Fachbereich Informatik
Dr. Marco Hülsmann
Sigrid Weil

Uebung 5

Aufgabe 5.1
Satz 1.3 besagt, daß die Äquivalenzklassen $A_i,\ i \in \mathbb{N}$, eine Partition auf dem zugrundegelegten Universum $\mathcal{U}$ bilden. Wir hatten in der Vorlesung bereits gezeigt, daß die Äquivalenzklassen paarweise disjunkt sind. Zeigen Sie noch:

$$\bigcup_{i \in \mathbb{N}} A_i = \mathcal{U}$$

Aufgabe 5.2
Betrachten Sie für $m \in \mathbb{N}$ die Äquivalenzrelation

$$\equiv_m : \mathbb{Z} \to \mathbb{Z}, \quad \text{definiert durch} \quad a \equiv_m b :\Leftrightarrow\ m \ \mid a - b$$

a) Geben Sie die folgenden Äquivalenzklassen an: $[1]_{\equiv_4},\ [3]_{\equiv_7},\ [2]_{\equiv_8}$.

b) Geben Sie ein Repräsentantensystem für $m = 4$ an. Verifizieren Sie, dass die Äquivalenzklassen für $m = 4$ eine Partition auf $\mathbb{Z}$ bilden!

c) Es seien $r_1, r_2 \in \mathbb{N}_0$. Es gelte $a \in [r_1]_{\equiv_m}$ und $b \in [r_2]_{\equiv_m}$.
Zeigen Sie, daß $a + b \in [r_1 + r_2]_{\equiv_m}$ und $ab \in [r_1 r_2]_{\equiv_m}$.

Aufgabe 5.3
a) Es ist 10 Uhr vormittags am Mittwoch, und Sie haben in 50 Stunden Mathe-Übung und in 70 Stunden ein Programmierpraktikum. Wann finden die Termine statt? Verwenden Sie hierzu die Modulo-Rechnung!

b) Berechnen Sie $54^{16} \mod 55$, $3^{333} \mod 26$ und $2^{271} \mod 19$.

Aufgabe 5.4
a) Zeigen Sie, daß für $k, m \in \mathbb{N}$ gilt:

$$\left(2^k - 1\right) \sum_{j=0}^{m-1} 2^{jk} = 2^{mk} - 1$$

b) Zeigen Sie, daß Mersenne-Primzahlen der Form $2^n - 1,\ n \in \mathbb{N}$, nur dann Primzahlen sein können, wenn $n \in \mathbb{P}$.

Aufgabe 5.5
a) Zeigen Sie mithilfe des Euklidischen Algorithmus, dass $\mathrm{ggT}(28, 15) = 1$, und bestimmen Sie das modulare Inverse von 15 modulo 28 mithilfe des erweiterten Euklidischen Algorithmus.

b) Zeigen Sie, dass $\mathrm{ggT}(160, 13) = 1$.
Lösen Sie die „modulare Gleichung“ $13x \equiv_{160} 1$.