Aufgabe 55. Wir betrachten die Funktionen

$$\delta : \mathbb{N} \to \mathbb{N} \qquad \sigma : \mathbb{N} \to \mathbb{N}$$
$$n \mapsto \sum_{\substack{1 \le d < n \\ d \mid n}} d \qquad n \mapsto \sum_{\substack{1 \le d \le n \\ d \mid n}} d$$

Eine Zahl heißt **perfekt** wenn $\delta(n) = n$. Zeige:

(a) Wenn $\mathrm{ggT}(a, b) = 1$, dann ist $\sigma(a \cdot b) = \sigma(a)\sigma(b)$.
(b) Wenn $p = 2^k - 1 \in \mathbb{P}$, dann ist $n = 2^{k-1}(2^k - 1)$ perfekt.

Aufgabe 56. Berechne ohne Hilfsmittel in $\mathbb{Z}_{50}$

$$(a) \quad [3]^{2^{31}} \qquad (b) \quad [2]^{3^{31}}$$

Aufgabe 57. Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$g = 3 \qquad p = 113$$
$$m = 54 \qquad n = 42$$

Bestimme wenn möglich die geheimen Parameter a, b und den Schlüssel r!

Aufgabe 58. Gegeben sei der RSA-Schlüssel $m = 2701$, $r = 1085$.

(a) Verschlüssle die Botschaft $(3, 4, 5)$.
(b) Bestimme den inversen Schlüssel s und entschlüssle die Botschaft $(2374, 601, 356)$.

Hinweis: Für einen Teil der Berechnungen ist wahrscheinlich ein Computer erforderlich.

Aufgabe 59. Sei $D = \{3k + 1 \mid k \in \mathbb{N}_0\}$.

(a) Zeige, daß D mit der üblichen Multiplikation ein Monoid (=Halbgruppe mit 1) ist.
(b) Eine Zahl $a \in D$ mit $d > 1$ heißt **irreduzibel**, wenn sie nicht in der Form $a = b \cdot c$, $b, c \in D \setminus \{1\}$ geschrieben werden kann. Bestimme alle irreduziblen Elemente ≤ 100.
(c) Zeige, daß jedes Element $a \in D$ als Produkt von irreduziblen Elementen geschrieben werden kann.
(d) Zeige, daß die Zerlegung in irreduzible Elemente nicht eindeutig sein muß.
(e) Ein Element $p \in D$ heißt **prim** wenn gilt:

$$p \mid ab \implies p \mid a \vee p \mid b.$$

Zeige, daß 4 nicht prim ist.