**Aufgabe 45.**
(a) Berechne $\varphi(2025)$ und $\varphi(10125000)$.
(b) Ermittle ohne Taschenrechner Zahlen $a, b$, sodaß

$$(25^4)^{2025} \equiv a \mod 77 \qquad 31^{(3^{2025})} \equiv b \mod 77$$

**Aufgabe 46.**
(a) Berechne die Eulersche Funktion $\varphi(m)$ für die Zahl $m = 6885$.
(b) Zeige, daß $a^{\varphi(81)+1} \not\equiv a \mod 81$ genau dann gilt, wenn $\mathrm{ggT}(a, 81) \in \{3, 9, 27\}$.
(c) Zeige, daß $a^{\varphi(6885)+1} \not\equiv a \mod 6885$ genau dann gilt, wenn $\mathrm{ggT}(a, 81) \in \{3, 9, 27\}$.
*Hinweis*: Chinesischer Restsatz!

**Aufgabe 47.**
(a) Zeige, daß für jeden Teiler $d$ von $n$ gilt

$$\varphi(n/d) = |\{a \mid 1 \leqslant a \leqslant n \wedge \mathrm{ggT}(a, n) = d\}|$$

(b) Zeige, daß

$$\sum_{d|n} \varphi(d) = n$$

**Aufgabe 48.**
(a) Beschreibe und berechne einen Diffie-Hellman-Merkle-Schlüsselaustausch mit den Parametern $p = 31$, $g = 3$, $a = 13$, $b = 11$.
(b) Zu einem Diffie-Hellman-Merkle-Schlüsselaustausch seien folgende Daten bekannt:

$$g = 8 \qquad p = 29$$
$$g^a = 24 \qquad g^b = 18$$

Bestimme die geheimen Parameter $a$, $b$ und den Schlüssel $r = g^{ab}$.

**Aufgabe 49.** 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 50.** Das folgende Beispiel illustriert, daß die Wahl kleiner Schlüssel die Sicherheit des RSA-Verfahrens verringert.
Agent Krasnov schickt dreimal die gleiche Botschaft an seine Kumpel Bibi, Eli und Vladi, die ihm vorher die öffentlichen Schlüssel $(m_1 = 1003, r_1 = 3)$, $(m_2 = 1081, r_2 = 3)$ und $(m_3 = 1189, r_3 = 3)$ bekanntgegeben haben. Die drei verschlüsselten Botschaften sind jeweils $y_1 = (205, 444, 16)$, $y_2 = (664, 1024, 19)$ und $y_3 = (1074, 40, 334)$.
Entschlüssle die Botschaft, ohne die Primfaktorzerlegung der Schlüssel $m_i$ durchzuführen (Computer oder Taschenrechner für Zwischenrechnungen ist zugelassen).