

---

# ALGEBRAISCHE STRUKTUREN: RINGE/KÖRPER EULERSCHE PHI-FUNKTION

**Fragen?**

\* **Ring oder Körper?** Welche Mengen bilden einen Ring oder Körper?

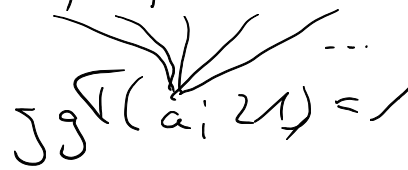
	Ring?	Körper?
a) $(\mathbb{N}, +, \cdot)$	X	X
b) $(\mathbb{Z}, +, \cdot)$	✓	X
c) $(\mathbb{Q}, +, \cdot)$	✓	✓
d) $(\mathbb{R}, +, \cdot)$	✓	✓
e) $(\mathbb{Z}_5, +, \cdot)$	✓	✓
f) $(\mathbb{Z}_4, +, \cdot)$	✓	X
g) $(\mathbb{Z}_n, +, \cdot)$	✓	✓ falls $n$ prim X falls $n$ nicht prim

**Eigener Lösungsversuch.**

	Ring?	Körper?
a) $(\mathbb{N}, +, \cdot)$		
b) $(\mathbb{Z}, +, \cdot)$		
c) $(\mathbb{Q}, +, \cdot)$		
d) $(\mathbb{R}, +, \cdot)$		
e) $(\mathbb{Z}_5, +, \cdot)$		
f) $(\mathbb{Z}_4, +, \cdot)$		
g) $(\mathbb{Z}_n, +, \cdot)$		

**Invertierbarkeitskriterium.** Welche Restklassen in  $\mathbb{Z}_{21}$  sind invertierbar (bzgl.  $\cdot$ ) ?

**Lösung.**

$$1; 2; 4; 5; 8; 10; 11; 13; 16; 17; 19; 20$$

$$\gcd(a; 21) = 1$$

**Eigener Lösungsversuch.**

**Inverses berechnen.** Was ist  $\bar{8}^{-1}$  in  $\mathbb{Z}_{21}$ ?

**Lösung.**

$$8 \cdot x = 1 \text{ in } \mathbb{Z}_{21}$$

$$\overline{\delta^{-1}} = \overline{\delta}$$

$$8x = 9 \cdot 21 + 1 \quad | - 21q$$

$$8x + 21 \cdot \underbrace{(-9)}_7 = 1$$

$$8x + 21y = 1 \rightarrow \text{Dioph. Gl.}$$

$$21_{x-3} + 8y_{x-8} = x$$

$$21 = 2 \cdot 8 + 5$$

$$8 = 1.543$$

$$5 = 1 - 3 + 7$$

3 2 1 (2) H 1

$$2 = 2 - 1 + 0$$

$$gg(21; 8) = 2$$

2-3

-1 2

7-1

01

$$x = -3 \quad y = 8$$

**Eulersche Phi-Funktion.** Wie kann man z.B.  $\varphi(21)$  bestimmen?

Laut Definition ist  $\varphi(21) := \underbrace{\varphi(3)}_{3-1} - \underbrace{\varphi(7)}_{7-1} = 12$

Bei kleinen Zahlen, wie 21, kann man also die invertierbaren Restklassen zählen (s.o.), aber wie kann man das effizient für beliebig Zahlen berechnen?

**Rechenregeln für die Eulersche Phi-Funktion.**

$$\begin{aligned} i) \ p \text{ prim} : & \quad \varphi(p) = \\ ii) \ p \text{ prim} : & \quad \varphi(p^k) = \\ iii) \ \text{ggT}(m, n) = 1 : & \quad \varphi(m \cdot n) = \end{aligned}$$

**Beweis.** *i)*  $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{p-1}\}$

$$ii) \ \mathbb{Z}_{p^k} = \{\overline{0}, \overline{1}, \dots, \overline{1 \cdot p}, \dots, \overline{2 \cdot p}, \dots, \overline{3 \cdot p}, \dots, \overline{p^{k-1} \cdot p} = \overline{p^k} = \overline{0}\}$$

*iii)* Am Beispiel:  $m = 3$  und  $n = 7$ , also  $m \cdot n = 21$ :

$$\mathbb{Z}_{21} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18}, \overline{19}, \overline{20}, \overline{21} = \overline{0}\}$$

**Berechnung der Eulerschen Phi-Funktion.** Berechnen Sie mit den RR:

1.  $\varphi(21)$

3.  $\varphi(7^3)$

5.  $\varphi(81.675)$

2.  $\varphi(30)$

4.  $\varphi(40)$

**Lösung.**

$$1.) \varphi(21) = 12 \quad 2.) \varphi(30) = \underbrace{\varphi(2)}_1 \cdot \underbrace{\varphi(3)}_2 \cdot \underbrace{\varphi(5)}_4 = 8$$

$$3.) \underbrace{\varphi(7^3)}_{7^3 - 7^2} = 294 \quad 4.) \varphi(40) = \underbrace{\varphi(2^3)}_{2^3 - 2^2} \cdot \underbrace{\varphi(5)}_4 = 16$$

$$5.) \varphi(81.675) = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 11 \cdot 4 = 25600 \\ = \underbrace{\varphi(3^3)}_{18} \cdot \varphi(5^2) \cdot \varphi(11^2) \\ 18 \cdot 20 \cdot 110$$

**Eigener Lösungsversuch.**