a)

alle Erzeuger der Gruppe $\mathbb{Z}_{11}^*$

$\mathbb{Z}_{11}^* = \{0,1,2,3,4,5,6,7,8,9,10\}$

ggT(0,11) = 0
daher kann man sich Ord(0) sparen

neutrales Element: 1

$g:1 \Rightarrow \quad g^1 = 1$

$g:2 \Rightarrow \quad g^1 = 2$

$g^2 = g \circ g = 4 \qquad g^4 = g^3 \circ g = 5 \qquad g^6 = g^5 \circ g = 9$

$g^3 = g^2 \circ g = 8 \qquad g^5 = g^4 \circ g = 10 \qquad g^7 = g^6 \circ g = 7$

$g^8 = g^7 \circ g = 6 \qquad g^9 = g^8 \circ g = 1$

! Ord(2) ist ein Erzeuger der Gruppe $\mathbb{Z}_{11}^*$

$g:3 \Rightarrow \quad g^1 = 3$

$g^2 = g \circ g = 9 \qquad g^4 = g^3 \circ g = 4$

$g^3 = g^2 \circ g = 5 \qquad g^5 = g^4 \circ g = 1$

$g:4 \Rightarrow \quad g^1 = 4$

$g^2 = g \circ g = 5 \qquad g^4 = g^3 \circ g = 3$

$g^3 = g^2 \circ g = 9 \qquad ^5 = g^4 \circ g = 1$

$g:5 \Rightarrow \quad g^1 = 5$

$g^2 = g \circ g = 3 \qquad g^4 = g^3 \circ g = 9$

$g^3 = g^2 \circ g = 4 \qquad g^5 = g^4 \circ g = 1$

$g:6 \Rightarrow \quad g^1 = 6$

$g^2 = g \circ g = 3 \qquad g^4 = g^3 \circ g = 9 \qquad g^6 = g^5 \circ g = 5$

$g^3 = g^2 \circ g = 7 \qquad g^5 = g^4 \circ g = 10 \qquad g^7 = g^6 \circ g = 8$

$g^1 = g^7 \circ g = 4 \qquad g^9 = g^8 \circ g = 2 \qquad g^{10} = g^9 \circ g = 1$!

$g : 7 \Rightarrow$ $g^1 = 7$

$g^2 = g \circ g = 5$ $\quad g^4 = g^3 \circ g = 3$ $\quad g^6 = g^5 \circ g = 4$

$g^3 = g^2 \circ g = 2$ $\quad g^5 = g^4 \circ g = 10$ $\quad g^7 = g^6 \circ g = 6$

$g^8 = g^7 \circ g = 8$ $\quad g^9 = g^8 \circ g = 1$

$g : 8 \Rightarrow$ $g^1 = 8$

$g^2 = g \circ g = 9$ $\quad g^4 = g^3 \circ g = 4$ $\quad g^6 = g^5 \circ g = 3$

$g^3 = g^2 \circ g = 6$ $\quad g^5 = g^4 \circ g = 10$ $\quad g^7 = g^6 \circ g = 2$

$g^8 = g^7 \circ g = 5$ $\quad g^9 = g^8 \circ g = 7$ $\quad g^{10} = g^9 \circ g = 1$!

$g : 9 \Rightarrow$ $g^1 = 9$

$g^2 = g \circ g = 4$ $\quad g^4 = g^3 \circ g = 5$

$g^3 = g^2 \circ g = 3$ $\quad g^5 = g^4 \circ g = 1$

$g : 10 \Rightarrow$ $g^1 = 10$ $\quad g^2 = g \circ g = 1$

(A) Die Erzeuger der Gruppe $\mathbb{Z}_m^*$ sind 2, 6, 8.

(3)

$1234 \in \mathbb{Z}_{2000}$ $\quad 567 \in \mathbb{Z}_{2000}$ $\quad \mathbb{Z}_{2000} = \mathbb{Z}_{2^4} \times \mathbb{Z}_{5^3} = \mathbb{Z}_{16} \times \mathbb{Z}_{125}$

$f(a) = (a \bmod 16, a \bmod 125)$

$f(1234) = (1234 \bmod 16, 1234 \bmod 125) = (2, 109)$

$f(567) = (567 \bmod 16, 567 \bmod 125) = (7, 67)$

$(2, 109) + (7, 67) = (9, 51)$ $\quad \mathbb{Z}_{16} \times \mathbb{Z}_{125}$

$x \bmod 16 = 9 \bmod 16$

$x \bmod 125 = 51 \bmod 125$

Erw. Euklid:

a	b	r	s	k
125	16	1	0	–
16	13	0	1	7
13	3	1	-7	1
3	1	-1	8	4
1	0	5	-39	3

$5 \cdot 125 + (-39 \cdot 16) = 1$

$5 \cdot 125 = 1 \bmod 16$

$5 \cdot 125 \cdot 9 = 9 \bmod 16$

$-39 \cdot 16 = 1 \bmod 125$

$-39 \cdot 16 \cdot 51 = 51 \bmod 125$

$x = 5 \cdot 125 \cdot 9 + (-39 \cdot 16 \cdot 51) = -26199 \bmod 2000$

$= 1801 \bmod 2000$

Überprüfen:

$$\begin{array}{r} 1234 \\ +\ 567 \\ \hline 1801 \end{array}$$

④

a) $x \equiv 4 \mod 11,\ x \equiv 3 \mod 17,\ x \equiv 6 \mod 18.$

ggT(11,17) = 1 ggT(17,18) = 1 ggT(11,18) = 1

⇒ sind teilerfremd, deshalb existiert genau eine Lösung.

b) $n = 11 \cdot 17 \cdot 18 = 3366$

$1 = r_1 \cdot 11 + s_1 \cdot 306$ $\quad x = 4 \mod 11$

$a_1 = s_1 \cdot 306$ $\quad x_1 = 4$

$1 = r_2 \cdot 17 + s_2 \cdot 198$ $\quad x = 3 \mod 17$

$a_2 = s_2 \cdot 198$ $\quad x_2 = 3$

$1 = r_3 \cdot 18 + s_3 \cdot 187$ $\quad x = 6 \mod 18$

$a_3 = s_3 \cdot 187$ $\quad x_3 = 6$

$1 = (-139) \cdot 11 + 5 \cdot 306$

$a_1 = 5 \cdot 306 = 1530$

$1 = 35 \cdot 17 - 3 \cdot 198$

$a_2 = -3 \cdot 198 = -594$

$1 = 52 \cdot 18 - 5 \cdot 187$

$a_3 = -5 \cdot 182 = -935$

$X = a_1 \cdot x_1 + a_2 \cdot x_2 + a_3 \cdot x_3$

$= 1530 \cdot 4 - 594 \cdot 3 - 935 \cdot 6 = -7272 \mod 3366 = 2094 \mod 3366$