

$$V_{n,d} := \{k \cdot d \in \mathbb{Z}_n \mid k \in \mathbb{N}_n\}$$

$$1 \leq kd \leq n$$

$\Rightarrow d$ teilt n

$$1 \leq k \leq \frac{n}{d}$$

$$|V_{n,d}| = \frac{n}{d}$$

b) Im Schnitt von V_{n,d_i} liegen alle gemeinsamen Vielfache der d_i s

$$n=30 \quad d_1=3 \quad d_2=2$$

$$\begin{array}{cc} 3 & 2 \\ 6 & 4 \\ 9 & 6 \\ \dots & \dots \end{array}$$

(kleinstes Element: $\text{kgV}(d_i)$)

$$V_{n, \text{kgV}(d_1, \dots, d_k)}$$

c) $\text{ggT}(x, n) > 1$ gdw $\exists p \in P \quad p|n \wedge p|x$

$$\mathbb{Z}_n \setminus \mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid p|n \wedge p|x : p \in P\}$$

$$= \bigcup_{p \in P_n} V_{n,p}$$

$$|\mathbb{Z}_n \setminus \mathbb{Z}_n^*| = \sum_{j=1}^{|P_n|} (-1)^{j-1} \sum_{\substack{I \subseteq P_n \\ |I|=j}} |\bigcap_{r \in I} V_{n,r}|$$

$$= \sum_{j=1}^{|P_n|} (-1)^{j-1} \sum_{\dots} \frac{n}{\prod_{p \in I} p}$$

$$Z_3 \mid Z_{30}^* = Z_{30} \mid \{1, 7, 11, 13, 19, 23, 29\}$$

$$P_n = \{2, 3, 5\}$$

$$U_{n,2} \cup U_{n,3} \cup U_{n,5} = \{0, 2, \dots, 28\} \cup \{0, 3, \dots, 27\} - \{0, 5, \dots, 25\}$$

a	b	k	α	β
7387	8633	1	-7	6
1246	7387	5	6	-1
1157	1146	1	-1	1
99	1157	13	1	0
0	89	—	0	1

$$-7 \cdot 7387 + 6 \cdot 8633 = 89$$

↳

a	b	k	α	β
21	34	1	13	-8
13	21	1	-8	5
8	13	1	5	-3
5	8	1	-3	2
3	5	1	2	-1
2	3	1	-1	1
1	2	2	1	0
0	1	—	0	1

$$12.3 a) \langle \mathbb{Z}_{15}^*, 15, 1 \rangle$$

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

\cdot_{15}	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

$$b) \quad 1) \quad \sigma \circ \sigma = \tau \circ \tau$$

$$(1, 2) = \tau$$

$$(4, 5) = \sigma \circ \tau \circ \sigma$$

$$(1, 7)(4, 5) = \tau \circ \sigma \circ \tau \circ \sigma = \sigma \circ \tau \circ \tau \circ \sigma$$

$$(1, 4)(2, 5) = \sigma$$

$$(1, 5)(2, 4) = \tau \circ \sigma \circ \tau \circ \sigma$$

$$(1, 4, 2, 5) = \tau \circ \sigma$$

$$(1, 5, 2, 4) = \sigma \circ \tau$$

σ	id	τ	$\sigma\tau\sigma$	$(\tau\sigma)^2$	σ	$\tau\sigma\tau$	$\tau\sigma$	$\sigma\tau$
id	id	τ	$\sigma\tau\sigma$	$(\tau\sigma)^2$	σ	$\tau\sigma\tau$	$\tau\sigma$	$\sigma\tau$
τ		id	$(\tau\sigma)^2$	$\sigma\tau\sigma$	$\tau\sigma$	$\sigma\tau$	σ	$\tau\sigma\tau$
$\sigma\tau\sigma$			id	τ	$\tau\tau$	$\tau\sigma$	$\tau\sigma\tau$	σ
$(\tau\sigma)^2$				id				
σ					id			
$\tau\sigma\tau$						id		
$\tau\sigma$							$(\tau\sigma)^2$	
$\sigma\tau$								$(\tau\sigma)^2$

$$\sigma = (1, 4), (1, 5)$$

$$\tau = (1, 2)$$

