Aufgabe 34. Zeige, dass die folgende Aussage wahr ist:

$$a \equiv b \mod m \text{ und } a \equiv b \mod n \implies a \equiv b \mod k \quad \text{für} \quad k = \mathrm{kgV}(m_1, m_2)\,.$$

Ist insbesondere $\mathrm{ggT}(m_1, m_2) = 1$, dann gilt also $a \equiv b\ (m_1 m_2)$.
Folgere daraus, daß die Menge aller Lösungen eines Kongruenzgleichungssystems $x \equiv c_i \mod m_i$, $i = 1, 2, \ldots, k$ und $\mathrm{ggT}(m_i, m_j) = 1$, gegeben ist durch $\{x_0 + km \mid k \in \mathbb{Z}\}$, wobei $m = m_1 m_2 \cdots m_k$.

Aufgabe 35. Welche der folgenden Gleichungssystems sind lösbar? Wenn ja, dann bestimme diese. Ist der chinesische Restsatz anwendbar?

$$(a)\quad \begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 2 \mod 9 \\ x &\equiv 1 \mod 10 \end{aligned} \qquad (b)\quad \begin{aligned} x &\equiv 1 \mod 5 \\ x &\equiv 3 \mod 9 \\ x &\equiv 2 \mod 10 \end{aligned}$$

Aufgabe 36.

(a) Berechne $\varphi(10!) = \varphi(2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10)$.
(b) Berechne $\varphi(5186)$, $\varphi(5187)$, $\varphi(5188)$.
(c) Finde alle $n \in \mathbb{N}$ mit $\varphi(n) = 1$.
(d) Finde alle $n \in \mathbb{N}$ mit $\varphi(n) = 2$.
(e) Finde alle $n \in \mathbb{N}$ mit $\varphi(n) = 3$.

Hinweis: Wenn $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, dann ist jedes $\varphi(p_i^{k_i})$ ein Teiler von $\varphi(n)$.

Aufgabe 37. Berechne (ohne Taschenrechner), mit Hilfe des Satzes von Euler-Fermat die Potenz

$$2^{(2^{32})} \mod 11\,.$$

Aufgabe 38. Berechne mit dem Satz von Euler-Fermat (ohne Taschenrechner) in $\mathbb{Z}_{60}$

$$[14]^{(2^{32})}$$

Hinweis: Der Satz von Euler-Fermat ist nicht sofort anwendbar (warum?). Man kann aber wie folgt vorgehen: Zerlege $60 = 2^2 \cdot 3 \cdot 5$. Bestimme $[14]^{(2^{32})} \mod 4$, $[14]^{(2^{32})} \mod 3$, $[14]^{(2^{32})} \mod 5$, und verwende den chinesischen Restsatz, um daraus $14^{(2^{32})} \mod 60$ zu bestimmen.

Aufgabe 39. Um Frequenzanalyse zu erschweren, empfiehlt es sich, Buchstabengruppen zu verschlüsseln, z.B. paarweise. Dazu numeriert man die Buchstaben A-Z von 0 bis 25 durch und faßt diese Zahlen als Ziffern in einem Zahlensystem zur Basis 26 auf. Das heißt, unser "Alphabet" besteht aus $26 \cdot 26 = 676$ Buchstabenpaaren:

$$\begin{array}{llll} AA \mathrel{\hat{=}} 0, & AB \mathrel{\hat{=}} 1, & AC \mathrel{\hat{=}} 2, & \ldots \quad AZ \mathrel{\hat{=}} 25 \\ BA \mathrel{\hat{=}} 26, & BB \mathrel{\hat{=}} 27, & BC \mathrel{\hat{=}} 28, & \ldots \quad BZ \mathrel{\hat{=}} 51 \\ CA \mathrel{\hat{=}} 52, & CB \mathrel{\hat{=}} 53, & CC \mathrel{\hat{=}} 54, & \ldots \quad CZ \mathrel{\hat{=}} 87 \\ \vdots & & & \\ ZA \mathrel{\hat{=}} 650, & ZB \mathrel{\hat{=}} 651, & ZC \mathrel{\hat{=}} 652 & \ldots \quad ZZ \mathrel{\hat{=}} 675, \end{array}$$

d.h. dem Buchstabenpaar $b_i b_j$ entspricht die Zahl $i \cdot 26 + j$
Mit diesen Zahlen kann dann weitergerechnet werden, indem z.B. ein Caesar-Schlüssel modulo 676 addiert wird.

(a) Stelle das Wort OKAY mit diesem Zahlencode dar, addiere dazu den Caesar-Schlüssel 84 und wandle den erhaltenen Code in ein verschlüsseltes Wort um.
(b) Entschlüssle das Wort EURSHX mit dem inversen Schlüssel.