

①

Da  $n, m \in \mathbb{Z} : \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$  gilt\* und  $2 \in P$ , woraus folgt  $\varphi(2) = 1$ , ist die Aussage wahr da  $\varphi(n)$  mit 1 multipliziert wird.

\*: Weil  $n$  ungerade ist gilt  $\text{ggT}(n, m) = 1$

$$\varphi(2n) = \varphi(n)$$

$$n = 15:$$

$$\varphi(30) = \varphi(15)$$

$$\varphi(2 \cdot 15) = \varphi(15)$$

$$\varphi(2 \cdot 3 \cdot 5) = \varphi(3 \cdot 5)$$

$$\varphi(2) \cdot \varphi(3) \cdot \varphi(5) = \varphi(3) \cdot \varphi(5)$$

$$1 \cdot 2 \cdot 4 = 2 \cdot 4$$

②

$$11^{1213} \bmod 26$$

Eulersche Funktion:

$$a^{\varphi(26)} = 1 \bmod 26$$

$$\Leftrightarrow \varphi(26) = \varphi(2) \cdot \varphi(13) = 12$$

$$11^{12} = 1 \bmod 26$$

$$\Leftrightarrow a^{12} = 1 \bmod 26$$

gilt

$$11^{12^2} = 11^{144} \bmod 26 = 1 \bmod 26$$

$$11^{1213} = (11^{144} \bmod 26)^8 \cdot 11^{61} \bmod 26$$

$$= 1^8 \bmod 26 \cdot 11^{61} \bmod 26$$

$$= \dots \cdot (11^{12} \cdot 11^{12} \cdot 11^{12} \cdot 11^{12} \cdot 11^{12} \cdot 11^1) \bmod 26$$

$$= 1 \bmod 26 \cdot 11 \bmod 26$$

$$= \underline{\underline{11 \bmod 26}}$$

③

$$(\mathbb{Z}_7, \cdot) = \{0, 1, 2, 3, 4, 5, 6\}$$

•	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$$(\mathbb{Z}_8, \cdot) = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

•	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(4)

$$S_1 = (1, 2, 4, 3)$$

$$S_{10} = (2, 4, 3, 1)$$

$$S_{19} = (3, 2, 4, 1)$$

$$S_2 = (1, 4, 2, 3)$$

$$S_{11} = (1, 4, 3, 2)$$

$$S_{20} = (3, 4, 2, 1)$$

$$S_3 = (4, 1, 2, 3)$$

$$S_{12} = (2, 4, 1, 3)$$

$$S_{21} = (3, 4, 1, 2)$$

$$S_4 = (1, 3, 2, 4)$$

$$S_{13} = (2, 1, 4, 3)$$

$$S_{22} = (3, 1, 2, 4)$$

$$S_5 = (1, 3, 4, 2)$$

$$S_{14} = (4, 1, 3, 2)$$

$$S_{23} = (3, 1, 4, 2)$$

$$S_6 = (2, 1, 3, 4)$$

$$S_{15} = (4, 2, 3, 1)$$

$$S_7 = (2, 3, 1, 4)$$

$$S_{16} = (4, 2, 1, 3)$$

$$S_8 = (2, 3, 4, 1)$$

$$S_{17} = (4, 3, 2, 1)$$

$$S_9 = (3, 2, 1, 4)$$

$$S_{18} = (4, 3, 1, 2)$$

Neutr. Element Ordnung 1 = id:  $\{1, 2, 3, 4\}$

Ordnung 2:  $S_1 \mid S_4 \mid S_6 \mid S_9 \mid S_{11} \mid S_{15}$

Ordnung 3:  $S_2 \mid S_5 \mid S_7 \mid S_{10} \mid S_{13} \mid S_{14} \mid S_{16} \mid S_{17} \mid S_{19} \mid S_{21} \mid S_{22}$

Ordnung 4:  $S_3 \mid S_8 \mid S_{12} \mid S_{18} \mid S_{20} \mid S_{23}$