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

SoSe 2009
Blatt 7

Übungen zur Vorlesung "Diskrete Strukturen"

Aufgabe 25

Sei $m = p \cdot q$ mit $p = 13$ und $q = 17$. Dann ist $\varphi(m) = (p-1)\cdot(q-1) = 192$.

Die Verschlüsselung der Nachricht $n \in \{0, ..., 221\}$ mit dem (öffentlichen) Schlüssel $(m, 29)$ ergebe 172.

Man bestimme n.

Aufgabe 26

Man löse die folgenden beiden Kongruenzsysteme

(a) $x \equiv 2 \bmod 7,\ \ x \equiv 4 \bmod 8,\ \ x \equiv 1 \bmod 9,$

(b) $x \equiv 5 \bmod 7,\ \ x \equiv 1 \bmod 8,\ \ x \equiv 3 \bmod 9.$

Aufgabe 27

(a) Sei $m = m_1 \cdot \ldots \cdot m_k$ mit paarweise teilerfremden $m_1, ..., m_k \in \mathbb{N}_1$.
Seien $a_1, \ldots, a_k \in \mathbb{N}_1$ mit $\mathsf{ggT}(a_i, m_i) = 1$ für $i = 1, ..., k$.
Man beweise: Es gibt ein $c \in \mathbb{N}$, so daß $[c]_m = \{x \in \mathbb{Z} : a_i x \equiv b_i \bmod m_i \text{ für } i = 1, ..., k\}$.

(b) Man bestimme die Menge aller $x \in \mathbb{Z}$, für die gilt:
$2x \equiv 3 \bmod 7\ \ \&\ \ 3x \equiv 6 \bmod 8\ \ \&\ \ 4x \equiv 3 \bmod 9.$

Aufgabe 28

Man beweise:

(a) Für $m = 561 = 3 \cdot 11 \cdot 17$ und beliebiges $a \in \mathbb{Z}$ gilt $a^m \equiv a \bmod m$.

(b) Sind $b_0, ..., b_k \in \mathbb{N}$ und ist $s = \max\{k, b_0, ..., b_k\} + 1$, sowie $m_i = s! \cdot (i+1) + 1$ für $i = 0, ..., k$, so sind die Zahlen $m_0, \ldots, m_k$ paarweise teilerfremd.

Abgabe: Dienstag, 16. 6. 2009, 18 Uhr (Übungskasten)