MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Dr. W. Buchholz

Übungen zur Vorlesung "Diskrete Strukturen"

Aufgabe 21

(a) Seien $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ $(n \geq 2)$ und seien $q_2, s_2, \ldots, q_n, s_n \in \mathbb{Z}$ mit $a_i = q_i a_1 + s_i$ für $i = 2, ..., n$.
Man zeige: $\mathsf{ggT}(a_1, \ldots, a_n) = \mathsf{ggT}(a_1, s_2, ..., s_n)$.

(b) Man beweise für $a, b, c \in \mathbb{N}_1$: $\mathsf{ggT}(ac, bc) = \mathsf{ggT}(a, b) \cdot c$

(c) Man beweise für $a, b, c \in \mathbb{N}_1$: $\mathsf{ggT}(a, b) = 1 \;\&\; c|ab \implies \mathsf{ggT}(a, c) \cdot \mathsf{ggT}(b, c) = c$.

Aufgabe 22

(a) Sei M die disjunkte Vereinigung der Mengen $M_i \neq \emptyset$ $(i \in I)$,
d.h. $M = \bigcup_{i \in I} M_i = \{x : \exists i \in I(x \in M_i)\}$ und $\forall i, j \in I(i \neq j \Rightarrow M_i \cap M_j = \emptyset)$.
Wir definieren eine binäre Relation $\sim$ auf M durch: $x \sim y \;:\Leftrightarrow\; \exists i \in I(x, y \in M_i)$.
Man zeige: $\sim$ ist eine Äquivalenzrelation auf M und $[x]_\sim = M_i$ für alle $x \in M_i$, $i \in I$.

(b) Sei $U \subseteq \mathbb{Z}$ und $\sim_U$ die binäre Relation $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x - y \in U\}$. Man beweise:
$\sim_U$ ist Äquivalenzrelation auf $\mathbb{Z} \iff 0 \in U \;\&\; \forall x, y \in U(x - y \in U)$.

(c) Für $a, b \in \mathbb{Z}_m := \{0, ..., m-1\}$ sei $a \oplus b := \mathbf{r}_m(a + b)$, $a \ominus b := \mathbf{r}_m(a - b)$, $a \otimes b := \mathbf{r}_m(ab)$.
Man zeige, daß für alle $a, b, c \in \mathbb{Z}_m$ gilt:
$a \oplus (b \ominus a) = b$, $a \ominus (b \ominus c) = (a \ominus b) \oplus c$, $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$.

Aufgabe 23

Auf der Menge $M := \mathbb{Z} \times \mathbb{N}_1$ definieren wir binäre Relationen $\sim$ und $\prec$ durch:
$(a, n) \sim (b, m) \;:\Leftrightarrow\; a{\cdot}m = b{\cdot}n$ und $(a, n) \prec (b, m) \;:\Leftrightarrow\; a{\cdot}m < b{\cdot}n$.

Man beweise:

(a) $\sim$ ist Äquivalenzrelation auf M.

(b) $(a, n) \prec (b, m) \;\&\; (a, n) \sim (a', n') \;\&\; (b, m) \sim (b', m') \implies (a', n') \prec (b', m')$.

Aufgabe 24

(a) Sei $m \geq 2$ und $y, \tilde{y}, k, \tilde{k}, x, \tilde{x}, i \in \mathbb{N}$. Man beweise:
$\tilde{y} = \mathbf{r}_m(y^2) \;\&\; k = 2\tilde{k} + i \;\&\; \tilde{x} = \mathbf{r}_m(y^i x) \implies y^k \cdot x \equiv_m \tilde{y}^{\tilde{k}} \cdot \tilde{x}$.

(b) Man beschreibe einen Algorithmus zur Berechnung von $\mathbf{r}_m(a^b)$ für $a, b, m \in \mathbb{N}$, $m \geq 2$.
[Hinweis: Teil (a) der Aufgabe]

(c) Mit Hilfe von (a) bzw. (b) bestimme man die letzten 3 Stellen von 79^{178}.

Abgabe: Dienstag, 9. 6. 2009, 18 Uhr (Übungskasten)