10.1) $n \equiv 1 \pmod 2$ (*)
$n \equiv 2 \pmod 3$
$n \equiv 1 \pmod 4$ (**)
$n \equiv 1+24 \pmod 5$ (***)

Wenn (**) erfüllt ist, dann ist auch (*) erfüllt, weshalb man (*) streichen kann. Dies ist notwendig, da alle Module teilerfremd sein müssen.

Aus (*) folgt auch, dass n ungerade sein muss. Deshalb muss der Rest aus (***) auch ungerade sein.
Somit entweder: 3 oder 1.

~~Fall 1:~~

Modul	Prod. d. R.	Bézout	Basis Lsg.
3	20	$7 \cdot 3 + (-1) \cdot 20 = 1$	$-20 = e_1$
4	15	$4 \cdot 4 + (-1) \cdot 15 = 1$	$-15 = e_2$
5	12	$5 \cdot 5 + (-2) \cdot 12 = 1$	$24 = e_3$

$y = 3 \cdot 4 \cdot 5 = 60$
Fall 1: Rest für (***) ist 1.
$x_1 = 2 \cdot e_1 + 1 \cdot e_2 + 1 \cdot e_3 = -79$
somit: $-79 + 2 \cdot y = 41$
$\mathbb{L}_1 := \{ 41 + 4 \cdot 60 : k \in \mathbb{N} \}$

Fall 2: Rest für (***) ist 3.
$x_2 = 2 \cdot e_1 + 1 \cdot e_2 + 3 \cdot e_3 = -127$

somit: $-127 + 3 \cdot 60 = 53$.
Da $53 \not\equiv 41$, ist die gesuchte Lösungsmenge L_1. Es sind also min. 41 Schüler in der Klasse. Beweis fehlt. -1,5P

2,5/4

10.2) „$\Rightarrow$": $x \equiv a \pmod{pq}$

Was ist zu zeigen?

$\Rightarrow x = a + k \cdot (pq)$ mit $k \in \mathbb{Z}$
offensichtlich gilt:
p teilt kpq und q teilt kpq.

Es folgt: $a + kpq \pmod p = a$
weshalb: $a \pmod p = a$
und: $a + kpq \pmod q = a$
weshalb: $a \pmod q = a$

„$\Leftarrow$": $x \equiv a \pmod p \wedge x \equiv a \pmod q$
$\Rightarrow x = a + k \cdot p \wedge x = a + m \cdot q$ mit $k, m \in \mathbb{N}$

d.h.: $x = a + kpmq$ weil? -0,5P
$\Rightarrow kpmq \equiv 0 \pmod{pq}$
$\Rightarrow a + kpmq \equiv a \pmod{pq}$ □

2,5/3

10.3) $x^2 \equiv 16 \pmod{77} \equiv 16 \pmod{7 \cdot 11}$

$\Leftrightarrow$: $x \equiv 4 \pmod 7 \vee x \equiv -4 \pmod 7$
$\vee\ x \equiv 4 \pmod{11} \vee x \equiv -4 \pmod{11}$

euklidischer Algo: $s \cdot a + t \cdot b = 1$
es folgt: $s = -21$, $t = 22$
$x_1 = 4 \cdot (-21) + (-4) \cdot 22 = -172$
$x_2 = -4 \cdot (-21) + (-4) \cdot 22 = -4$
$x_3 = 4 \cdot (-21) + (+4) \cdot 22 = 4$
$x_4 = -4 \cdot (-21) + (-4) \cdot 22 = 172$

$\overline{\mathbb{L}} := \{-172, -4, 4, 172\}$
$\mathbb{L} := \{\overline{\mathbb{L}} + k \cdot 77 : k \in \mathbb{Z}\}$

↑ Das ist eine Menge keine Zahl −0,5P

5,5/6

10.4) a)

j	m_j	r_j	s_j	t_j
0	/	30	1	0
1	4	7	0	1
2	3	2	1	−4
3	2	1	−3	(13)
4	/	0	/	/

13 ist das inverse Element zu 7 in $(\mathbb{Z}_{30}^{\times}, \odot_{30})$.

10.4) b)

j	m_j	r_j	s_j	t_j
0	/	41	1	0
1	3	11	0	1
2	1	8	1	-3
3	2	3	-1	4
4	1	2	3	-11
5	2	1	-4	(15)
6	/	0	/	/

15 ist das inverse Element in $(\mathbb{Z}_{41}^*, \odot_{41})$.

c) Nein, denn 15 und 12 sind nicht teilerfremd: $\exists\, a, b \in \mathbb{N}$:

$$a \cdot 12 = b \cdot 15$$

Was ist zu zeigen?

Lösbar mit: $a = 5$, $b = 4$

somit: $5 \odot_{15} 12 = 0 \notin \{1, 2, \dots, 15\}$

Diese Gruppe ist nicht abgeschlossen.

unvollständig - 0/5 P

5/6

10.5) $a \equiv b^2 \pmod p$

$$a^{\frac{p-1}{2}} = b^{2 \cdot \frac{(p-1)}{2}}$$

$$= b^{(p-1)}$$

$(p-1) = |\mathbb{Z}_p^*|$ (siehe Beweis; 4, 11: $a^{|G|} = e$)

somit: $b^{|\mathbb{Z}_p^*|} \equiv 1 \pmod p$ □

15,5/23