11. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)

Abgabe: Freitag 24.6.2011, 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!**

28. Aufgabe: Seien $a, b \in \mathbb{Z}$. Beweise in der angegebenen Reihenfolge:

a) $a \mid b \implies a \mid (kb)$ für alle $k \in \mathbb{Z}$.

b) $a \mid b \iff a \mid |b|$ (d.h. a ist ein Teiler von $|b|$).

c) $T(a) = T(|a|)$.

d) Leite mit Hilfe von **c)** her: Sind a und b nicht beide 0, so gilt $\operatorname{ggT}(a, b) = \operatorname{ggT}(|a|, |b|)$.

(4)

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

a) $a \bmod n = b \bmod n \implies \operatorname{ggT}(a, n) = \operatorname{ggT}(b, n)$.

b) $a^m \bmod n = 1 \implies \operatorname{ggT}(a, n) = 1$ für alle $m \in \mathbb{N}$.

c) $ab \bmod n = 1$ und $b \bmod n = c \bmod n \implies ac \bmod n = 1$. (4)

30. Aufgabe: Untersuche, ob $a = 86\,275$ ein Inverses modulo $n = 624$ besitzt. Wenn ja, berechne $c \in \mathcal{R}_n$ mit $ac \bmod n = 1$.

Hinweis: Diese Aufgabe läßt sich zum einen mit Satz (8.10) bearbeiten, der allerdings erst am Montag in der Vorlesung besprochen wird. Zum anderen ist aber der Spezialfall $n = 26$ schon im Beweis von (4.6a) behandelt worden. Die Überlegungen dort lassen sich nun leicht auf diese Aufgabe übertragen. (6)