

10. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)**Abgabe: Freitag 17.6.2011, 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!**

25. Aufgabe: Seien $a, b, c \in \mathbb{Z}$.a) Beweise: $a \mid b$ und $a \mid c \implies a \mid (xb + yc)$ für alle $x, y \in \mathbb{Z}$.**Hinweis:** Arbeite mit der ursprünglichen Definition (8.1) der Teilbarkeit.b) Leite aus a) her: $a \mid b$ und $a \mid c \implies a \mid (b + c)$ und $a \mid (2b - c)$. (3)**26. Aufgabe:** Seien $a, b \in \mathbb{Z}$.a) Beweise: $a \mid b \iff T(a) \subseteq T(b)$ b) Sei $a \neq 0$. Beweise auf Grundlage von (8.3) unter Benutzung von a):

$$a \mid b \iff \text{ggT}(a, b) = |a|.$$

Hinweis zu a) und b): Es sind jeweils zwei Beweisrichtungen erforderlich!c) Seien $q, r \in \mathbb{Z}$ beliebige ganze Zahlen, für die $a = qb + r$ gilt. Beweise:

$$T(a) \cap T(b) = T(b) \cap T(r).$$

Hinweis zu c): Um die Gleichheit $M = N$ zweier Mengen M und N zu beweisen, muss man zeigen, dass jedes Element aus M auch in N liegt und dass umgekehrt auch jedes Element aus N in M liegt. (7)

27. Aufgabe: a) Berechne $\text{ggT}(54\,312, 128\,472)$ mit Hilfe des Euklidischen Algorithmus. Die Zwischenrechnungen sind anzugeben!

b) Seien $a = -731$ und $b = 1071$. Bestimme mit Hilfe des erweiterten Euklidischen Algorithmus ganze Zahlen x und y mit $\text{ggT}(a, b) = xa + yb$. Die Zwischenrechnungen sind anzugeben! (6)