10. Aufgabenblatt „Kryptographie" (SS 2011)

Lösungsvorschläge

(25) a) $a|b$ bedeutet: es ex. $k \in \mathbb{Z}$ mit $b = a \cdot k$
$a|c$ bedeutet: es ex. $l \in \mathbb{Z}$ mit $c = a \cdot l$ } nach (8.1)

$\Rightarrow \quad xb + yc = x(ak) + y(al) = a(xk) + a(yl) = a(\underbrace{xk + yl}_{\in \mathbb{Z}})$

d.h. $a \mid (xb + yc)$

b) Setzt man in a) $x = y = 1$, so folgt $a \mid (b + c)$
Setzt man in a) $x = 2$ und $y = -1$, so folgt $a \mid (2b - c)$

---

(26) a) „$\Rightarrow$"

Zu zeigen: ein beliebiges Element $t \in T(a)$ gehört auch zu $T(b)$
$t \in T(a) \Rightarrow t \mid a$. $a \mid b$ nach Vor. $\Rightarrow t \mid b$ (Transitivität von $|$)
$\Rightarrow t \in T(b)$.

„$\Leftarrow$" Es gilt $a \in T(a)$. $T(a) \subseteq T(b)$ nach Vor. $\Rightarrow a \in T(b)$, d.h. $a \mid b$

b) „$\Rightarrow$" $a \mid b \overset{a)}{\Rightarrow} T(a) \subseteq T(b)$ $\quad (\Rightarrow T(a) \cap T(b) = T(a))$

$ggT(a,b) = \max(T(a) \cap T(b)) \overset{(*)}{=} \max(T(a)) = |a|$

„$\Leftarrow$" $ggT(a,b) = |a| \Rightarrow |a| \mid b \Rightarrow a \mid b$.

Bem: Die Vor. $a \neq 0$ wird benötigt, damit $ggT(a,b)$ überhaupt definiert ist.

c) „$\subseteq$" Sei $t \in T(a) \cap T(b)$ bel. zz: $t \in T(b) \cap T(r)$

$t \in T(a) \cap T(b) \Rightarrow t \in T(b)$
noch zz: $t \in T(r)$ Nach Vor. $r = a - qb$
$t \mid a$ und $t \mid b \Rightarrow t \mid \underbrace{a - qb}_{=r}$ (nach Aufg. 25a) mit $x = 1, y = -q) \Rightarrow t \mid r$
Also $t \in T(b)$ und $t \in T(r)$, d.h. $t \in T(b) \cap T(r)$

„$\supseteq$" Sei $t \in T(b) \cap T(r)$ bel. zz: $t \in T(a) \cap T(b)$

$t \in T(b) \cap T(r) \Rightarrow t \in T(b)$
noch zz: $t \in T(a)$ Nach Vor. $a = qb + r$
$t \mid b$ und $t \mid r \Rightarrow t \mid \underbrace{qb + r}_{=a}$ (nach Aufg 25a) mit $x = q, y = 1) \Rightarrow t \mid a$
Also $t \in T(b)$ und $t \in T(a)$, d.h. $t \in T(a) \cap T(b)$