1) *Lösung.* a) Es gilt $(1100)_2 = 12$, somit benötigt der Algorithmus des schnellen Potenzierens 3 Schleifendurchläufe, die jeweils zumindest einer Quadrierung (= Multiplikation) entsprechen. Außerdem steht an der zweiten Position 1, also kommt im ersten Durchlauf noch eine Multiplikation hinzu. Insgesamt sind es also 4 Multiplikationen. Anschaulich gilt $3^{12} = ((3^2 * 3)^2)^2 = 531441$.

b)

$$\begin{aligned} 3^{1100} &= (3^{110})^2 \\ &= ((3^{11})^2)^2 \\ &= (((3^1)^2 * 3)^2)^2 \\ &= ((((3^\epsilon)^2 * 3)^2 * 3)^2)^2 \\ &= (((1^2 * 3)^2 * 3)^2)^2 \\ &= ((9 * 3)^2)^2 \\ &= 729^2 \\ &= 531441 \end{aligned}$$

In der fünften Zeile sehen wir 4 Quadrierungen und 2 Multiplikationen, daher haben wir insgesamt 6 Multiplikationen. Im Allgemeinen entspricht die Anzahl der Quadrierungen der Länge des Wortes und die Anzahl der Multiplikationen der Anzahl der enthaltenen 1-Bits.

Der Unterschied zu Antwort a) sind 2 Multiplikationen. Da wir einen Basisfall für das Leere Wort ϵ haben, haben wir für positive Exponenten im Allgemeinen jeweils eine Quadrierung und eine Multiplikation mehr.

c) Wir zeigen, dass für alle Bit-Strings w and für alle natürlichen Zahlen x gilt, $x^w = x^{(w)_2}$, wobei $(\_)_2$ induktiv definiert ist:

$$\begin{aligned} (\epsilon)_2 &= 0 \\ (w0)_2 &= (w)_2 * 2 \\ (w1)_2 &= (w)_2 * 2 + 1 \end{aligned}$$

Im Basisfall $x^\epsilon = 1 = x^0 = x^{(\epsilon)_2}$. Im Schrittfall $x^{w0} = (x^w)^2 =_{\mathsf{IH}} (x^{(w)_2})^2 = x^{(w)_2 * 2} = x^{(w0)_2}$, und $x^{w1} = (x^w)^2 * x =_{\mathsf{IH}} (x^{(w)_2})^2 * x = x^{(w)_2 * 2 + 1} = x^{(w1)_2}$.

□

4) *Lösung.* a) Observe that a and p are coprimes. Using Bézout's identity, we get $a \cdot b + k \cdot p = 1$ for some integers b and k. This gives $(a \cdot b + k \cdot p) \equiv 1 \ (mod\ p)$. Since $k \cdot p \equiv 0 \ (mod\ p)$, we have $a \cdot b \equiv 1 \ (mod\ p)$.

b)
- Given $a \cdot b \equiv 1 \ (mod\ p)$ and $a \cdot c \equiv 1 \ (mod\ p)$, we have $c \cdot a \cdot b \equiv c \ (mod\ p)$ and $a \cdot c \cdot b \equiv b \ (mod\ p)$. Therefore $c \equiv b \ (mod\ p)$.

- If a is the inverse of itself, then it must be either $a \equiv 1 \ (mod\ p)$ or $a \equiv -1 \equiv (p-1) \ (mod\ p)$:

$$\begin{aligned} a^2 &\equiv 1 \ (mod\ p) \\ a^2 - 1 &\equiv 0 \ (mod\ p) \\ (a-1) \cdot (a+1) &\equiv 0 \ (mod\ p). \end{aligned}$$

  Any term apart from 1 and $(p-1)$ in $\mathbb{Z}/p$ has an inverse different from itself.

c) We now pair off each term leaving 1 and $(p-1)$ in the product $(p-1)!$ with their unique inverses in $\mathbb{Z}/p$, and therefore obtain $(p-1)! \equiv 1 \cdot (1 \cdot \ldots \cdot 1) \cdot (p-1) \equiv (p-1) \equiv -1 \ (mod\ p)$.

□

5) *Lösung.* Gegeben ist das folgende System von Kongruenzen:

$$\begin{aligned} x &\equiv_3 2 \\ x &\equiv_5 4 \\ x &\equiv_7 4 \end{aligned}$$

Wir lösen die ersten beiden Kongruenzen mit Hilfe des Chinesischen Restsatzes:

$$\begin{aligned} x &\equiv_{3\cdot 5} 5 \cdot 2 \cdot v + 3 \cdot 4 \cdot u \\ u \cdot 3 + v \cdot 5 &= 1 = \mathrm{ggT}(3,5) \end{aligned}$$

Durch den erweiterten Euklidischen Algorithmus erhalten wir $u = 2, v = -1$.

$$x \equiv_{3\cdot 5} 14$$

Dann lösen wir das folgende System von Kongruenzen:

$$\begin{aligned} x &\equiv_7 4 \\ x &\equiv_{15} 14 \end{aligned}$$

$$\begin{aligned} x &\equiv_{7\cdot 15} 15 \cdot 4 \cdot v + 7 \cdot 14 \cdot u \\ u \cdot 7 + v \cdot 15 &= 1 = \mathrm{ggT}(7,15) \end{aligned}$$

Durch Anwendung des erweiterten Euklidischen Algorithmus erhalten wir $u = -2, v = 1$

$$x \equiv_{105} -136 \equiv_{105} 74$$

Da die Armee aus 1500 Soldaten bestand, wovon zwischen 400 und 500 fielen, ist die Anzahl der übringen Soldaten $74 + 105 \cdot 9 = 1019$. □