1) a) Berechnen Sie 3^{12} mit dem Verfahren des schnellen Potenzierens (Satz **??**). Wie viele Multiplikationen benötigt man?

   b) Die Operation x^w, welche x zur w-ten Potenz berechnet, wobei w als Bit-String gegeben ist, ist wie folgt induktiv definiert:

$$\begin{aligned} x^{\epsilon} &= 1 \\ x^{w0} &= (x^w)^2 \\ x^{w1} &= (x^w)^2 * x \end{aligned}$$

   Beispiel: $3^{101} = (3^{10})^2 * 3 = ((3^1)^2)^2 * 3 = (((3^{\epsilon})^2 * 3)^2)^2 * 3 = (3^2)^2 * 3 = 9^2 * 3 = 243$. Berechnen Sie 3^{1100}. Wie viele Multiplikationen benötigt man? Erklären Sie sowohl die Übereinstimmung mit, als auch den Unterschied zu a).

   c) Zeigen Sie, dass für alle natürlichen Zahlen x und Bit-Strings w gilt, dass $x^w = x^{(w)_2}$, wobei auf der linken Seite die Potenzierung mit einem Bit-String gemeint ist und auf der rechten Seite die Potenzierung mit einer natürlichen Zahl. $(w)_2$ stellt dabei die natürliche Zahl dar, welche dem Bit-String w entspricht.

   Hinweis: Geben Sie zuerst eine Induktive Definition von $(\_)_2$ an (siehe Aufgabe 5 von Blatt 3).

2) Gegeben seien $a = 1173$ und $b = 816$. Berechnen Sie den größten gemeinsamen Teiler von a und b.

   Hinweis: Sie haben richtig erkannt, dass 17 ein Teiler von 816 ist. Verwenden Sie diese Information, um die Berechnung des ggT zu vereinfachen, und wenden Sie danach den euklidischen Algorithmus für ganze Zahlen an.

3) Berechnen Sie $\text{ggT}(-75, 42)$ mit Hilfe des erweiterten euklidischen Algorithmus. Berechnen Sie des weiteren $\text{kgV}(-75, 42)$.

4) Sei p eine Primzahl. Beweisen Sie entlang der folgenden drei Schritte, dass $(p-1)! \equiv -1 \ (mod\ p)$ gilt.

   a) Für jede ganze Zahl a mit $1 \leq a < p$, gibt eine ganze Zahl b (das inverse Element von a genannt), so dass $a \cdot b \equiv 1 \ (mod\ p)$ gilt.

   Hinweis: Verwenden Sie das Lemma von Bézout (im Skriptum ist es der Satz vom erweiterten euklidischen Algorithmus).

   b) Zeigen Sie, dass für jede ganze Zahl a, $1 \leq a < p$, Folgendes gilt:

   - Das inverse Element von a ist modulo p einzig. Genauer, $\forall b, c \in \mathbb{Z}, a \cdot b \equiv 1 \ (mod\ p) \wedge a \cdot c \equiv 1 \ (mod\ p) \implies b \equiv c \ (mod\ p)$.
   - Wenn a sein eigenes Inverses modulo p ist, dann ist a kongruent entweder mit $1 \ (mod\ p)$ oder mit $-1 \equiv (p-1) \ (mod\ p)$.

c) $(p-1)! \equiv -1 \ (mod\ p)$.
Hinweis: Ordnen Sie jedem Faktor von $(p-1)!$ sein inverses Element zu. Erklären Sie, warum dadurch jedem Element a mit $1 < a < p-1$, ein einziges, von a verschiedenes Element zugeordnet wird. Z.B. $6! = 1{\cdot}2{\cdot}3{\cdot}4{\cdot}5{\cdot}6 = 1{\cdot}(2{\cdot}4){\cdot}(3{\cdot}5){\cdot}6 \equiv 1{\cdot}1{\cdot}1{\cdot}6 \equiv -1 \ (mod\ 7)$.

5) Der chinesische General Han Xin, welcher circa um 200 v. Chr. lebte, wird gerne mit dem chinesischem Restsatz assoziiert. Die folgende (möglicherweise nicht ganz wahre) Geschichte handelt um seine 1500 Mann starke Armee. Nach einem Gefecht wollte Han Xin genau wissen, wie viele Soldaten noch übrig waren. Der General wusste, dass zwischen 400 und 500 der Soldaten im Gefecht gefallen waren.

Wenn sich die Soldaten in Dreierreihen aufstellten, blieben in der letzen Reihe 2 Soldaten übrig. Wenn die Soldaten in Fünferreihen aufgestellt waren, so blieben 4 übrig und bei 7 Soldaten pro Reihe blieben 4 übrig.

Han Xin wusste sofort wie viele der 1500 Soldaten noch am Leben waren.

Wie viele Soldaten waren es?