Algebraische Strukturen: Ringe/Körper
Eulersche Phi-Funktion

Fragen?

$7^{44} \mod 8$

Satz von Euler. Für $ggT(a,m)=1$: $\boxed{a^{\varphi(m)} \equiv 1 \mod m}$

$ggT(7,8)=1 \Longrightarrow 7^{\varphi(m)} = 7^4 \equiv 1 \mod 8$

$\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 8-4 = 4$

$7^{44} = (\underbrace{7^4}_{\equiv 1})^{11} \equiv 1^{11} = 1 \pmod 8.$

$(R, +, \cdot)$

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

Ring: $(R, +)$ abelsche Gruppe, $(R, \cdot)$ Halbgruppe, $+/\cdot$: Distributivität

Körper: $(R, +)$ abelsche Gruppe, $(R \setminus \{0\}, \cdot)$ abelsche Gruppe, $+/\cdot$: Distributivität

	Ring?	Körper?
a) $(\mathbb{N}, +, \cdot)$	✗ $(R,+)$: $0 \notin \mathbb{N}$ (neutr. Elt.) ✗; $-2 \notin \mathbb{N}$ (inv. Elt zu 2) ✗; $\rightarrow (R,+)$ keine Gruppe	✗
b) $(\mathbb{Z}, +, \cdot)$	✓	✗ $2 \cdot \_\_ \neq 1$ da $\frac{1}{2} \notin R \setminus \{0\}$; $(R \setminus \{0\}, \cdot)$ keine Gruppe!
c) $(\mathbb{Q}, +, \cdot)$	✓	✓ (da Inversen dabei!)
d) $(\mathbb{R}, +, \cdot)$	✓	✓
e) $(\mathbb{Z}_5, +, \cdot)$	✓	✓ 5 prim!
f) $(\mathbb{Z}_4, +, \cdot)$	✓	✗ 4 nicht prim! (z.B. $\bar{2}$ nicht invert.) $ggT(2,4) = 2 \neq 1$
g) $(\mathbb{Z}_n, +, \cdot)$	✓	? ✓ falls n prim; ✗ falls n nicht prim

Restklassen: e), f), g)

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.

$$\bar{a} \in \mathbb{Z}_{21} \text{ inv.} \iff \operatorname{ggT}(a, \overset{3\cdot 7}{21}) = 1$$

a Vielf. von 3/7 hat ggT 3/7

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

$\varphi(21) = 12$ Stück

Eigener Lösungsversuch.

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

Lösung. $\overline{8}\cdot\underbrace{\overline{x}} = \overline{1} \iff 8x = 1 + q\cdot 21 \iff 8x + 21\cdot\underbrace{(-q)}_{y} = 1$

EEA mit a = 8 und b = 21 :

a =	q *	b +	r	x	y	ggT =	a *	x +	b *	y
8 =	0 *	21 +	8	$\boxed{8}$	-3	1 =	8 *	8 +	21 *	-3
21 =	2 *	8 +	5	-3	8	1 =	21 *	-3 +	8 *	8
8 =	1 *	5 +	3	2	-3	1 =	8 *	2 +	5 *	-3
5 =	1 *	3 +	2	-1	2	1 =	5 *	-1 +	3 *	2
3 =	1 *	2 +	$\boxed{1}$	1	-1	1 =	3 *	1 +	2 *	-1
2 =	2 *	$\boxed{1}$ +	0	0	1	1 =	2 *	0 +	1 *	1

ggT(8,21) = 1 ✓

$\overline{8}^{-1} = \overline{x} = \overline{8}$

[Probe: $\overline{8}\cdot\overline{8} = \overline{64} = \overline{1}$ in $\mathbb{Z}_{21}$]

Eigener Lösungsversuch.

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

Laut Definition ist $\varphi(21) :=$ Anz. der inv. Elte. in $\mathbb{Z}_{21}$ $= \left|\{\bar{a} \in \mathbb{Z}_{21} \mid \overbrace{\bar{a} \text{ invertierbar}}^{ggT(a,n)=1}\}\right| \overset{s.o.}{=} 12$

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.

$$\boxed{\begin{array}{lrl} i)\ p \text{ prim}: & \varphi(p) = & p-1 \\ ii)\ p \text{ prim};\ k \geq 1: & \varphi(p^k) = & p^k - p^{k-1} = p^{k-1} \cdot (p-1) \\ iii)\ \mathrm{ggT}(m,n) = 1: & \varphi(m \cdot n) = & \varphi(m) \cdot \varphi(n) \end{array}}$$

Mit diesen Formeln kann man $\varphi(n)$ für ein beliebiges n über die PFZ berechnen!

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

$p-1$ Stück mit $ggT(a,p) = 1$, da $p \nmid a$ wegen $a = 1, \ldots, p-1 < p$

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

$ggT(a, p^k) \neq 1 \iff p \mid a \iff a$ Vielfaches von p (p^{k-1} – Stück!)

$\varphi(p^k) =$ Alle − nicht inv. $= p^k - p^{k-1}$

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

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

Vielf. von 3: $1\cdot3$, $2\cdot3$, $3\cdot3$, $4\cdot3$, $5\cdot3$, $6\cdot3$, $7\cdot3$ ← 7 Stück

Vielf. von 7: $1\cdot7$, $2\cdot7$, $3\cdot7$ ← 3 Stück

doppelt!

$\underset{3\cdot7}{\varphi(21)} =$ Alle − nicht inv. $= \underbrace{3 \cdot 7}_{\text{Alle}} - (7 + 3 - 1) =$

$= (3-1) \cdot (7-1) = \varphi(3) \cdot \varphi(7)$

Allgemein ✓.

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.

Strategie: Bilde PFZ von n & wende RR an:

1. $\varphi(\underbrace{21}_{3\cdot 7}) \overset{iii)}{=} \underbrace{\varphi(3)}_{\overset{i)}{=}\,2} \cdot \underbrace{\varphi(7)}_{\overset{i)}{=}\,6} = 2\cdot 6 = 12$ (vgl. Aufgabe "Invert. Krit." zuvor)

2. $\varphi(\underbrace{30}_{2\cdot 3\cdot 5}) \overset{iii)}{=} \underbrace{\varphi(2)}_{\overset{i)}{=}\,1} \cdot \underbrace{\varphi(3)}_{\overset{i)}{=}\,2} \underbrace{\varphi(5)}_{\overset{i)}{=}\,4} = 8$

3. $\varphi(7^3) \overset{ii)}{=} \underbrace{7^3}_{343} - \underbrace{7^2}_{49} = 294$

   $= \underbrace{(7-1)}_{6} \cdot \underbrace{7^2}_{49} = 294$

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

5. $\varphi(\underbrace{81.675}_{3^3\cdot 5^2\cdot 11^2}) \overset{iii)}{\overset{!}{=}} \underbrace{\varphi(3^3)}_{(\underbrace{3^3}_{27}-\underbrace{3^2}_{9})} \underbrace{\varphi(5^2)}_{(\underbrace{5^2}_{25}-5)} \underbrace{\varphi(11^2)}_{(\underbrace{11^2}_{121}-11)} = 18\cdot 20\cdot 110$

   $= \underline{39.600}$

Eigener Lösungsversuch.