7.1

$$r_i = (-1)^i \cdot (-v_i \cdot r_{-1} + u_i \cdot r_0)$$

(I) $i = 1$

$$\begin{aligned} r_1 &= -(-v_1 \cdot r_{-1} + u_1 \cdot r_0) \\ r_1 &= r_{-1} - q_1 \cdot r_0 \\ r_{-1} &= r_1 + q_1 \cdot r_0 \end{aligned}$$

→ nach Voraussetzung wahr.

$i = 2$

$$\begin{aligned} r_2 &= -v_2 \cdot r_{-1} + u_2 \cdot r_0 \\ r_2 &= -q_2 \cdot r_{-1} + (q_1 q_2 + 1) \cdot r_0 \\ r_2 &= \dots \end{aligned}$$

7.2

(a)

$a = 83200; b = 26520$

$$\begin{aligned} 83200 &= 3 \cdot 26520 + 3640 \\ 26520 &= 7 \cdot 3640 + 1040 \\ 3640 &= 3 \cdot 1040 + 520 \\ 1040 &= 2 \cdot 520 \end{aligned}$$

$d := 83200 \sqcap 26520 = 520$

$$\begin{aligned} 520 &= 3640 - 3 \cdot 1040 \\ &= 3640 - 3 \cdot (26520 - 7 \cdot 3640) \\ &= 22 \cdot 3640 - 3 \cdot 26520 \\ &= 22 \cdot (83200 - 3 \cdot 26520) - 3 \cdot 26520 \\ &= 22 \cdot 83200 - 69 \cdot 26520 \end{aligned}$$

$\alpha = 22$
$\beta = -69$

(b)

$a = 20723; b = 5888$

$$\begin{aligned} 20723 &= 3 \cdot 5888 + 3059 \\ 5888 &= 1 \cdot 3059 + 2829 \\ 3059 &= 1 \cdot 2829 + 230 \\ 2829 &= 12 \cdot 230 + 69 \\ 230 &= 3 \cdot 69 + 23 \\ 69 &= 3 \cdot 23 \end{aligned}$$

$d := 20723 \sqcap 5888 = 23$

$$\begin{aligned} 23 &= 230 - 3 \cdot 69 \\ &= 230 - 3 \cdot (2829 - 12 \cdot 230) \\ &= 37 \cdot 230 - 3 \cdot 2829 \\ &= 37 \cdot (3059 - 2829) - 3 \cdot 2829 \\ &= 37 \cdot 3059 - 40 \cdot 2829 \\ &= 37 \cdot 3059 - 40 \cdot (5888 - 3059) \\ &= 77 \cdot 3059 - 40 \cdot 5888 \\ &= 77 \cdot (20723 - 3 \cdot 5888) - 40 \cdot 5888 \\ &= 77 \cdot 20723 - 271 \cdot 5888 \end{aligned}$$

$\alpha = 77$
$\beta = -271$

(c)

$a = 8959; b = 1729$

$$\begin{aligned}
8959 &= 5 \cdot 1729 + 314 \\
1729 &= 5 \cdot 314 + 159 \\
314 &= 1 \cdot 159 + 155 \\
159 &= 1 \cdot 155 + 4 \\
155 &= 38 \cdot 4 + 3 \\
4 &= 1 \cdot 3 + \underline{\underline{1}} \\
3 &= 3 \cdot 1
\end{aligned}$$

$d := 8959 \sqcap 1729 = 1$

$$\begin{aligned}
1 &= 4 - 1 \cdot \underline{3} \\
&= 4 - (\underline{155 - 38 \cdot 4}) \\
&= 39 \cdot \underline{4} - 155 \\
&= 39 \cdot (\underline{159 - 155}) - 155 \\
&= 39 \cdot 159 - 40 \cdot \underline{155} \\
&= 39 \cdot 159 - 40 \cdot (\underline{314 - 159}) \\
&= 79 \cdot \underline{159} - 40 \cdot 314 \\
&= 79 \cdot (\underline{1729 - 5 \cdot 314}) - 40 \cdot 314 \\
&= 79 \cdot 1729 - 435 \cdot \underline{314} \\
&= 79 \cdot 1729 - 435 \cdot (\underline{8959 - 5 \cdot 1729}) \\
&= 2254 \cdot 1729 - 435 \cdot 8959
\end{aligned}$$

$\alpha = -435$
$\beta = 2254$

7.3

(a)

$G = P_{14} := (\{1, 3, 5, 9, 11, 13\}, \cdot \pmod{14})$

$\cdot \pmod{14}$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

(b)

ord 1 = 1
ord 3 = 6
ord 5 = 6
ord 9 = 3
ord 11 = 3
ord 13 = 2

(c)

Untergruppen von G:

$U_1 := (\{1\}, \cdot \pmod{14})$
$U_2 := (\{1, 13\}, \cdot \pmod{14})$
$U_3 := (\{1, 9, 11\}, \cdot \pmod{14})$
$U_4 := G$

Eine zu G isomorphe Gruppe der Form $(\mathbb{Z}_n; + \pmod{n})$ muss $n = \operatorname{ord} G$ erfüllen, womit $n = 6$ ist und es damit entweder genau eine isomorphe Gruppe der o. g. Form gibt oder keine.
Eine Verknüpfungstafel der Gruppe $(\mathbb{Z}_6; + \pmod{6})$ sähe wie folgt aus:

+ (mod 6)	0	1	5	2	4	3
0	0	1	5	2	4	3
1	1	2	0	3	5	4
5	5	0	4	1	3	2
2	2	3	1	4	0	5
4	4	5	3	0	2	1
3	3	4	2	5	1	0

Diese ist, wie ersichtlich, isomorph zu G.

7.4

Anm.: Im Folgenden werden Restklassen modulo 6 angenommen.

Angenommen, es gäbe ein z^2 in folgender Form:

$$z^2 = 6 \cdot n + 2$$

damit ist

$$z^2 = [2]$$

$[z^2] = [z] \cdot [z]$ wird für die möglichen z:

$[z] = 0 \rightarrow [0]$
$[z] = 1 \rightarrow [1]$
$[z] = 2 \rightarrow [4]$
$[z] = 3 \rightarrow [3]$
$[z] = 4 \rightarrow [4]$
$[z] = 5 \rightarrow [1]$

Damit gibt es kein $[z]$, welches zu einer Lösung führt. Somit ist die Annahme falsch.

7.5

Anm.: Die Lösungen wurden z. T. mittels eines Computerprogramms, d. h. durch Ausprobieren gefunden.

(a)

$x \in \mathbb{Z}_8$
$2 \cdot x + 3 = 6 \pmod 8$
$2 \cdot x = [3]_8$

$\mathrm{L} = \varnothing$

(b)

$x \in \mathbb{Z}_{63}$
$7 \cdot x = 0 \pmod{63}$
$7 \cdot x = [0]_{63}$

$\mathrm{L} = \{[0], [9], [18], [27], [36], [45], [54]\}$

(c)

$x \in \mathbb{Z}_{1001}$
$17 \cdot x = 1 \pmod{1001}$
$17 \cdot x = [1]_{1001}$

$\mathrm{L} = [530]_{1001} = \{x \in \mathbb{Z}_{1001} \mid \exists\, k \in \mathbb{Z}: x = 1001k + 530\}$