

Die Ringe \mathbb{Z}_n

- für $n > 0$ wird auf $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ definiert:

$$+_n : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n : (a, b) \mapsto (a + b) \bmod n$$

$$*_n : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n : (a, b) \mapsto (a * b) \bmod n$$

Beispiel $n = 15$

$$9 +_{15} 11 = 5$$

$$9 *_{15} 11 = 9$$

$$9 *_{15} 5 = 0$$

$$9 \wedge_{15} 11 = 9$$

- $\langle \mathbb{Z}_n; +_n, *_n \rangle$ ist ein Ring mit kommutativer Addition und Multiplikation
- $\langle \mathbb{Z}_n; +_n, *_n \rangle$ ist genau dann nullteilerfrei, wenn n eine Primzahl ist



Algebraische Bemerkung (äquivalente Definition)

Der Ring $\langle \mathbb{Z}_n; +_n, *_n \rangle$ entsteht aus dem Ring $\langle \mathbb{Z}; +, * \rangle$, indem man Restklassen bezüglich der Untergruppe (sogar: Ideal)

$n\mathbb{Z} = \{n \cdot k; k \in \mathbb{Z}\}$ betrachtet:

- Die n verschiedenen Restklassen

$$[a]_n = a + n\mathbb{Z} = \{a + n \cdot k; k \in \mathbb{Z}\}$$

bilden die Elemente des Ringes $\langle \mathbb{Z}/(n\mathbb{Z}); \oplus_n, \odot_n \rangle$ mit

$$[a]_n \oplus_n [b]_n = [a + b]_n \quad (a, b \in \mathbb{Z})$$

$$[a]_n \odot_n [b]_n = [a \cdot b]_n \quad (a, b \in \mathbb{Z})$$

- $[a]_n = [b]_n \Leftrightarrow a \equiv b \pmod n \Leftrightarrow n|(a - b)$
- Die Ringe $\langle \mathbb{Z}/(n\mathbb{Z}); \oplus_n, \odot_n \rangle$ und $\langle \mathbb{Z}_n; +_n, *_n \rangle$ sind isomorph:

$$\langle \mathbb{Z}/(n\mathbb{Z}) \ni [a]_n \Leftrightarrow a \bmod n \in \mathbb{Z}_n$$



Invertierbare Elemente ("Einheiten")

- beachte: für $a, n \in \mathbb{Z}$ gilt (Bézout!!)

$$\text{ggT}(a, n) = 1 \Leftrightarrow \exists b \exists k \in \mathbb{Z} : a * b + n * k = 1$$

- Dabei gilt

$$\text{ggT}(a, n) = 1 \Rightarrow \text{ggT}(b, n) = 1$$

- b ist bis auf Vielfache von n eindeutig bestimmt, ist also ein Element von \mathbb{Z}_n !
- Man berechnet b (bzw. $b \bmod n$) mit Hilfe des erweiterten euklidischen Algorithmus.



- für $a \in \mathbb{Z}_n$

$$\exists b \in \mathbb{Z}_n : a *_n b = 1 \Leftrightarrow \exists b \in \mathbb{Z} \exists k \in \mathbb{Z} : a * b + n * k = 1$$

$$\Leftrightarrow \text{ggT}(a, n) = 1$$

- dieses $b \in \mathbb{Z}_n$ ist das Inverse von $a \in \mathbb{Z}_n$ bezüglich der Multiplikation: $b = a^{-1}$
- Menge der invertierbaren Elemente von \mathbb{Z}_n :

$$\mathbb{Z}_n^* = \{a \in \{1, 2, \dots, n-1\}; \text{ggT}(a, n) = 1\}$$

- Beispiel:

$$EEA(11, 19) \Rightarrow 11 \cdot 7 + 19 * (-4) = 1 \Rightarrow 11^{-1} = 7 \text{ in } \mathbb{Z}_{19}$$

- Beispiel \mathbb{Z}_{18}

a	1	5	7	11	13	17
a^{-1}	1	11	13	5	7	17



- ▶ \mathbb{Z}_n^* hat multiplikative Gruppenstruktur, denn wegen

$$\text{ggT}(a, n) = 1, \text{ggT}(b, n) = 1 \Rightarrow \text{ggT}(a * b, n) = 1$$

gilt

- ▶ $\forall a, b \in \mathbb{Z}_n^* : a * b \in \mathbb{Z}_n^*$
- ▶ $\forall a \in \mathbb{Z}_n^* \exists b \in \mathbb{Z}_n^* : a * b = 1$ (eeA!!!)

und daher:

$$U_n = \langle \mathbb{Z}_n^*; *_n \rangle \text{ ist eine kommutative Gruppe}$$

(“Einheitengruppe modulo n ”)

Beispiel $\mathbb{Z}_{18}^* = U_{18}$:

*18	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

- ▶ Folgerung (Gleichungslösen in \mathbb{Z}_n)

$$\forall a \in \mathbb{Z}_n^* \forall b \in \mathbb{Z}_n \exists_1 x \in \mathbb{Z}_n : a * x = b$$

nämlich $x = a^{-1} *_n b$

- ▶ Aus dem Lösungsverfahren für \mathbb{Z} folgt:

- ▶ Für $a, b \in \mathbb{Z}_n$ gilt:

$$a * x = b \text{ lösbar} \iff \text{ggT}(a, n) \mid b$$

- ▶ Falls $\text{ggT}(a, n) = d$, so gibt es genau d verschiedene Lösungen

$$x_0 + k \cdot \frac{n}{d} \quad (0 \leq k < d) \quad \text{wobei} \quad \frac{a}{d} \cdot x_0 = \frac{b}{d} \text{ in } \mathbb{Z}_{n/d} \text{ (eindeutig)}$$

Eulers φ -Funktion

- ▶ Definition: $\#U_n = \#\mathbb{Z}_n^* = \varphi(n)$

- ▶ erste Werte:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

- ▶ φ ist *multiplikativ* in folgendem Sinne:

$$\text{ggT}(a, b) = 1 \Rightarrow \varphi(a * b) = \varphi(a) * \varphi(b)$$

- ▶ Multiplikativität ist äquivalent zu

$$n = \sum_{d \mid n} \varphi(d) \quad (n > 0)$$

$\sum_{d \mid n}$: Summe über alle positiven Teiler d von n

- ▶ Beispiel: $18 = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(9) + \varphi(18) = 1 + 1 + 2 + 2 + 6 + 6$

Folgerung aus der Multiplikativität

- φ ist durch seine Werte auf Primzahlpotenzen bestimmt:

$$p \text{ prim} \Rightarrow \varphi(p^e) = p^{e-1}(p-1) \quad (e > 0)$$

- Speziell: $\langle \mathbb{Z}_n; +_n, *_n \rangle$ Körper $\Leftrightarrow n$ Primzahl $\Leftrightarrow \varphi(n) = n-1$
- Folgerung: falls $n = \prod_{i=1}^k p_i^{e_i}$

$$\varphi(n) = \prod_{i=1}^k p_i^{e_i-1}(p_i-1) = n \cdot \prod_{\substack{p|n \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right)$$

- Also: Berechnung von $\varphi(n)$ einfach, falls Primfaktorisierung von n bekannt
- Aber: bis heute ist kein effizientes Verfahren zur Berechnung von $\phi(n)$ (z.B. ohne Kenntnis der Primfaktorisierung) bekannt!



Beispiele

- $n = 12$

$$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\} \quad \varphi(12) = \#\mathbb{Z}_{12}^* = 4$$

$$12 = 2^2 * 3 \quad \varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 4$$

- $n = 13$

$$\mathbb{Z}_{13}^* = \{1, 2, 3, \dots, 12\} \quad \varphi(13) = \#\mathbb{Z}_{13}^* = 12$$

$$13 = 13 \quad \varphi(13) = 13 \cdot \left(1 - \frac{1}{13}\right) = 12$$

- $n = 67914$

$$67914 = 2 * 3^2 * 7^3 * 11$$

$$\varphi(67914) = n \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{7}\right) \cdot \left(1 - \frac{1}{11}\right) = 17640$$



Beispiel: Zerlegung von \mathbb{Z}_{18}

$$\begin{aligned} \mathbb{Z}_{18} &= \{0, 1, 2, 3, \dots, 17\} \\ &= \underbrace{\{1, 5, 7, 11, 13, 17\}}_{\text{ggT}(a,18)=1} \uplus \underbrace{\{2, 4, 8, 10, 14, 16\}}_{\text{ggT}(a,18)=2} \\ &\quad \uplus \underbrace{\{3, 15\}}_{\text{ggT}(a,18)=3} \uplus \underbrace{\{6, 12\}}_{\text{ggT}(a,18)=6} \uplus \underbrace{\{9\}}_{\text{ggT}(a,18)=9} \uplus \underbrace{\{0\}}_{\text{ggT}(a,18)=18} \\ &= 1 \cdot \{1, 5, 7, 11, 13, 17\} \uplus 2 \cdot \{1, 2, 4, 5, 7, 8\} \\ &\quad \uplus 3 \cdot \{1, 5\} \uplus 6 \cdot \{1, 2\} \uplus 9 \cdot \{1\} \uplus 18 \cdot \{0\} \\ &= 1 \cdot \mathbb{Z}_{18}^* \uplus 2 \cdot \mathbb{Z}_9^* \uplus 3 \cdot \mathbb{Z}_6^* \uplus 6 \cdot \mathbb{Z}_3^* \uplus 9 \cdot \mathbb{Z}_2^* \uplus 18 \cdot \mathbb{Z}_1^* \\ &= \biguplus_{d|18} d \cdot \mathbb{Z}_{18/d}^* \\ \Rightarrow 18 &= \sum_{d|18} \#\mathbb{Z}_{18/d}^* = \sum_{d|18} \varphi\left(\frac{18}{d}\right) = \sum_{d|18} \varphi(d) \end{aligned}$$



Nachweis der Multiplikativität

- Für $n \in \mathbb{N}$ und $d | n$ ist

$$A_{n,d} := \{a \in \mathbb{Z}_n; \text{ggT}(a, n) = d\} = d \cdot \mathbb{Z}_{n/d}^*$$

- Wegen $\mathbb{Z}_n = \biguplus_{d|n} A_{n,d}$ folgt

$$n = \#\mathbb{Z}_n = \sum_{d|n} \#A_{n,d} = \sum_{d|n} \#\mathbb{Z}_{n/d}^* = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d)$$

- Induktion über Teilerstruktur für a, b mit $\text{ggT}(a, b) = 1$:

- Angenommen: für e, f mit $e|a, f|b$ und $e \cdot f \neq a \cdot b$ sei $\varphi(e) \cdot \varphi(f) = \varphi(e \cdot f)$ bereits gezeigt, dann folgt $\varphi(a) \cdot \varphi(b) = \varphi(a \cdot b)$ aus

$$\sum_{e|a} \sum_{f|b} \varphi(e \cdot f) = \sum_{d|a \cdot b} \varphi(d) = a \cdot b = \sum_{e|a} \varphi(e) \cdot \sum_{f|b} \varphi(f)$$



Exkurs: Möbius-Inversion

(A.F. Möbius: *Über eine besondere Art der Umkehrung von Reihen*, 1831)

- Definiere eine multiplikative Funktion $\mu : \mathbb{N}_{>0} \rightarrow \{0, \pm 1\}$ (die *Möbiusfunktion*) durch

$$\mu(1) = 1, \quad \mu(p^e) = \begin{cases} -1 & \text{für } e = 1 \\ 0 & \text{für } e > 1 \end{cases} \quad (p \text{ Primzahl})$$

also für $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$

$$\mu(n) = \begin{cases} (-1)^k & \text{falls } e_1 = e_2 = \dots = e_k = 1 \text{ (quadratfrei)} \\ 0 & \text{sonst} \end{cases}$$

- erste Werte:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1



- Sind $f, g : \mathbb{N}_{>0} \rightarrow \mathbb{C}$ Funktionen, so sind die beiden Aussagen

$$g(n) = \sum_{d|n} f(d) \quad (n \geq 1)$$

$$f(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot g(d) \quad (n \geq 1)$$

äquivalent zueinander. Insbesondere ist dann jede der beiden Funktionen durch die andere eindeutig bestimmt

- Beweis (durch Vertauschen von Summationen):

$$\begin{aligned} \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \cdot \sum_{e|\frac{n}{d}} f(e) = \sum_{e|n} f(e) \cdot \sum_{d|\frac{n}{e}} \mu(d) \\ &= \sum_{e|n} f(e) \cdot \delta_{e,n} = f(n) \end{aligned}$$



- μ hat die Eigenschaft

$$\sum_{d|n} \mu(d) = \delta_{n,1} = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

- Beweis mittels Binomialformel. Für $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$ ist

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum \{ \mu(d); d|n, d \text{ quadratfrei} \} \\ &= \sum_{0 \leq j \leq k} \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq k} \mu(p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_j}) \\ &= \sum_{0 \leq j \leq k} \binom{k}{j} (-1)^j = (1-1)^k = \delta_{k,0} = \begin{cases} 0 & k > 0 \\ 1 & k = 0 \end{cases} \end{aligned}$$



Das spezielle Beispiel $g(n) = n, f(n) = \varphi(n)$

$$g(n) = n = \sum_{d|n} \varphi(d) = \sum_{d|n} f(d)$$

$$f(n) = \varphi(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$$

Beachte nun für $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$

$$\begin{aligned} \sum_{d|n} \mu(d) \cdot \frac{n}{d} &= \sum_{0 \leq j \leq k} \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq k} \mu(p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_j}) \cdot \frac{n}{p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_j}} \\ &= n \cdot \sum_{0 \leq j \leq k} \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq k} \frac{(-1)^j}{p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_j}} \\ &= n \cdot \prod_{\substack{p|n \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right) \end{aligned}$$



Gruppentheoretisches Intermezzo (additiv)

G kommutative Gruppe, H Untergruppe von G

- Definition der H -Äquivalenz:

$$\forall a, b \in G : a \sim_H b \leftrightarrow b - a \in H$$

$$\begin{aligned} 0 \in H &\Rightarrow \sim_H \text{ ist reflexiv} \\ a \in H \rightarrow -a \in H &\Rightarrow \sim_H \text{ ist symmetrisch} \\ a, b \in H \rightarrow a + b \in H &\Rightarrow \sim_H \text{ ist transitiv} \end{aligned}$$

- Folgerung: \sim_H ist eine Äquivalenzrelation auf G
 Die Äquivalenzklassen ("Nebenklassen" (cosets) von H)

$$[a]_H = \{b \in G ; a \sim_H b\} = \{a + h ; h \in H\} = a + H$$

partitionieren G in "gleich grosse" Teile, denn

$$H \rightarrow [a]_H : h \mapsto a + h \text{ ist bijektiv, also } \forall a \in G : \# [a]_H = \# H$$



Gruppentheoretisches Intermezzo (multiplikativ)

G Gruppe, H Untergruppe von G

- Definition der H -Äquivalenz:

$$\forall a, b \in G : a \sim_H b \leftrightarrow a^{-1} * b \in H$$

$$\begin{aligned} e \in H &\Rightarrow \sim_H \text{ ist reflexiv} \\ a \in H \rightarrow a^{-1} \in H &\Rightarrow \sim_H \text{ ist symmetrisch} \\ a, b \in H \rightarrow a * b \in H &\Rightarrow \sim_H \text{ ist transitiv} \end{aligned}$$

- Folgerung: \sim_H ist eine Äquivalenzrelation auf G
 Die Äquivalenzklassen ("Nebenklassen" (cosets) von H)

$$[a]_H = \{b \in G ; a \sim_H b\} = \{a * h ; h \in H\} = a * H$$

partitionieren G in "gleich grosse" Teile, denn

$$H \rightarrow [a]_H : h \mapsto a * h \text{ ist bijektiv, also } \forall a \in G : \# [a]_H = \# H$$



Bemerkung für die Definitionen der H -Äquivalenz bezüglich einer Untergruppe H in einer nicht-kommutativen Gruppe G :

- Es kommt bei der Multiplikation auf die Reihenfolge der Faktoren an. Die Aussagen $a^{-1} * b \in H$ (d.h. $b \in a * H$) und $b * a^{-1} \in H$ (d.h. $b \in H * a$) sind i.a. nicht gleichwertig. Entsprechend muss man "Linksnebenklassen" $a * H$ und "Rechtsnebenklassen" $H * a$ unterscheiden. Es kann vorkommen, dass $a * H \neq H * a$
- Ist H eine Untergruppe von G und gilt $a * H = H * a$ für alle $a \in G$, so spricht man von H als einer normalen Untergruppe oder einem Normalteiler von G .

Normalteiler sind besonders angenehme Untergruppen, weil man auf der Menge der Nebenklassen wieder eine Gruppenoperation definieren kann

$$\forall a, b \in G : [a]_H * [b]_H := [a * b]_H$$

Für Nicht-Normalteiler funktioniert das nicht!



Zyklische Gruppen

- G Gruppe (multiplikativ), $a \in G$

$$\langle a \rangle = \{ \dots, a^{-2}, a^{-1}, e = a^0, a = a^1, a^2, a^3, \dots \} = \{ a^k ; k \in \mathbb{Z} \}$$

ist eine Untergruppe von G : die von a erzeugte Untergruppe

- Falls $\# \langle a \rangle = \infty$: $\langle a \rangle$ hat die gleiche Struktur wie $(\mathbb{Z}, +)$:
 - a hat unendliche Ordnung, $ord_G(a) = \infty$,
 - $\langle a \rangle$ ist eine unendliche zyklische Gruppe.
- Falls $\# \langle a \rangle = n < \infty$: $\langle a \rangle$ hat die gleiche Struktur wie $(\mathbb{Z}_n, +_n)$:
 - a hat endliche Ordnung, $ord_G(a) = n$,
 - $\langle a \rangle$ ist eine endliche zyklische Gruppe der Ordnung n .
- Eine Gruppe G heisst *zyklische Gruppe*, wenn es ein $a \in G$ gibt mit $G = \langle a \rangle$.
- Die Gruppen $(\mathbb{Z}, +)$ und $(\mathbb{Z}_n, +_n)$ (für $n \geq 1$) sind — bis auf Isomorphie — die einzigen zyklischen Gruppen.



Beispiele

Betrachten Einheitengruppen $U_n = \mathbb{Z}_n^*$:
 $\# \langle a \rangle = \text{ord}_n(a)$: die Ordnung (Periode) von a modulo n

► $n = 7$

$\langle 1 \rangle = \{1\}$	$\text{ord}_7(1) = 1$
$\langle 2 \rangle = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 1, \dots\} = \{1, 2, 4\}$	$\text{ord}_7(2) = 3$
$\langle 3 \rangle = \{1, 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1, \dots\}$ $= \{1, 2, 3, 4, 5, 6\}$	$\text{ord}_7(3) = 6$
$\langle 4 \rangle = \{1, 4, 2, 1, \dots\} = \{1, 2, 4\}$	$\text{ord}_7(4) = 3$
$\langle 5 \rangle = \{1, 5, 4, 6, 2, 3, 1, \dots\} = \{1, 2, 3, 4, 5, 6\}$	$\text{ord}_7(5) = 6$
$\langle 6 \rangle = \{1, 6, 1, \dots\} = \{1, 6\}$	$\text{ord}_7(6) = 2$

$U_7 = \mathbb{Z}_7^* = \langle 3 \rangle = \langle 5 \rangle$ ist also eine zyklische Gruppe



Beispiele

► $n = 8$

$\langle 1 \rangle = \{1\}$	$\text{ord}_8(1) = 1$
$\langle 3 \rangle = \{1, 3, 3^2 = 1, \dots\} = \{1, 3\}$	$\text{ord}_8(3) = 2$
$\langle 5 \rangle = \{1, 5, 5^2 = 1, \dots\} = \{1, 5\}$	$\text{ord}_8(5) = 2$
$\langle 7 \rangle = \{1, 7, 7^2 = 1, \dots\} = \{1, 7\}$	$\text{ord}_8(7) = 2$

$U_8 = \mathbb{Z}_8^* = \{1, 3, 5, 7\} \neq \langle 1 \rangle, \langle 3 \rangle, \langle 5 \rangle, \langle 7 \rangle$.
 U_8 ist also keine zyklische Gruppe.



Beispiele

► $n = 9$

$\langle 1 \rangle = \{1\}$	$\text{ord}_9(1) = 1$
$\langle 2 \rangle = \{1, 2, 2^2 = 4, 2^3 = 8, 2^4 = 7, 2^5 = 5, 2^6 = 1, \dots\}$ $= \{1, 2, 4, 5, 7, 8\}$	$\text{ord}_9(2) = 6$
$\langle 4 \rangle = \{1, 4, 7, 1, \dots\} = \{1, 4, 7\}$	$\text{ord}_9(4) = 3$
$\langle 5 \rangle = \{1, 5, 7, 8, 4, 2, 1, \dots\} = \langle 2 \rangle$	$\text{ord}_9(5) = 6$
$\langle 7 \rangle = \langle 4 \rangle$	$\text{ord}_9(7) = 3$
$\langle 8 \rangle = \{1, 8\}$	$\text{ord}_9(8) = 2$

$U_9 = \mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\} = \langle 2 \rangle = \langle 5 \rangle$

U_9 ist also eine zyklische Gruppe.



Beispiele

► $n = 10$

$\langle 1 \rangle = \{1\}$	$\text{ord}_{10}(1) = 1$
$\langle 3 \rangle = \{1, 3, 9, 7, 1, \dots\}$	$\text{ord}_{10}(3) = 4$
$\langle 7 \rangle = \{1, 7, 9, 3, 1, \dots\}$	$\text{ord}_{10}(7) = 4$
$\langle 9 \rangle = \{1, 9, 1, \dots\}$	$\text{ord}_{10}(9) = 2$

$U_{10} = \mathbb{Z}_{10}^* = \{1, 3, 7, 9\} = \langle 3 \rangle = \langle 7 \rangle$
 U_{10} ist also eine zyklische Gruppe.



► $n = 11$

$\langle 1 \rangle = \{1\}$	$ord_{11}(1) = 1$
$\langle 2 \rangle = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1, \dots\}$	$ord_{11}(2) = 10$
$\langle 3 \rangle = \{1, 3, 9, 5, 4, 1, \dots\}$	$ord_{11}(3) = 5$
$\langle 4 \rangle = \{1, 4, 5, 9, 3, 1, \dots\}$	$ord_{11}(4) = 5$
$\langle 5 \rangle = \{1, 5, 3, 4, 9, 1, \dots\}$	$ord_{11}(5) = 5$
$\langle 6 \rangle = \{1, 6, 3, 7, 9, 10, 5, 8, 4, 2, 1, \dots\}$	$ord_{11}(6) = 10$
$\langle 7 \rangle = \{1, 7, 5, 2, 3, 10, 4, 6, 9, 8, 1, \dots\}$	$ord_{11}(7) = 10$
$\langle 8 \rangle = \{1, 8, 9, 6, 4, 10, 3, 2, 5, 7, 1, \dots\}$	$ord_{11}(8) = 10$
$\langle 9 \rangle = \{1, 9, 4, 3, 5, 1, \dots\}$	$ord_{11}(9) = 5$
$\langle 10 \rangle = \{1, 10, 1, \dots\}$	$ord_{11}(10) = 2$

$U_{11} = \mathbb{Z}_{11}^* = \{1, 2, 3, \dots, 10\} = \langle 2 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle$
 U_{11} ist also eine zyklische Gruppe.



► $n = 12$

$\langle 1 \rangle = \{1\}$	$ord_{12}(1) = 1$
$\langle 5 \rangle = \{1, 5, 1, \dots\}$	$ord_{12}(5) = 2$
$\langle 7 \rangle = \{1, 7, 1, \dots\}$	$ord_{12}(7) = 2$
$\langle 11 \rangle = \{1, 11, 1, \dots\}$	$ord_{12}(10) = 2$

$U_{12} = \mathbb{Z}_{12}^* = \{1, 5, 7, 11\} \neq \langle 1 \rangle, \langle 5 \rangle, \langle 7 \rangle, \langle 11 \rangle$
 U_{12} ist also keine zyklische Gruppe.



Die Sätze von LAGRANGE, FERMAT und EULER

► Satz von LAGRANGE

G endliche Gruppe, $H \subseteq G$ Untergruppe $\Rightarrow \#H \mid \#G$.

► Folgerung:

- G endliche (multiplikative) Gruppe mit neutralem Element e .
 Für jedes $a \in G$ gilt:

$$ord_G(a) \mid \#G$$

und somit

$$a^{\#G} = a^{ord_G(a)} = e$$

- $ord_G(a)$ ist die kleinste positive Zahl t mit $a^t = e$



Nützliche Regeln für das Rechnen mit Ordnungen:

- Wegen der Divisionseigenschaft gilt für $k \in \mathbb{Z}$:

$$a^k = a^{k \bmod ord_G(a)} = a^{k \bmod \#G}$$

also

$$a^k = e \Leftrightarrow ord_G(a) \mid k$$

- Für $k \in \mathbb{Z}$ gilt:

$$ord_G(a^k) = \frac{ord_G(a)}{\text{ggT}(k, ord_G(a))} = \frac{\text{kgV}(k, ord_G(a))}{k}$$

Begründung: für $a, b, c \in \mathbb{Z}$ gilt

$$a \mid (b \cdot c) \Leftrightarrow \frac{a}{\text{ggT}(a, b)} \mid c \Leftrightarrow \frac{\text{kgV}(a, b)}{b} \mid c$$



- ▶ Spezielle Situation der Einheitengruppen $U_n = \mathbb{Z}_n^*$ modulo n :

$$\forall a \in U_n : \text{ord}_n(a) = \# \langle a \rangle \mid \#G = \varphi(n)$$

also

$$\forall a \in U_n : a^{\varphi(n)} = a^{\text{ord}_n(a)} = 1$$

- ▶ Satz von EULER: Für alle $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

- ▶ Satz von FERMAT: Für jede Primzahl p und beliebiges $a \in \mathbb{Z}$ mit $p \nmid a$ gilt

$$a^{p-1} \equiv 1 \pmod{p}$$

und damit auch $a^p \equiv a \pmod{p}$ für alle $a \in \mathbb{Z}$.

- ▶ Für alle $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ und $k \in \mathbb{Z}$ gilt:

$$a^k = a^{k \bmod \varphi(n)} = a^{k \bmod \text{ord}_n(a)} \pmod{n}$$



Zur Illustration: \mathbb{Z}_{36}^*

- ▶ $\mathbb{Z}_{36}^* = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$, $\varphi(36) = 12$
- ▶ $\varphi(36) = 36 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3}) = 12$
- ▶ $\langle 5 \rangle = \{1, 5, 25, 17, 13, 29\}$, $\text{ord}_{36}(5) = 6$
- ▶ $5^{117} \equiv 5^9 \equiv 5^3 \equiv 17 \pmod{36}$
- ▶ $\langle 13 \rangle = \{1, 13, 25\}$, $\text{ord}_{36}(13) = 3$
- ▶ $13^{116} \equiv 13^8 \equiv 13^2 \equiv 25 \pmod{36}$



Zur Illustration: \mathbb{Z}_{17}^*

- ▶ $\mathbb{Z}_{17}^* = \{1, 2, 3, \dots, 16\}$, $\varphi(17) = 16$
- ▶ $\varphi(17) = 17 \cdot (1 - \frac{1}{17}) = 16$
- ▶ $\langle 3 \rangle = \{1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6\}$,
 $\text{ord}_{17}(3) = 16$
- ▶ $3^{99} \equiv 3^3 \equiv 10 \pmod{17}$
- ▶ $\langle 4 \rangle = \{1, 4, 16, 13\}$, $\text{ord}_{17}(4) = 4$
- ▶ $4^{106} \equiv 4^{10} \equiv 4^2 \equiv 16 \pmod{17}$



Ein Blick in Richtung Faktorisierung

- ▶ Problem: eine grosse Zahl $N \in \mathbb{N}$ soll faktorisiert werden.
- ▶ Annahme: man kann für a mit $1 < a < N$ die Ordnung (Periode) $\text{ord}_N(a)$ bestimmen.
- ▶ Man wählt sich ein a und berechnet $\text{ggT}(a, N)$.
 - ▶ Falls $\text{ggT}(a, N) > 1$ hat man einen Faktor von N gefunden!
 - ▶ Andernfalls ist $a \in \mathbb{Z}_N^*$ und $\text{ord}_N(a)$ ist definiert.
- ▶ Falls $\text{ord}_N(a)$ ungerade, ist a nicht weiter brauchbar. (Der Fall tritt nur selten ein)
- ▶ Falls $\text{ord}_N(a) = 2t$, so gilt $N \mid (a^{2t} - 1)$ und $N \nmid (a^t - 1)$, also

$$N \mid (a^{2t} - 1) = (a^t - 1)(a^t + 1)$$

- ▶ Falls $N \mid (a^t + 1)$, ist a nicht weiter brauchbar. (Der Fall tritt nur selten ein)
- ▶ Falls $N \nmid (a^t + 1)$, müssen $\text{ggT}(N, a^t + 1)$ und $\text{ggT}(N, a^t - 1)$ echte Faktoren von N liefern!



Beispiel: die Faktorisierung von $N = 15$

- ▶ Für $a \in \{3, 5, 6, 9, 10, 12\}$ ist $\text{ggT}(a, 15) > 1$
- ▶ Für $a \in U_{15}$:

a	$\text{ord}_{15}(a)$	t	a^t+1	$\text{ggT}(15, a^t+1)$	a^t-1	$\text{ggT}(15, a^t-1)$
2	4	2	5	5	3	3
4	2	1	5	5	3	3
7	4	2	50	5	48	3
8	4	2	65	5	63	3
11	2	1	12	3	19	5
13	4	2	170	5	168	3
14	2	1	15	15	13	1

- ▶ Ausser $a = 14$ (und $a = 1$, natürlich!) liefern alle $a \in U_{14}$ eine Faktorisierung, falls man $\text{ord}_{15}(a)$ kennt.

▶ $N = 77$:

- ▶ $\varphi(77) = 77 \cdot (1 - \frac{1}{7}) \cdot (1 - \frac{1}{11}) = 60$
- ▶ Von den 60 Elementen $a \in U_{77}$ haben 15 eine ungerade Ordnung $\text{ord}_{77}(a)$.
- ▶ Von den 45 Elementen $a \in U_{77}$ mit gerader Ordnung $\text{ord}_{77}(a) = 2t$ liefern 30 mittels $\text{ggT}(a^t + 1, 77)$ einen echten Teiler von 77.

▶ $N = 119$

- ▶ $\varphi(119) = 119 \cdot (1 - \frac{1}{7}) \cdot (1 - \frac{1}{17}) = 96$
- ▶ Von den 96 Elementen $a \in U_{119}$ haben drei (1,18,86) eine ungerade Ordnung $\text{ord}_{119}(a)$.
- ▶ Von den 93 Elementen $a \in U_{119}$ mit gerader Ordnung $\text{ord}_{119}(a) = 2t$ liefern 90 (ausgenommen 33, 101, 118) , mittels $\text{ggT}(a^t + 1, 119)$ einen echten Teiler von 119.