Aufgabe 28. Berechne $\varphi(2023)$ und $\varphi(10125000)$.

Aufgabe 29. Ermittle ohne Taschenrechner Zahlen a, b, c , sodaß

$$(25^4)^{2023} \equiv a \pmod{77} \quad (25^{(4^{2023})}) \equiv b \pmod{77} \quad 14^{(2023^{2023})} \equiv c \pmod{60}.$$

Hinweis: Sollte der Satz von Euler-Fermat nicht direkt anwendbar sein, den chinesischen Restsatz wie in Aufgabe 24 anwenden!

Aufgabe 30. (a) Berechne die Eulersche Funktion $\varphi(m)$ für die Zahl $m = 6885$.

(b) Zeige, daß $a^{\varphi(81)+1} \not\equiv a \pmod{81}$ genau dann gilt, wenn $\text{ggT}(a, 81) \in \{3, 9, 27\}$.

(c) Zeige, daß $a^{\varphi(6885)+1} \not\equiv a \pmod{6885}$ genau dann gilt, wenn $\text{ggT}(a, 81) \in \{3, 9, 27\}$.

Hinweis: Chinesischer Restsatz!

(d) Überprüfe diese Tatsachen am Computer für $a \in \{1, 2, \dots, 6885\}$.

Aufgabe 31 (Asmuth-Bloom-Verfahren). Der chinesische Restsatz kann verwendet werden, um ein Geheimnis auf n Personen so aufzuteilen, daß mindestens k Personen nötig sind, um es zu lösen. Hier ist $n = 3$ und $k = 2$.

- Wähle positive teilerfremde Zahlen $m_0 < m_1 < m_2 < m_3$, sodaß $m_0 m_3 < m_1 m_2$.
- Das Geheimnis ist eine Zahl $0 \leq r < m_0$. Wähle eine zufällige natürliche Zahl t , sodass $a = r + t m_0 < m_1 m_2$.
- Berechne $c_i = a \pmod{m_i}$ für $i = 1, 2, 3$.
- Die Zahl m_0 ist öffentlich bekannt, das Geheimnis wird wie folgt aufgeteilt: Alice erhält (c_1, m_1) , Bob erhält (c_2, m_2) und Charlie erhält (c_3, m_3) .
- Um die geheime Zahl r wiederherzustellen, müssen mindestens zwei, zum Beispiel Alice und Bob, gemeinsam das Gleichungssystem

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned} \quad \text{lösen und können dann } r = x \pmod{m_0} \text{ berechnen.}$$

- (a) Begründe, warum am Ende $x = r \pmod{m_0}$ ist. Worauf ist dabei zu achten?
- (b) Seien konkret $m_0 = 5$, $m_1 = 7$, $m_2 = 9$, $m_3 = 11$. Angenommen, Alice erhält das Paar $(0, 7)$ und Bob erhält das Paar $(6, 9)$. Wie lautet das Geheimnis r ? Kann t rekonstruiert werden? Welches Paar (c_3, m_3) hat Charlie erhalten?
- (c) Angenommen, Charlie erhält das Paar $(8, 11)$ und die Information, daß $0 \leq t \leq 5$ ist (er kennt m_1 und m_2 nicht). Welche möglichen Werte hat r ?

Aufgabe 32. (a) Beschreibe und berechne einen Diffie-Hellman-Schlüsselaustausch mit den Parametern $p = 31$, $g = 7$, $a = 13$, $b = 11$.

(b) Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$\begin{array}{ll} g = 8 & p = 29 \\ m = 10 & n = 16 \end{array}$$

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