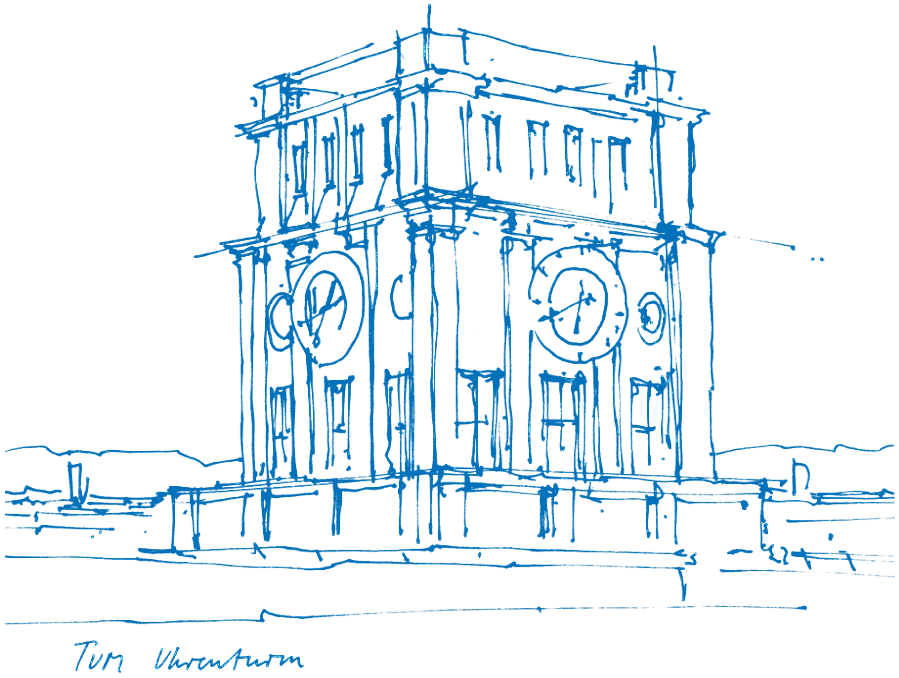
Diskrete Strukturen Tutorium

Jay Zhou
Technische Universität München
Garching b. München, 5. Februar 2023



Algebra

Algebra — Definition

— $p \mid n$ bedeutet n durch p teilbar $n > p$

— $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid \text{ggT}(k, n) = 1\}$

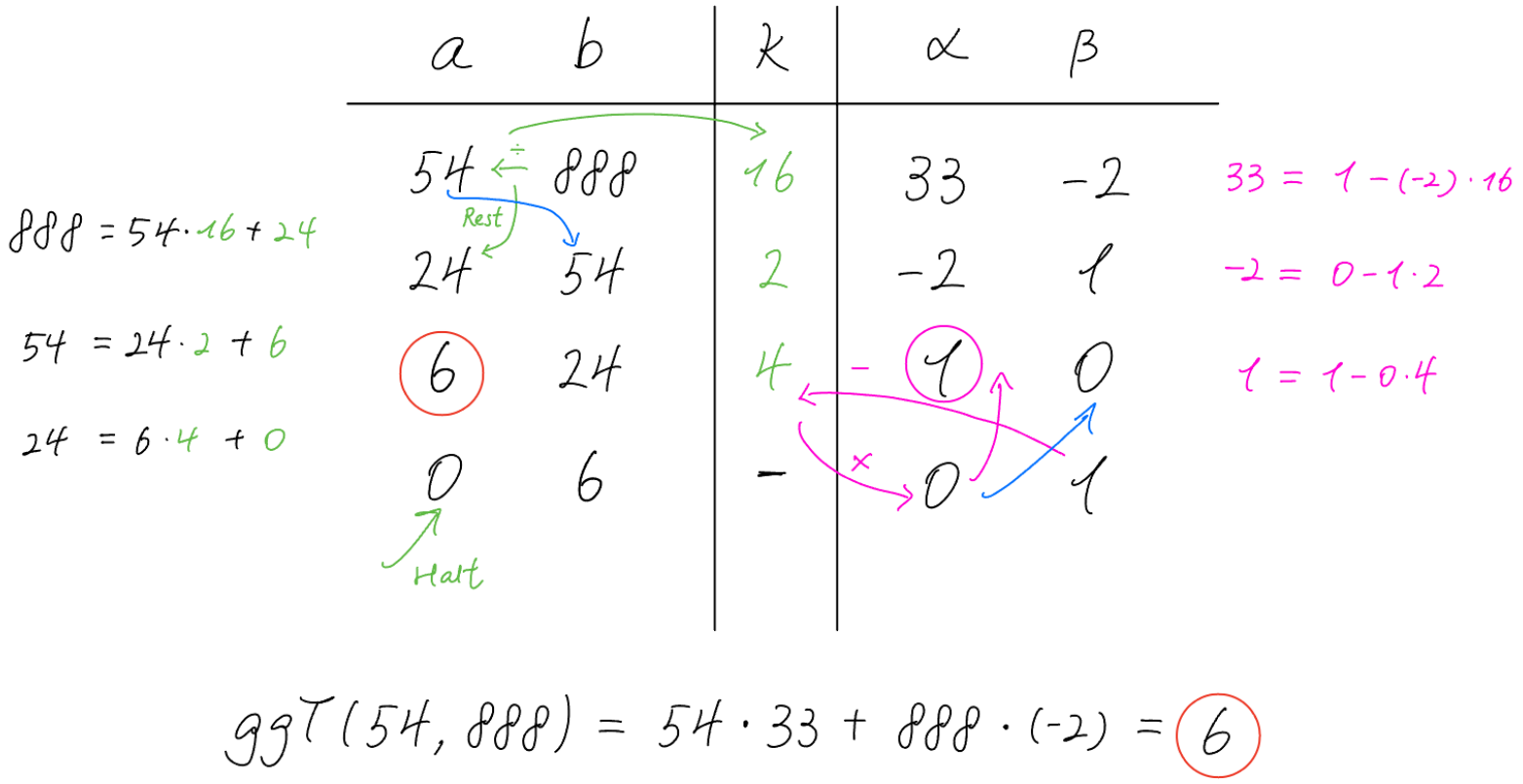
— $\varphi(n) = |\mathbb{Z}_n^*| = n \cdot \prod_{p \mid n} (1 - \frac{1}{p})$

— Ordnung: $\text{op}_1^{\text{ord}}\ n =$ neutral n op sich selbst ord mal

— $< n >$ bezeichnet die Gruppe von aller Elemente eines Ordnungsrechens

Algebra — Inverse

Erweiterter Euklidische Algorithmus



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

Algebra — Modulo

— $(a \cdot b) \equiv_n (a \mod n) \cdot (b \mod n)$
— $a^b \equiv_n (a \mod n)^b$
— $a^b \equiv_n (a \mod n)^{b \mod (n-1)}$ nur wenn n is prim, und a nicht teilbar durch n
— $a^{\varphi(n)-1} \equiv_n a^{-1}$

Beispiel:
$38^5 \equiv_{83} 38^4 \cdot 38 \equiv_{83} 1444^2 \cdot 38 \equiv_{83} 33^2 \cdot 38 \equiv_{83} 1089 \cdot 38 \equiv_{83} 10 \cdot 38 \equiv_{83} 48$
$5^{216} \equiv_{13} 25^{108} \equiv_{13} 12^0 \equiv_{13} 1$, da 13 prim ist und 13 nicht teilbar durch 5
$23^{9791} \equiv_{9991} 23^{-1} \equiv_{9991} 2172$, 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 $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$.

Aufgabe 14.2

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

(a) Berechnen Sie $|\mathbb{Z}_n^*|$ für $n = 1491$.

(b) Tabellieren Sie den erweiterten euklidischen Algorithmus für a und n entsprechend der Vorlesung.

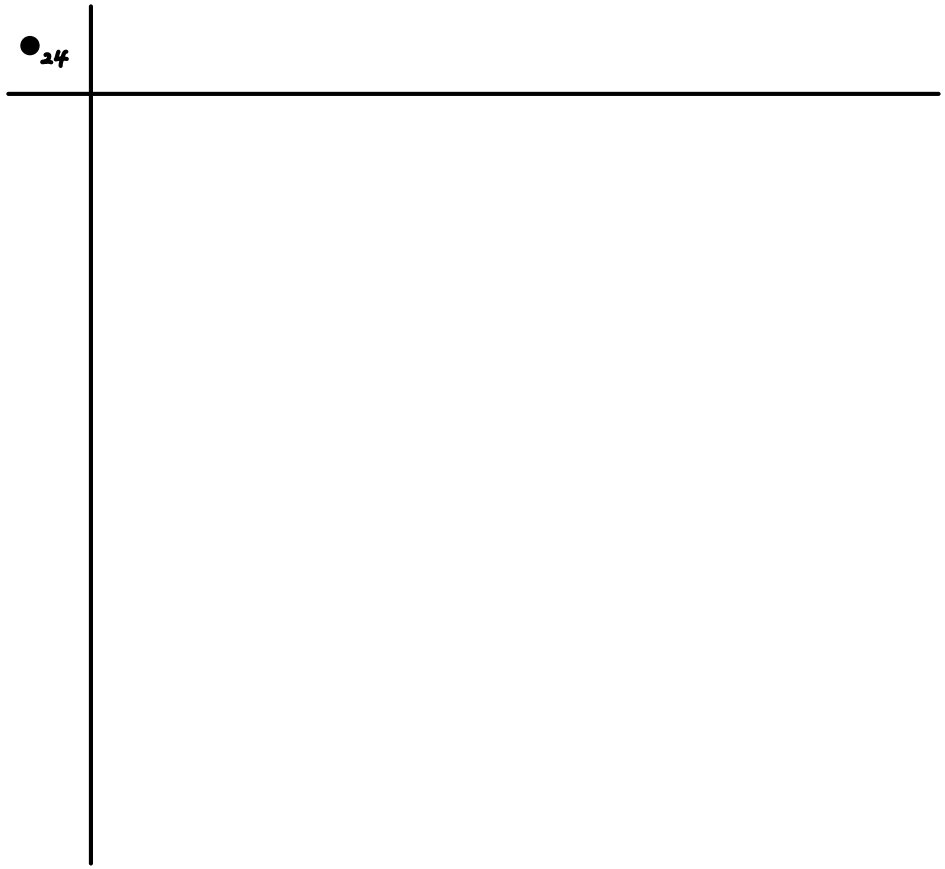
(c) Berechnen Sie das multiplikative Inverse von a in $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$.

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.



Aufgabe 14.3

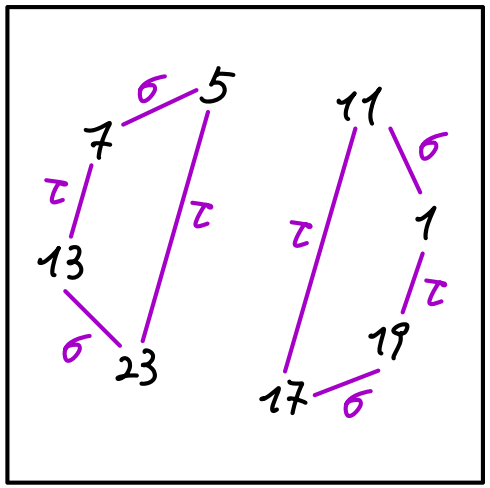
Sei $n = 24$ im Weiteren.

(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.

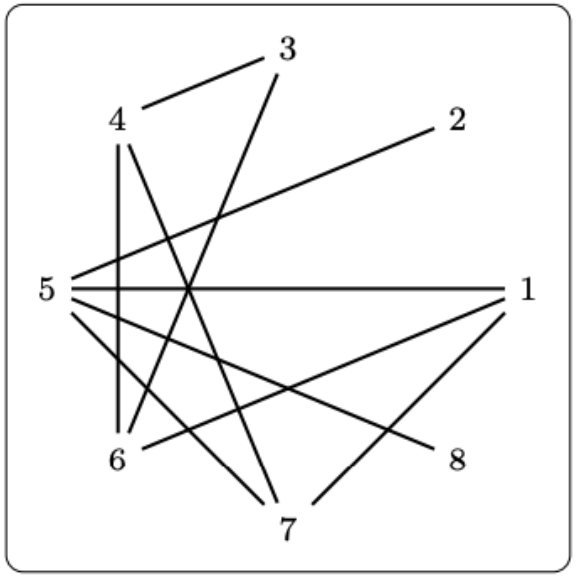
(c) Bestimmen Sie $\langle x \rangle$ für jedes $x \in \mathbb{Z}_n^*$ bzgl. $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$

(d) 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 $a \in \{\sigma, \tau\}$.



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 $\langle A, \circ, \mathsf{Id}_A \rangle$ entsprechend der Vorlesung und den Tutorübungen.

EEA Source Code

von Jay aus dem 1. Semester :)

auf Python

```python
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 :)