deine Antwort! (3)

**32. Aufgabe:** Es ist  $\mathcal{R}'_{26} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ .

a) Berechne explizit alle Elemente der Menge  $T = \{(-3) \cdot r \bmod 26 \mid r \in \mathcal{R}'_{26}\}$ .

b) In welchem Verhältnis stehen die beiden Mengen  $T$  und  $\mathcal{R}'_{26}$  zueinander?

**Hinweis:** Satz (9.6) darf für diese Aufgabe nicht benutzt werden! (3)

**33. Aufgabe:** a) Berechne  $\varphi(729)$ ,  $\varphi(2048)$ ,  $\varphi(323)$ .

b) Beweise: Für alle  $k \in \mathbb{N}$  gilt:  $\varphi(2^k) = 2^{k-1}$ ,  $\varphi(3^k) = 2 \cdot 3^{k-1}$ .

c) Sei  $a = 2^m \cdot 3^n$  mit beliebigen Exponenten  $m, n \in \mathbb{N}$ . Beweise unter Benutzung von (9.5b):  $\varphi(a) = \frac{a}{3}$ .

d) Berechne  $\varphi(3500)$  unter Benutzung von (9.5b). (6)

**34. Aufgabe:** Seien  $a = 441\,218$  und  $b = 29\,374$ .

a) Berechne  $\text{ggT}(a, b)$

1) mit Hilfe von Primfaktorzerlegungen (das Bestimmen der Primfaktorzerlegungen ist zu dokumentieren und für Zahlen  $\geq 100$  ist ein Primzahlachweis erforderlich!)

2) mit Hilfe des euklidischen Algorithmus.

b) Stelle  $\text{ggT}(a, b)$  als ganzzahlige Linearkombination von  $a$  und  $b$  dar. Ist dies mit der ersten Methode möglich? (6)