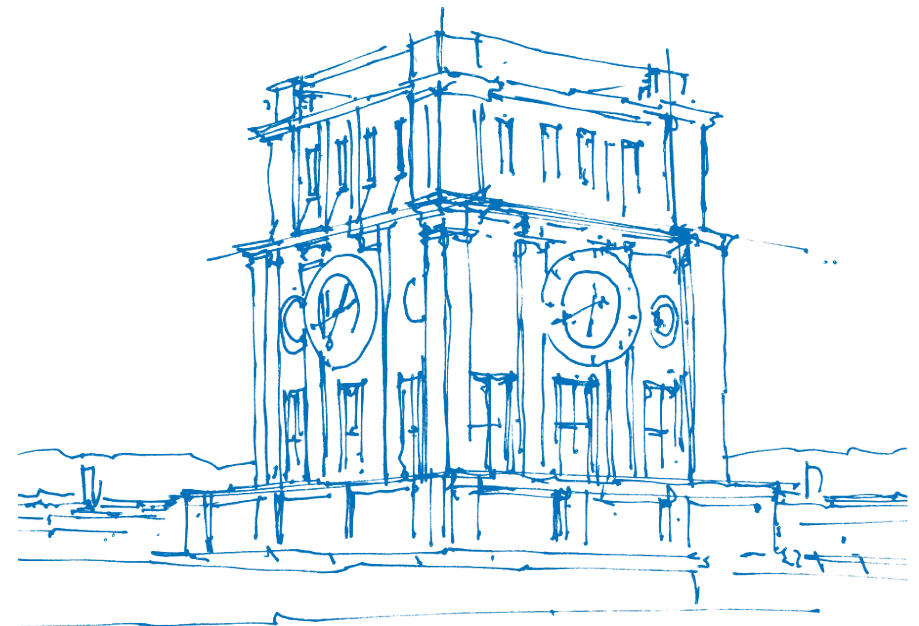


Diskrete Strukturen Tutorium

Jay Zhou

Technische Universität München

Garching b. München, 5. Februar 2023



TUM Uhrenturm

Algebra

Algebra — Definition

- $p \mid n$ bedeutet n durch p teilbar $n > p$
- $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid \text{ggT}(k, n) = 1\}$
- $\varphi(n) = |\mathbb{Z}_n^*| = n \cdot \prod_{\substack{p \mid n \\ \text{Alle Primfaktoren}}} \left(1 - \frac{1}{p}\right)$
- Ordnung: $\text{op}_1^{\text{ord}} n = \text{neutral}$ n op sich selbst ord mal
- $\langle n \rangle$ bezeichnet die Gruppe von aller Elemente eines Ordnungsrechnens

Algebra — Inverse

Erweiterter Euklidischer Algorithmus

$ggT = 54 \cdot 16 + 24$

$54 = 24 \cdot 2 + 6$

$24 = 6 \cdot 4 + 0$

a	b	k	α	β
54	888	16	33	-2
24	54	2	-2	1
6	24	4	1	0
0	6	-	0	1

$33 = 1 - (-2) \cdot 16$

$-2 = 0 - 1 \cdot 2$

$1 = 1 - 0 \cdot 4$

Letzte Zeile optional

$$ggT(54, 888) = 54 \cdot 33 + 888 \cdot (-2) = 6$$

Algebra — Modulo

$$— (a \cdot b) \equiv_n (a \bmod n) \cdot (b \bmod n)$$

$$— a^b \equiv_n (a \bmod n)^b$$

$$— a^b \equiv_n (a \bmod n)^{b \bmod (n-1)} \quad \text{nur wenn } n \text{ ist prim, und } a \text{ nicht teilbar durch } n$$

$$— a^{\varphi(n)-1} \equiv_n a^{-1}$$

Beispiel:

$$38^5 \equiv_{83} 38^4 \cdot 38 \equiv_{83} 1444^2 \cdot 38 \equiv_{83} 33^2 \cdot 38 \equiv_{83} 1089 \cdot 38 \equiv_{83} 10 \cdot 38 \equiv_{83} 48$$

$$5^{216} \equiv_{13} 25^{108} \equiv_{13} 12^0 \equiv_{13} 1, \text{ da } 13 \text{ prim ist und } 13 \text{ nicht teilbar durch } 5$$

$$23^{9791} \equiv_{9991} 23^{-1} \equiv_{9991} 2172, \text{ da } 9791 = \varphi(9991) - 1$$

Aufgaben

Aufgabe 14.1

Sei $n = 1383$ mit Primfaktorzerlegung $n = 3^1 \cdot 461^1$ im Weiteren.

- (a) Berechnen Sie $\varphi(n)$.
- (b) Tabellieren Sie den erweiterten euklidischen Algorithmus für $a = 860$ und $b = n$ entsprechend der Vorlesung.
- (c) Berechnen Sie das multiplikative Inverse von a in $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$.

$$a) \quad \varphi(n) = n \cdot \prod_{p \in \{3, 461\}} \left(1 - \frac{1}{p}\right) = 1383 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{461}\right) = 920$$

b)

a	b	[b/a]	α	β
860	1383	1	632	-393
523	860	1	-393	239
337	523	1	239	-154
186	337	1	-154	85
151	186	1	85	-69
35	151	4	-69	16
11	35	3	16	-5
2	11	5	-5	1
1	2	-	1	0

$$\text{gcd} = \alpha \cdot a + \beta \cdot b = 1$$

Danke DSolver :)

dsolver.de

$$c) \quad \text{Da } \text{ggT}(860, 1383) = 1$$

$$a^{-1} = \alpha = 632$$

Aufgabe 14.2

Sei $n = 1491$ und $a = 935$ im Weiteren.

- Berechnen Sie $|\mathbb{Z}_n^*|$ für $n = 1491$.
- Tabellieren Sie den erweiterten euklidischen Algorithmus für a und n entsprechend der Vorlesung.
- Berechnen Sie das multiplikative Inverse von a in $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$.

a) $2 \nmid 3 \mid 1491 = 3 \cdot 7 \cdot 71 \Rightarrow |\mathbb{Z}_n^*| = \varphi(n) = n \cdot \prod_{p \in \{3, 7, 71\}} (1 - \frac{1}{p})$

$3 \nmid 7 \mid 497$
 71

$$= 1491 \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{7}) \cdot (1 - \frac{1}{71})$$

$$= 840$$

b)

a	b	[b/a]	α	β
935	1491	1	716	-449
556	935	1	-449	267
379	556	1	267	-182
177	379	2	-182	85
25	177	7	85	-12
2	25	12	-12	1
1	2	-	1	0

$$\text{gcd} = \alpha \cdot a + \beta \cdot b = 1$$

c) Da $\text{ggT}(935, 1491) = 1$

$$a^{-1} = \alpha = 716$$

$$a) \quad 2 \mid 24 = 2^3 \cdot 3 \Rightarrow |\mathbb{Z}_n^*| = \varphi(n) = n \cdot \prod_{p \in \{2,3\}} \left(1 - \frac{1}{p}\right)$$

$$\begin{array}{r} 2 \mid 24 \\ 2 \mid 12 \\ 2 \mid 6 \\ 3 \end{array}$$

Aufgabe 14.3

Sei $n = 24$ im Weiteren.

(a) Bestimmen Sie $|\mathbb{Z}_n^*|$.

(b) Tabellieren Sie die Gruppenoperation von $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$ entsprechend der Vorlesung und den Tutorübungen.

$$b) \quad \mathbb{Z}_n^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$$

Beispiel

$$13 \cdot 11 = 143 \equiv_{24} 23$$

$$7 \cdot 19 = 133 \equiv_{24} 13$$

\bullet_{24}	1	5	7	11	13	17	19	23
1	1	5	7	11	13	17	19	23
5	5	1	11	7	17	13	23	19
7	7	11	1	5	19	23	13	17
11	11	7	5	1	23	19	17	13
13	13	17	19	23	1	5	7	11
17	17	13	23	19	5	1	11	7
19	19	23	13	17	7	11	1	5
23	23	19	17	13	11	7	5	1

$$\mathbb{Z}_n^* = \{ 1, 5, 7, \\ 11, 13, 17, \\ 19, 23 \}$$

Aufgabe 14.3

Sei $n = 24$ im Weiteren.

- (a) Bestimmen Sie $|\mathbb{Z}_n^*|$.
- (b) Tabellieren Sie die Gruppenoperation von $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$ entsprechend der Vorlesung und den Tutorübungen.
- (c) Bestimmen Sie $\langle x \rangle$ für jedes $x \in \mathbb{Z}_n^*$ bzgl. $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$

$$\langle 1 \rangle = \{ 1 \} \quad \begin{array}{l} \text{1}^2 \equiv_{24} 1 \text{ (neutrales Elem.)} \\ \text{ord} = 1 \end{array}$$

$$\langle 5 \rangle = \{ 5, 1 \} \quad \begin{array}{l} \text{5}^2 \equiv_{24} 1 \text{ (neutrales Elem.)} \\ \text{ord} = 2 \end{array}$$

$$\langle 7 \rangle = \{ 7, 1 \} \quad \begin{array}{l} \text{7}^2 \equiv_{24} 1 \text{ (neutrales Elem.)} \\ \text{ord} = 2 \end{array}$$

$$\langle 11 \rangle = \{ 11, 1 \}$$

$$\langle 13 \rangle = \{ 13, 1 \}$$

$$\langle 17 \rangle = \{ 17, 1 \}$$

$$\langle 19 \rangle = \{ 19, 1 \}$$

$$\langle 23 \rangle = \{ 23, 1 \}$$

$$\mathbb{Z}_n^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$$

Aufgabe 14.3

Sei $n = 24$ im Weiteren.

- Bestimmen Sie $|\mathbb{Z}_n^*|$.
- Tabellieren Sie die Gruppenoperation von $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$ entsprechend der Vorlesung und den Tutorübungen.
- Bestimmen Sie $\langle x \rangle$ für jedes $x \in \mathbb{Z}_n^*$ bzgl. $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$
- Zeichnen Sie den gerichteten Graphen $\langle \mathbb{Z}_n^*, \{(x, x \cdot_n a) \mid a \in \{\sigma, \tau\}\} \rangle$ für $\sigma = 11$ und $\tau = 19$. Beschriften Sie dabei jede Kante mit dem zugehörigen $a \in \{\sigma, \tau\}$.

Beispiel

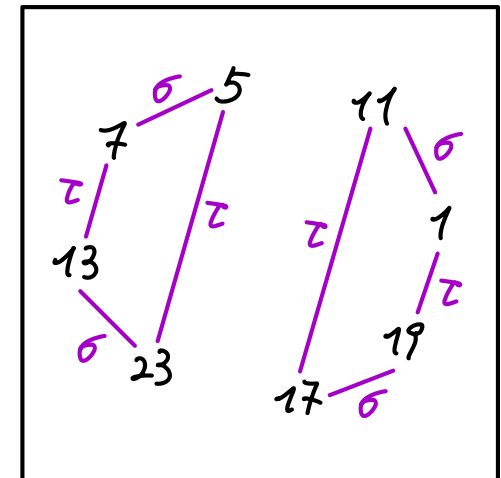
$$1 \cdot \sigma \equiv_{24} 11$$

$$1 \cdot \tau \equiv_{24} 19$$

$$5 \cdot \sigma \equiv_{24} 7$$

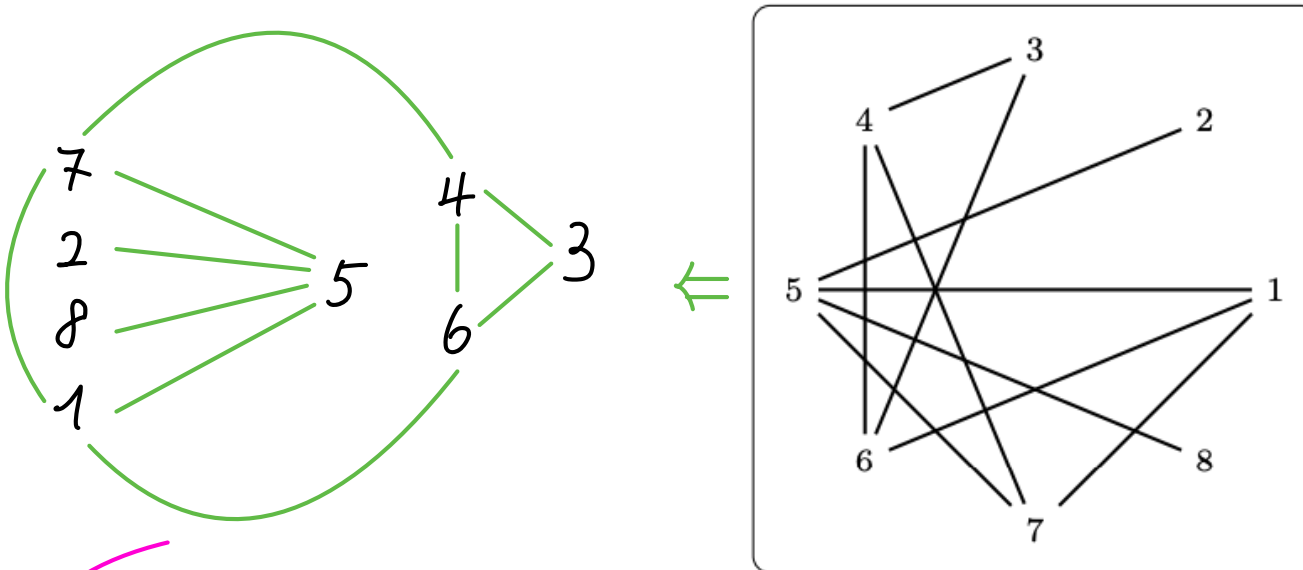
$$5 \cdot \tau \equiv_{24} 23$$

	1	5	7	11	13	17	19	23
σ	11	7	5	1	23	19	17	13
τ	19	23	7	17	7	11	1	5



Aufgabe 14.4

Gegeben ist der folgende einfache Graph G über der Knotenmenge $V = [8]$:



- (a) Sei A die Menge der Automorphismen von G . Geben Sie alle Elemente von A in Zykelschreibweise an.
 (b) Tabellieren Sie die Gruppenoperation von $\langle A, \circ, \text{Id}_A \rangle$ entsprechend der Vorlesung und den Tutorübungen.

a) Automorphismen

b) $A \circ A \cong A$ / $A \circ \text{Id} \cong A$

- Id
- $(2, 8)$
- $(1, 7)(4, 6)$
- $(1, 7)(4, 6)(2, 8)$

	$(1, 7)(2, 8)(4, 6)$	$(2, 8)$	Id	$(1, 7)(4, 6)$
$(1, 7)(2, 8)(4, 6)$	Id	$(1, 7)(4, 6)$	$(1, 7)(2, 8)(4, 6)$	$(2, 8)$
$(2, 8)$	$(1, 7)(4, 6)$	Id	$(2, 8)$	$(1, 7)(2, 8)(4, 6)$
Id	$(1, 7)(2, 8)(4, 6)$	$(2, 8)$	Id	$(1, 7)(4, 6)$
$(1, 7)(4, 6)$	$(2, 8)$	$(1, 7)(2, 8)(4, 6)$	$(1, 7)(4, 6)$	Id

EEA Source Code

von Jay aus dem 1. Semester :)

```

import sys

a = {}
b = {}
k = {}
s = {}
t = {}
a[0] = int(sys.argv[1])
b[0] = int(sys.argv[2])

while a[len(a) - 1] != 0:
    k[len(k)] = int(b[len(b) - 1] / a[len(a) - 1])
    a[len(a)] = b[len(b) - 1] % a[len(a) - 1]
    b[len(b)] = a[len(a) - 2]
    l = len(a)
    s[l - 1] = 0
    s[l - 2] = 1
    t[l - 2] = 0
    t[l - 3] = 1
    for i in range(l - 3):
        s[l - 3 - i] = t[l - 2 - i] - k[l - 3 - i] * s[l - 2 - i]
        t[l - 4 - i] = s[l - 3 - i]
    s[0] = t[1] - k[0] * s[1]

print("-----")
print("| a | b | k | s | t |")
for i in range(l - 1):
    print("| " + str(a[i]) + " | " + str(b[i]) + " | " + str(k[i]) + " | " + str(s[i]) + " | " + str(t[i]) + " |")
print("ggT(" + str(a[0]) + ", " + str(b[0]) + ") = " + str(a[0]) + " * " + str(s[0]) + " + " + str(b[0]) + " * " + str(t[0]) + " \\"
      + " = " + str(a[0] * s[0] + b[0] * t[0]))

```

Danke fürs Teilnehmen!
Viel Erfolg bei der Klausur :)