Hochschule Rosenheim
University of Applied Sciences

Algebraische Strukturen: Ringe/Körper
Eulersche Phi-Funktion

Fragen?

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

	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) $(\mathbb{Z}_n, +, \cdot)$	✓	✓ falls n prim ✗ 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.

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

...

$\mathrm{ggT}(a; 21) = 1$

Eigener Lösungsversuch.

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

Lösung.

$8 \cdot x = 1$ in $\mathbb{Z}_{21}$ $\qquad \overline{8}^{-1} = \overline{8}$

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

$$8\underset{=8}{x} + 21 \cdot \underbrace{(-q)}_{y}{}_{=-3} = 1$$

$$8\underset{=8}{x} + 21\underset{=-3}{y} = 1 \longrightarrow \text{Dioph. Gl.}$$

$$21\underset{=-3}{x} + 8\underset{=8}{y} = 1$$

$\operatorname{ggT}(21; 8) = 2$ $\qquad x = -3 \qquad y = 8$

$21 = 2 \cdot 8 + 5$	-3	8
$8 = 1 \cdot 5 + 3$	2	-3
$5 = 1 \cdot 3 + 2$	-1	2
$3 = 1 \cdot 2 + 1$	1	-1
$2 = 2 \cdot 1 + 0$	0	1

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

Laut Definition ist $\varphi(21) :=$ $\underbrace{\varphi(3)}_{\underbrace{3-1}_{2}} \cdot \underbrace{\varphi(7)}_{\underbrace{7-1}_{6}} = 12$

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.

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

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

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

$iii)$ 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. $\varphi(21)$
2. $\varphi(30)$
3. $\varphi(7^3)$
4. $\varphi(40)$
5. $\varphi(81.675)$

Lösung.

1.) $\varphi(21) = 12$ 2.) $\varphi(30) = \underbrace{\varphi(2)}_{1} \cdot \underbrace{\varphi(3)}_{2} \cdot \underbrace{\varphi(5)}_{4} = 8$

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

5.) $\varphi(81.675) = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 11 \cdot 11 = 39600$

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

Eigener Lösungsversuch.