Diskrete Strukturen – Q&A

Sommer 2019

Prof. Stefan Lucks, Jannis Bossert
<firstname>.<lastname>(at)uni-weimar.de

Bauhaus-Universität Weimar

September 11, 2020

Section 1

Beweise

Induktive Beweise

Grundlegende Idee: Wir beweisen, dass eine Aussage gilt indem wir

1. zeigen, dass sie für das kleinste Element m_0 gilt (Induktionsanfang),
2. zeigen, dass sie für $m + 1$ gilt, wenn sie für m gilt (Induktionsschritt).

Daraus folgt, dass sie für $\texttt{next}(m_0)$ gilt – und damit für das darauf Folgende und so weiter.

Induktive Beweise

Grundlegende Idee: Wir beweisen, dass eine Aussage gilt indem wir

1. zeigen, dass sie für das kleinste Element m_0 gilt (Induktionsanfang),
2. zeigen, dass sie für $m + 1$ gilt, wenn sie für m gilt (Induktionsschritt).

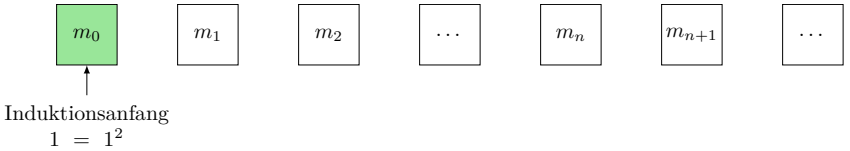
Daraus folgt, dass sie für $\texttt{next}(m_0)$ gilt – und damit für das darauf Folgende und so weiter.

Induktive Beweise

Grundlegende Idee: Wir beweisen, dass eine Aussage gilt indem wir

1. zeigen, dass sie für das kleinste Element m_0 gilt (Induktionsanfang),
2. zeigen, dass sie für $m + 1$ gilt, wenn sie für m gilt (Induktionsschritt).

Daraus folgt, dass sie für $\texttt{next}(m_0)$ gilt – und damit für das darauf Folgende und so weiter.

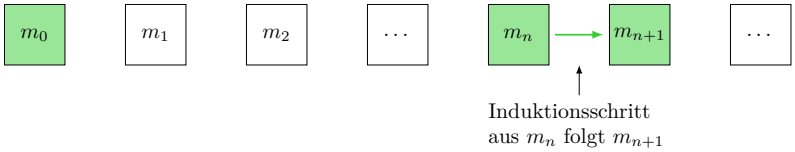


Induktive Beweise

Grundlegende Idee: Wir beweisen, dass eine Aussage gilt indem wir

1. zeigen, dass sie für das kleinste Element m_0 gilt (Induktionsanfang),
2. zeigen, dass sie für $m + 1$ gilt, wenn sie für m gilt (Induktionsschritt).

Daraus folgt, dass sie für $\texttt{next}(m_0)$ gilt – und damit für das darauf Folgende und so weiter.

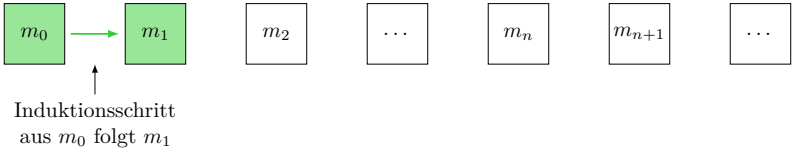


Induktive Beweise

Grundlegende Idee: Wir beweisen, dass eine Aussage gilt indem wir

1. zeigen, dass sie für das kleinste Element m_0 gilt (Induktionsanfang),
2. zeigen, dass sie für $m + 1$ gilt, wenn sie für m gilt (Induktionsschritt).

Daraus folgt, dass sie für $\texttt{next}(m_0)$ gilt – und damit für das darauf Folgende und so weiter.

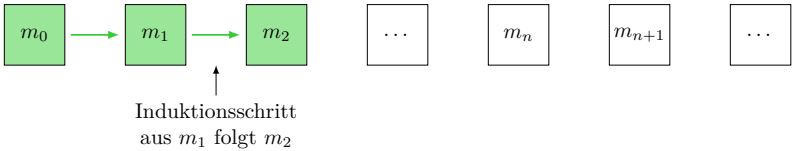


Induktive Beweise

Grundlegende Idee: Wir beweisen, dass eine Aussage gilt indem wir

1. zeigen, dass sie für das kleinste Element m_0 gilt (Induktionsanfang),
2. zeigen, dass sie für $m + 1$ gilt, wenn sie für m gilt (Induktionsschritt).

Daraus folgt, dass sie für $\texttt{next}(m_0)$ gilt – und damit für das darauf Folgende und so weiter.



Induktive Beweise

Grundlegende Idee: Wir beweisen, dass eine Aussage gilt indem wir

1. zeigen, dass sie für das kleinste Element m_0 gilt (Induktionsanfang),
2. zeigen, dass sie für $m + 1$ gilt, wenn sie für m gilt (Induktionsschritt).

Daraus folgt, dass sie für $\texttt{next}(m_0)$ gilt – und damit für das darauf Folgende und so weiter.

Induktive Beweise

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)
Als Formel: $\sum_{k=1}^{n} 2k - 1 = n^2$.

Induktionsanfang:

Induktive Beweise

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)
Als Formel: $\sum_{k=1}^{n} 2k - 1 = n^2$.

Induktionsanfang: $n = 1 \rightarrow$ Die erste ungerade Zahl ist die $1 = 1^2$.
Induktionsschritt: $n \rightarrow n + 1$:

Induktive Beweise

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

Als Formel: $\sum_{k=1}^{n} 2k - 1 = n^2$.

Induktionsanfang: $n = 1 \rightarrow$ Die erste ungerade Zahl ist die $1 = 1^2$.

Induktionsschritt: $n \rightarrow n + 1$:

$$\sum_{k=1}^{n+1} 2k - 1 = 2(n+1) - 1 + \sum_{k=1}^{n} 2k - 1 = (n+1)^2$$

Induktive Beweise

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)
Als Formel: $\sum_{k=1}^{n} 2k - 1 = n^2$.

Induktionsanfang: $n = 1 \rightarrow$ Die erste ungerade Zahl ist die $1 = 1^2$.
Induktionsschritt: $n \rightarrow n + 1$:
Unter der Annahme, dass unsere Formel für $m = n$ gilt $\left(\sum_{k=1}^{n} 2k - 1 = n^2 \right)$ erhalten wir:

$$\sum_{k=1}^{n+1} 2k - 1 = 2(n+1) - 1 + \sum_{k=1}^{n} 2k - 1 = 2(n+1) - 1 + n^2 = 2n + 1 + n^2$$

Dank der binomischen Formeln wissen wir: $2n + 1 + n^2 = (n+1)^2$. $\square$

Induktive Beweise

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

Als Formel: $\sum_{k=1}^{n} 2k - 1 = n^2$.

Induktionsanfang: $n = 1 \rightarrow$ Die erste ungerade Zahl ist die $1 = 1^2$.

Induktionsschritt: $n \rightarrow n + 1$:

Unter der Annahme, dass unsere Formel für $m = n$ gilt $\left(\sum_{k=1}^{n} 2k - 1 = n^2 \right)$ erhalten wir:

$$\sum_{k=1}^{n+1} 2k - 1 = 2(n+1) - 1 + \sum_{k=1}^{n} 2k - 1 = 2(n+1) - 1 + n^2 = 2n + 1 + n^2$$

Dank der binomischen Formeln wissen wir: $2n + 1 + n^2 = (n+1)^2$. $\square$

m_0 m_1 m_2 $\dots$ m_n m_{n+1} $\dots$

Induktive Beweise

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

Als Formel: $\sum_{k=1}^{n} 2k - 1 = n^2$.

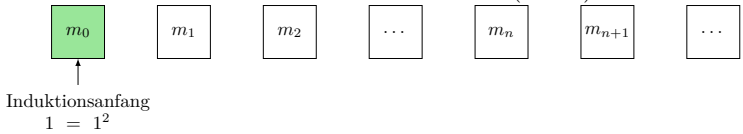
Induktionsanfang: $n = 1 \rightarrow$ Die erste ungerade Zahl ist die $1 = 1^2$.

Induktionsschritt: $n \rightarrow n + 1$:

Unter der Annahme, dass unsere Formel für $m = n$ gilt $\left(\sum_{k=1}^{n} 2k - 1 = n^2 \right)$ erhalten wir:

$$\sum_{k=1}^{n+1} 2k - 1 = 2(n+1) - 1 + \sum_{k=1}^{n} 2k - 1 = 2(n+1) - 1 + n^2 = 2n + 1 + n^2$$

Dank der binomischen Formeln wissen wir: $2n + 1 + n^2 = (n+1)^2$. □



Induktive Beweise

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

Als Formel: $\sum_{k=1}^{n} 2k - 1 = n^2$.

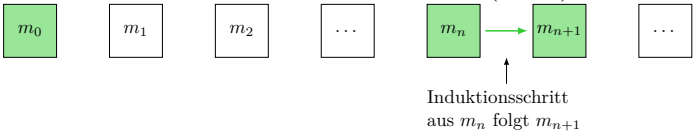
Induktionsanfang: $n = 1 \rightarrow$ Die erste ungerade Zahl ist die $1 = 1^2$.

Induktionsschritt: $n \rightarrow n + 1$:

Unter der Annahme, dass unsere Formel für $m = n$ gilt $\left(\sum_{k=1}^{n} 2k - 1 = n^2 \right)$ erhalten wir:

$$\sum_{k=1}^{n+1} 2k - 1 = 2(n+1) - 1 + \sum_{k=1}^{n} 2k - 1 = 2(n+1) - 1 + n^2 = 2n + 1 + n^2$$

Dank der binomischen Formeln wissen wir: $2n + 1 + n^2 = (n+1)^2$. □



Induktive Beweise

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

Als Formel: $\sum_{k=1}^{n} 2k - 1 = n^2$.

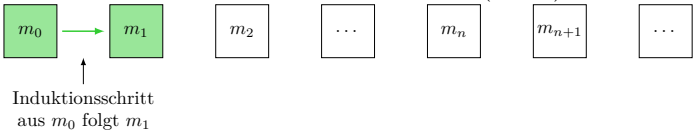
Induktionsanfang: $n = 1 \rightarrow$ Die erste ungerade Zahl ist die $1 = 1^2$.

Induktionsschritt: $n \rightarrow n + 1$:

Unter der Annahme, dass unsere Formel für $m = n$ gilt $\left(\sum_{k=1}^{n} 2k - 1 = n^2 \right)$ erhalten wir:

$$\sum_{k=1}^{n+1} 2k - 1 = 2(n+1) - 1 + \sum_{k=1}^{n} 2k - 1 = 2(n+1) - 1 + n^2 = 2n + 1 + n^2$$

Dank der binomischen Formeln wissen wir: $2n + 1 + n^2 = (n+1)^2$. □



Induktive Beweise

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

Als Formel: $\sum_{k=1}^{n} 2k - 1 = n^2$.

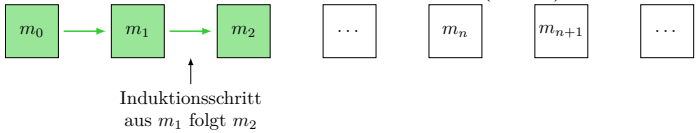
Induktionsanfang: $n = 1 \rightarrow$ Die erste ungerade Zahl ist die $1 = 1^2$.

Induktionsschritt: $n \rightarrow n + 1$:

Unter der Annahme, dass unsere Formel für $m = n$ gilt $\left(\sum_{k=1}^{n} 2k - 1 = n^2 \right)$ erhalten wir:

$$\sum_{k=1}^{n+1} 2k - 1 = 2(n+1) - 1 + \sum_{k=1}^{n} 2k - 1 = 2(n+1) - 1 + n^2 = 2n + 1 + n^2$$

Dank der binomischen Formeln wissen wir: $2n + 1 + n^2 = (n+1)^2$. □



Induktive Beweise

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

Als Formel: $\sum_{k=1}^{n} 2k - 1 = n^2$.

Induktionsanfang: $n = 1 \rightarrow$ Die erste ungerade Zahl ist die $1 = 1^2$.

Induktionsschritt: $n \rightarrow n + 1$:

Unter der Annahme, dass unsere Formel für $m = n$ gilt $\left(\sum_{k=1}^{n} 2k - 1 = n^2 \right)$ erhalten wir:

$$\sum_{k=1}^{n+1} 2k - 1 = 2(n+1) - 1 + \sum_{k=1}^{n} 2k - 1 = 2(n+1) - 1 + n^2 = 2n + 1 + n^2$$

Dank der binomischen Formeln wissen wir: $2n + 1 + n^2 = (n+1)^2$. □

Direkte Beweise

In diesem Fall wäre ein direkter Beweis einfacher:

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

$$\sum_{k=1}^{n} 2k - 1 = n^2$$

Direkte Beweise

In diesem Fall wäre ein direkter Beweis einfacher:

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

$$\sum_{k=1}^{n} 2k - 1 = n^2$$

$$\left(\sum_{k=1}^{n} 2k \right) - n = n^2$$

Direkte Beweise

In diesem Fall wäre ein direkter Beweis einfacher:

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

$$\sum_{k=1}^{n} 2k - 1 = n^2$$

$$\left(\sum_{k=1}^{n} 2k \right) - n = n^2$$

$$2 \cdot \left(\sum_{k=1}^{n} k \right) - n = n^2$$

Direkte Beweise

In diesem Fall wäre ein direkter Beweis einfacher:

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

$$\sum_{k=1}^{n} 2k - 1 = n^2$$

$$\left(\sum_{k=1}^{n} 2k\right) - n = n^2$$

$$2 \cdot \left(\sum_{k=1}^{n} k\right) - n = n^2$$

$$2 \cdot \left(\frac{n^2 + n}{2}\right) - n = n^2$$

Direkte Beweise

In diesem Fall wäre ein direkter Beweis einfacher:

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

$$\sum_{k=1}^{n} 2k - 1 = n^2$$

$$\left(\sum_{k=1}^{n} 2k\right) - n = n^2$$

$$2 \cdot \left(\sum_{k=1}^{n} k\right) - n = n^2$$

$$2 \cdot \left(\frac{n^2 + n}{2}\right) - n = n^2$$

$$n^2 + n - n = n^2$$

Direkte Beweise

In diesem Fall wäre ein direkter Beweis einfacher:

Beispiel: Die Summe über die ersten n ungeraden Zahlen ist $= n^2$. (Für $n \in \mathbb{N}$)

$$\begin{aligned}
\sum_{k=1}^{n} 2k - 1 &= n^2 \\
\left(\sum_{k=1}^{n} 2k\right) - n &= n^2 \\
2 \cdot \left(\sum_{k=1}^{n} k\right) - n &= n^2 \\
2 \cdot \left(\frac{n^2 + n}{2}\right) - n &= n^2 \\
n^2 + n - n &= n^2 \\
n^2 &= n^2
\end{aligned}$$

□

Indirekte Beweise

Indirekte Beweise sind in der Regel dann nützlich, wenn die anderen Beweisarten nicht gehen oder zu aufwendig wären.
Ein Standardbeispiel ist zu zeigen, dass $\sqrt{2}$ irrational ist. Um dies zu beweisen, nehmen wir nun zuerst das Gegenteil an: $\sqrt{2}$ ist rational:

$$\exists a, b \in \mathbb{N} : \frac{a}{b} = \sqrt{2} \text{ mit } ggT(a, b) = 1$$

Indirekte Beweise

Indirekte Beweise sind in der Regel dann nützlich, wenn die anderen Beweisarten nicht gehen oder zu aufwendig wären.
Ein Standardbeispiel ist zu zeigen, dass $\sqrt{2}$ irrational ist. Um dies zu beweisen, nehmen wir nun zuerst das Gegenteil an: $\sqrt{2}$ ist rational:

$$\exists a, b \in \mathbb{N} : \frac{a}{b} = \sqrt{2} \text{ mit } ggT(a, b) = 1$$

Damit gilt: $2 = \frac{a^2}{b^2}$ und somit $2 \cdot b^2 = a^2$.

Somit ist a^2 gerade, was bedeutet, dass auch a gerade ist. Wir können also schreiben: $a = 2n$.

Indirekte Beweise

Indirekte Beweise sind in der Regel dann nützlich, wenn die anderen Beweisarten nicht gehen oder zu aufwendig wären.
Ein Standardbeispiel ist zu zeigen, dass $\sqrt{2}$ irrational ist. Um dies zu beweisen, nehmen wir nun zuerst das Gegenteil an: $\sqrt{2}$ ist rational:

$$\exists a, b \in \mathbb{N} : \frac{a}{b} = \sqrt{2} \text{ mit } ggT(a, b) = 1$$

Damit gilt: $2 = \frac{a^2}{b^2}$ und somit $2 \cdot b^2 = a^2$.

Somit ist a^2 gerade, was bedeutet, dass auch a gerade ist. Wir können also schreiben: $a = 2n$.

$$\begin{aligned} 2 \cdot b^2 = a^2 = (2n)^2 = 4n^2 // : 2 \\ b^2 = 2n^2 \end{aligned}$$

Somit ist also auch b gerade (da b^2 gerade ist).

Indirekte Beweise

Indirekte Beweise sind in der Regel dann nützlich, wenn die anderen Beweisarten nicht gehen oder zu aufwendig wären.
Ein Standardbeispiel ist zu zeigen, dass $\sqrt{2}$ irrational ist. Um dies zu beweisen, nehmen wir nun zuerst das Gegenteil an: $\sqrt{2}$ ist rational:

$$\exists a, b \in \mathbb{N} : \frac{a}{b} = \sqrt{2} \text{ mit } ggT(a, b) = 1$$

Damit gilt: $2 = \frac{a^2}{b^2}$ und somit $2 \cdot b^2 = a^2$.

Somit ist a^2 gerade, was bedeutet, dass auch a gerade ist. Wir können also schreiben: $a = 2n$.

$$\begin{aligned} 2 \cdot b^2 = a^2 = (2n)^2 = 4n^2 // : 2 \\ b^2 = 2n^2 \end{aligned}$$

Somit ist also auch b gerade (da b^2 gerade ist). Dies würde jedoch bedeuten, dass a und b nicht teilerfremd sind ($ggT(a, b) = 1$), da mindestens 2 ein Teiler von a und b ist. Dies ist ein Widerspruch zur initialen Annahme, womit deren Gegenteil bewiesen wäre: $\sqrt{2}$ ist irrational.

□

Section 2

Gruppen

Gruppen – Gruppeneigenschaften

1. Abgeschlossenheit: $\circ : G \times G \to G$ ($(G, \circ)$ ist ein Gruppoid)
2. Assoziativität: $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$ ($(G, \circ)$ ist eine Halbgruppe)
3. Neutrales Element $\exists e \in G : \forall x \in G : x \circ e = e \circ x = x$ ($(G, \circ)$ ist ein Monoid)
4. Inverses Element: $\forall x \in G : \exists x^{-1} : x \circ x^{-1} = e$ ($(G, \circ)$ ist eine Gruppe)

Außerdem: Wenn $\forall a, b \in G : a \circ b = b \circ a$, so ist $(G, \circ)$ abelsch/ kommutativ.

Verknüpfungstafeln

Eine Verknüpfungstafel stellt eine Verknüpfung $\circ : X \times Y \to Z$ dar.

$\circ$	y_1	y_2	$\dots$	y_m
x_1	$x_1 \circ y_1$	$x_1 \circ y_2$	$\dots$	$x_1 \circ y_m$
x_2	$x_2 \circ y_1$	$x_2 \circ y_2$	$\dots$	$x_2 \circ y_m$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
x_n	$x_n \circ y_1$	$x_n \circ y_2$	$\dots$	$x_n \circ y_m$

Verknüpfungstafeln

Eine Verknüpfungstafel stellt eine Verknüpfung $\circ : X \times Y \to Z$ dar.

Verknüpfung $\circ$

	Input y_1	y_2	$\dots$	y_m
Input x_1	$x_1 \circ y_1$	$x_1 \circ y_2$	$\dots$	$x_1 \circ y_m$
x_2	$x_2 \circ y_1$	$x_2 \circ y_2$	$\dots$	$x_2 \circ y_m$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
x_n	$x_n \circ y_1$	$x_n \circ y_2$	$\dots$	$x_n \circ y_m$

Output

Verknüpfungstafeln

Eine Verknüpfungstafel stellt eine Verknüpfung $\circ : X \times Y \to Z$ dar.

Verknüpfung

Input

$\circ$	y_1	y_2	$\dots$	y_m
x_1	$x_1 \circ y_1$	$x_1 \circ y_2$	$\dots$	$x_1 \circ y_m$
x_2	$x_2 \circ y_1$	$x_2 \circ y_2$	$\dots$	$x_2 \circ y_m$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
x_n	$x_n \circ y_1$	$x_n \circ y_2$	$\dots$	$x_n \circ y_m$

Input

Output

$x^2 - y$	1	2	$\dots$	8
1	0	-1	$\dots$	-7
2	3	2	$\dots$	-4
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
5	24	23	$\dots$	17

Verknüpfungstafeln

Eine Verknüpfungstafel stellt eine Verknüpfung $\circ : X \times Y \to Z$ dar.

Verknüpfung $\circ$

Input	y_1	y_2	$\dots$	y_m
x_1	$x_1 \circ y_1$	$x_1 \circ y_2$	$\dots$	$x_1 \circ y_m$
x_2	$x_2 \circ y_1$	$x_2 \circ y_2$	$\dots$	$x_2 \circ y_m$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
x_n	$x_n \circ y_1$	$x_n \circ y_2$	$\dots$	$x_n \circ y_m$

Input (oben) — Input (links) — Output

$x^2 - y$	1	2	$\dots$	8
1	0	-1	$\dots$	-7
2	3	2	$\dots$	-4
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
5	24	23	$\dots$	17

$\vee$	00	01	10	11
00	00	01	10	11
01	01	01	11	11
10	10	11	10	11
11	11	11	11	11

Verknüpfungstafeln – Gruppeneigenschaften

Anhand von Verknüpfungstafeln können wir gewisse Gruppeneigenschaften überprüfen:

Eine Verknüpfung ist **abgeschlossen**, wenn in jeder Zeile und in jeder Spalte jeder Werte $g_i \in G$ genau einmal vorkommt.

Eine Verknüpfung ist kommutativ, wenn die Verknüpfungstafel spiegelsymmetrisch bezüglich der Diagonale $((0,0)-(n,n))$ ist.

$(\mathbb{Z}_4, \circ)$	0	1	2	3
0	0	1	0	1
1	0	1	1	0
2	1	0	0	1
3	1	0	1	0

Verknüpfungstafeln – Gruppeneigenschaften

Anhand von Verknüpfungstafeln können wir gewisse Gruppeneigenschaften überprüfen:

Eine Verknüpfung ist **abgeschlossen**, wenn in jeder Zeile und in jeder Spalte jeder Werte $g_i \in G$ genau einmal vorkommt.

Eine Verknüpfung ist kommutativ, wenn die Verknüpfungstafel spiegelsymmetrisch bezüglich der Diagonale $((0,0)-(n,n))$ ist.

$(\mathbb{Z}_4, \circ)$	0	1	2	3
0	0	1	0	1
1	0	1	1	0
2	1	0	0	1
3	1	0	1	0

Weder abgeschlossen, noch kommutativ.

Verknüpfungstafeln – Gruppeneigenschaften

Anhand von Verknüpfungstafeln können wir gewisse Gruppeneigenschaften überprüfen:

Eine Verknüpfung ist **abgeschlossen**, wenn in jeder Zeile und in jeder Spalte jeder Werte $g_i \in G$ genau einmal vorkommt.

Eine Verknüpfung ist kommutativ, wenn die Verknüpfungstafel spiegelsymmetrisch bezüglich der Diagonale $((0,0)-(n,n))$ ist.

$(\mathbb{Z}_4, \circ)$	0	1	2	3
0	0	1	0	1
1	0	1	1	0
2	1	0	0	1
3	1	0	1	0

Weder abgeschlossen, noch kommutativ.

$(\mathbb{Z}_4, \diamond)$	0	1	2	3
0	1	2	3	0
1	3	0	1	2
2	2	3	0	1
3	0	1	2	3

Verknüpfungstafeln – Gruppeneigenschaften

Anhand von Verknüpfungstafeln können wir gewisse Gruppeneigenschaften überprüfen:

Eine Verknüpfung ist **abgeschlossen**, wenn in jeder Zeile und in jeder Spalte jeder Werte $g_i \in G$ genau einmal vorkommt.

Eine Verknüpfung ist kommutativ, wenn die Verknüpfungstafel spiegelsymmetrisch bezüglich der Diagonale $((0,0)-(n,n))$ ist.

$(\mathbb{Z}_4, \circ)$	0	1	2	3
0	0	1	0	1
1	0	1	1	0
2	1	0	0	1
3	1	0	1	0

Weder abgeschlossen, noch kommutativ.

$(\mathbb{Z}_4, \diamond)$	0	1	2	3
0	1	2	3	0
1	3	0	1	2
2	2	3	0	1
3	0	1	2	3

Abgeschlossen, aber nicht kommutativ.

Verknüpfungstafeln – Gruppeneigenschaften

Anhand von Verknüpfungstafeln können wir gewisse Gruppeneigenschaften überprüfen:

Eine Verknüpfung ist **abgeschlossen**, wenn in jeder Zeile und in jeder Spalte jeder Werte $g_i \in G$ genau einmal vorkommt.

Eine Verknüpfung ist kommutativ, wenn die Verknüpfungstafel spiegelsymmetrisch bezüglich der Diagonale $((0,0)-(n,n))$ ist.

$(\mathbb{Z}_4, \circ)$	0	1	2	3
0	0	1	0	1
1	0	1	1	0
2	1	0	0	1
3	1	0	1	0

Weder abgeschlossen, noch kommutativ.

$(\mathbb{Z}_4, \diamond)$	0	1	2	3
0	1	2	3	0
1	3	0	1	2
2	2	3	0	1
3	0	1	2	3

Abgeschlossen, aber nicht kommutativ.

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Verknüpfungstafeln – Gruppeneigenschaften

Anhand von Verknüpfungstafeln können wir gewisse Gruppeneigenschaften überprüfen:

Eine Verknüpfung ist **abgeschlossen**, wenn in jeder Zeile und in jeder Spalte jeder Werte $g_i \in G$ genau einmal vorkommt.

Eine Verknüpfung ist kommutativ, wenn die Verknüpfungstafel spiegelsymmetrisch bezüglich der Diagonale $((0,0)-(n,n))$ ist.

$(\mathbb{Z}_4, \circ)$	0	1	2	3
0	0	1	0	1
1	0	1	1	0
2	1	0	0	1
3	1	0	1	0

Weder abgeschlossen, noch kommutativ.

$(\mathbb{Z}_4, \diamond)$	0	1	2	3
0	1	2	3	0
1	3	0	1	2
2	2	3	0	1
3	0	1	2	3

Abgeschlossen, aber nicht kommutativ.

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Sowohl abgeschlossen, als auch kommutativ.

Verknüpfungstafeln – Gruppeneigenschaften

Anhand von Verknüpfungstafeln können wir gewisse Gruppeneigenschaften überprüfen:

Eine Verknüpfung ist **abgeschlossen**, wenn in jeder Zeile und in jeder Spalte jeder Werte $g_i \in G$ genau einmal vorkommt.

Eine Verknüpfung ist kommutativ, wenn die Verknüpfungstafel spiegelsymmetrisch bezüglich der Diagonale $((0,0)-(n,n))$ ist.

$(\mathbb{Z}_4, \circ)$	0	1	2	3
0	0	1	0	1
1	0	1	1	0
2	1	0	0	1
3	1	0	1	0

Weder abgeschlossen, noch kommutativ.

$(\mathbb{Z}_4, \diamond)$	0	1	2	3
0	1	2	3	0
1	3	0	1	2
2	2	3	0	1
3	0	1	2	3

Abgeschlossen, aber nicht kommutativ.

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Sowohl abgeschlossen, als auch kommutativ.

Gruppen – Inverse Elemente

Damit ein Monoid $(G, \circ)$ eine Gruppe ist, muss jedes Element des Monoids ein Inverses Element haben:

$$\forall x \in G : \exists x^{-1} : x \circ x^{-1} = e$$

Beispiele:

$(\mathbb{Z}_n, +)$ $\forall x \in G : x^{-1} = n - x \bmod n$ Warum?
$\rightarrow x + x^{-1} \equiv x + n - x \equiv n \equiv 0 (\mathrm{mod} n)$

$(\mathbb{Z}_n^*, \cdot)$ Wie berechnen wir hier das Inverse von x? $\frac{1}{x}$ ist nicht in $\mathbb{Z}_n^*$ enthalten.

Gruppen – Der Erweiterte Euklidische Algorithmus (xggT)

Wir wollen das multiplikative Inverse $x^{-}1$ von x in $\mathbb{Z}_n^*$ berechnen. Dies können wir effizient durch xggT(x,n) tun.
Beispiel: xggT(113, 5):

a	b	$r = a \bmod b$	$z = a$ div b	d	x	y
113	5	3	22			

Gruppen – Der Erweiterte Euklidische Algorithmus (xggT)

Wir wollen das multiplikative Inverse $x^{-}1$ von x in $\mathbb{Z}_n^*$ berechnen. Dies können wir effizient durch xggT(x,n) tun.
Beispiel: xggT$(113, 5)$:

a	b	$r = a \bmod b$	$z = a$ div b	d	x	y
113	5	3	22			
5	3	2	1			

Gruppen – Der Erweiterte Euklidische Algorithmus (xggT)

Wir wollen das multiplikative Inverse $x^{-}1$ von x in $\mathbb{Z}_n^*$ berechnen. Dies können wir effizient durch xggT(x,n) tun.
Beispiel: xggT$(113, 5)$:

a	b	$r = a \bmod b$	$z = a$ div b	d	x	y
113	5	3	22			
5	3	2	1			
3	2	1	1			

Gruppen – Der Erweiterte Euklidische Algorithmus (xggT)

Wir wollen das multiplikative Inverse $x^{-}1$ von x in $\mathbb{Z}_n^*$ berechnen. Dies können wir effizient durch xggT(x,n) tun.
Beispiel: xggT(113, 5):

a	b	$r = a \bmod b$	$z = a$ div b	d	x	y
113	5	3	22			
5	3	2	1			
3	2	1	1			
2	1	0	2			

In jeder neuen Zeile gilt: $a = b$ (b aus vorheriger Zeile) und $b = r$ (r aus vorheriger Zeile).
Der größte gemeinsame Teiler ist also 1. Wenn $ggT \neq 1$, gibt es kein multiplikatives Inverses!

Gruppen – Der Erweiterte Euklidische Algorithmus (xggT)

Wir wollen das multiplikative Inverse $x^{-}1$ von x in $\mathbb{Z}_n^*$ berechnen. Dies können wir effizient durch xggT(x,n) tun.
Beispiel: xggT(113, 5):

a	b	$r = a \bmod b$	$z = a$ div b	d	x	y
113	5	3	22			
5	3	2	1			
3	2	1	1			
2	1	0	2	1	0	1

In jeder neuen Zeile gilt: $a = b$ (b aus vorheriger Zeile) und $b = r$ (r aus vorheriger Zeile).
Der größte gemeinsame Teiler ist also 1. Wenn $ggT \neq 1$, gibt es kein multiplikatives Inverses!
Nun beginnen wir den zweiten Teil der Tabelle von unten nach oben zu füllen. Dafür füllen wir die letzte Zeile mit $1, 0, 1$.

Gruppen – Der Erweiterte Euklidische Algorithmus (xggT)

Wir wollen das multiplikative Inverse $x^{-}1$ von x in $\mathbb{Z}_n^*$ berechnen. Dies können wir effizient durch xggT(x,n) tun.
Beispiel: xggT(113, 5):

a	b	$r = a \bmod b$	$z = a$ div b	d	x	y
113	5	3	22			
5	3	2	1			
3	2	1	1	1	1	-1
2	1	0	2	1	0	1

In jeder neuen Zeile gilt: $a = b$ (b aus vorheriger Zeile) und $b = r$ (r aus vorheriger Zeile).
Der größte gemeinsame Teiler ist also 1. Wenn $ggT \neq 1$, gibt es kein multiplikatives Inverses!
Nun beginnen wir den zweiten Teil der Tabelle von unten nach oben zu füllen. Dafür füllen wir die letzte Zeile mit $1, 0, 1$.
$d =$ ggT(a,b), $\quad x_{neu} = y, \quad y_{neu} = x - zy$. x, y aus Zeile darunter, z aus aktueller.

Gruppen – Der Erweiterte Euklidische Algorithmus (xggT)

Wir wollen das multiplikative Inverse $x^{-}1$ von x in $\mathbb{Z}_n^*$ berechnen. Dies können wir effizient durch xggT(x,n) tun.
Beispiel: xggT(113, 5):

a	b	$r = a \bmod b$	$z = a$ div b	d	x	y
113	5	3	22			
5	3	2	1	1	-1	2
3	2	1	1	1	1	-1
2	1	0	2	1	0	1

In jeder neuen Zeile gilt: $a = b$ (b aus vorheriger Zeile) und $b = r$ (r aus vorheriger Zeile).
Der größte gemeinsame Teiler ist also 1. Wenn $ggT \neq 1$, gibt es kein multiplikatives Inverses!
Nun beginnen wir den zweiten Teil der Tabelle von unten nach oben zu füllen. Dafür füllen wir die letzte Zeile mit $1, 0, 1$.
$d =$ ggT(a,b), $\quad x_{neu} = y, \quad y_{neu} = x - zy$. x, y aus Zeile darunter, z aus aktueller.

Gruppen – Der Erweiterte Euklidische Algorithmus (xggT)

Wir wollen das multiplikative Inverse $x^{-}1$ von x in $\mathbb{Z}_n^*$ berechnen. Dies können wir effizient durch xggT(x,n) tun.
Beispiel: xggT(113, 5):

a	b	$r = a \bmod b$	$z = a$ div b	d	x	y
113	5	3	22	1	2	-45
5	3	2	1	1	-1	2
3	2	1	1	1	1	-1
2	1	0	2	1	0	1

In jeder neuen Zeile gilt: $a = b$ (b aus vorheriger Zeile) und $b = r$ (r aus vorheriger Zeile).
Der größte gemeinsame Teiler ist also 1. Wenn $ggT \neq 1$, gibt es kein multiplikatives Inverses!
Nun beginnen wir den zweiten Teil der Tabelle von unten nach oben zu füllen. Dafür füllen wir die letzte Zeile mit $1, 0, 1$.
$d =$ ggT(a,b), $\quad x_{neu} = y, \quad y_{neu} = x - zy$. x, y aus Zeile darunter, z aus aktueller.

Das multiplikative Inverse von $x = 5$ in $\mathbb{Z}_{113}^*$ ist also $x^{-1} \equiv -45 \equiv 68 (\mathrm{mod} 113)$

Test: $68 \cdot 5 \equiv 340 \equiv 1 \bmod 113 \qquad //(3 \cdot 113 = 339)$

Gruppen – Anwendung: RSA

RSA ist ein asymmetrisches Verschlüsselungssystem. Die Idee ist, dass mit einem öffentlichen Schlüssel e verschlüsselt wird, und mit einem geheimen Schlüssel d entschlüsselt.
Dazu werden zwei geheime Primzahlen p und q gewählt, aus denen $n = p \cdot q$ berechnet wird. Nun wird der öffentliche Schlüssel e gewählt. Dieser muss teilerfremd zu $\varphi(n) = (p-1) \cdot (q-1)$ sein. Denn es gilt: $x^y \bmod n = x^{y \bmod \varphi(n)} \bmod n$. Wären e und $\varphi(n)$ also nicht teilerfremd, so hätte e kein multiplikatives Inverse. Eben dieses ist jedoch unser geheimer Schlüssel d.

Verschlüsselung mit RSA: $y \equiv x^e \bmod n$
Entschlüsselung mit RSA: $x \equiv y^d \equiv x^{e^d} \equiv x^{e \cdot d} \equiv x^{e \cdot e^{-1} \bmod \varphi(n)} \equiv x (\mathrm{mod} n)$
Schlüsselgenerierung:

geheim: $p, q \in \mathbb{P}, \quad d = e^{-1} \bmod \varphi(n)$

öffentlich: $n = p \cdot q, \quad e = d^{-1} \bmod \varphi(n)$

Gruppen – Symmetrische Gruppen S_n

S_n ist die Menge aller Permutationen über $\{1, \ldots, n\}$ $(n \in \mathbb{N})$
Die Verknüpfung bildet hierbei das Hintereinanderausführen:

$$(a \circ b)(x) = a(b(x))$$

S_n ist immer eine Gruppe:

Abgeschlossenheit: Da alle Elemente von S_n Permutationen $\{1, \ldots, n\}$ sind, ist auch das Verknüpfen beliebig vieler Elemente von S_n eine Permutation.

Halbgruppe: $((a \circ b) \circ c)(x) = (a \circ (b \circ c))(x) = a(b(c(x)))$

Neutrales Element: Die Identität $(\{1, \ldots, n\})$

Inverses Element: Da alle möglichen Permutationen über $\{1, \ldots, n\}$ in S_n enthalten sind, muss es für jede Permutation π auch die Inverse geben.

Gruppen – Symmetrische Gruppen S_n

Anmerkung zu den Inversen am Beispiel von S_5:
Wir suchen das Inverse einer zufälligen Permutation $\pi \in S_5$. Angenommen $\pi = \{3, 1, 4, 5, 2\}$. Dann ist das Inverse $\pi^{-1} = \{p_1, p_2, p_3, p_4, p_5\}$. p_i ist der jeweilige Index (beginnend bei 1), wo i in π steht, also:

$$\pi^{-1} = \{2, 5, 1, 3, 4\}$$

Gruppen – Symmetrische Gruppen S_n

Anmerkung zu den Inversen am Beispiel von S_5:
Wir suchen das Inverse einer zufälligen Permutation $\pi \in S_5$. Angenommen $\pi = \{3, 1, 4, 5, 2\}$. Dann ist das Inverse $\pi^{-1} = \{p_1, p_2, p_3, p_4, p_5\}$. p_i ist der jeweilige Index (beginnend bei 1), wo i in π steht, also:

$$\pi^{-1} = \{2, 5, 1, 3, 4\}$$

Test:

x	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(x))$
1	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(1)) = \{3,1,4,5,2\}(2) = 1$
2	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(2)) = \{3,1,4,5,2\}(5) = 2$
3	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(3)) = \{3,1,4,5,2\}(1) = 3$
4	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(4)) = \{3,1,4,5,2\}(3) = 4$
5	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(5)) = \{3,1,4,5,2\}(4) = 5$

Gruppen – Symmetrische Gruppen S_n

Anmerkung zu den Inversen am Beispiel von S_5:
Wir suchen das Inverse einer zufälligen Permutation $\pi \in S_5$. Angenommen $\pi = \{3, 1, 4, 5, 2\}$. Dann ist das Inverse $\pi^{-1} = \{p_1, p_2, p_3, p_4, p_5\}$. p_i ist der jeweilige Index (beginnend bei 1), wo i in π steht, also:

$$\pi^{-1} = \{2, 5, 1, 3, 4\}$$

Test:

x	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(x))$
1	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(1)) = \{3,1,4,5,2\}(2) = 1$
2	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(2)) = \{3,1,4,5,2\}(5) = 2$
3	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(3)) = \{3,1,4,5,2\}(1) = 3$
4	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(4)) = \{3,1,4,5,2\}(3) = 4$
5	$\{3,1,4,5,2\}(\{2,5,1,3,4\}(5)) = \{3,1,4,5,2\}(4) = 5$

Oder man gibt π^{-1} nacheinander in π und erhält:

$$\{3, 1, 4, 5, 2\}(\{2, 5, 1, 3, 4\}) = \{1, 2, 3, 4, 5\}$$

Gruppen – Zyklische Gruppen

Eine Gruppe $(G, \circ)$ ist zyklisch, wenn sie einen Generator hat.
Das heißt, wenn es ein $g \in G$ gibt, mit dem man alle anderen Elemente der Gruppe erzeugen kann ($G = \{g^z | z \in \mathbb{Z}\}$).
Zyklische Gruppen sind immer kommutativ.

Gruppen – Zyklische Gruppen

Beispiele:

$(\mathbb{Z}_n, +)$ Generatoren?

Gruppen – Zyklische Gruppen

Beispiele:

$(\mathbb{Z}_n, +)$ Generatoren? Abhängig von n, aber auf jeden Fall 1.

$(\mathbb{Z}_{13} \setminus \{0\}, \cdot)$ Generatoren?

Gruppen – Zyklische Gruppen

Beispiele:

$(\mathbb{Z}_n, +)$ Generatoren? Abhängig von n, aber auf jeden Fall 1.

$(\mathbb{Z}_{13} \setminus \{0\}, \cdot)$ Generatoren?

$$< 1 > = \{1\}, \text{ kein Generator}$$
$$< 2 > = \{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}, \text{ Generator}$$
$$< 3 > = \{3, 9, 1\}, \text{ kein Generator}$$
$$< 4 > = \{4, 3, 12, 9, 10, 1\}, \text{ kein Generator}$$
$$< 5 > = \{5, 12, 8, 1\}, \text{ kein Generator}$$
$$< 6 > = \{6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1\}, \text{ Generator}$$
$$< 7 > = \{7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1\}, \text{ Generator}$$
$$< 8 > = \{8, 12, 5, 1\}, \text{ kein Generator}$$
$$< 9 > = \{9, 3, 1\}, \text{ kein Generator}$$
$$< 10 > = \{10, 9, 12, 3, 4, 1\}, \text{ kein Generator}$$
$$< 11 > = \{11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6, 1\}, \text{ Generator}$$
$$< 12 > = \{12, 1\}, \text{ kein Generator}$$

Gruppen – Isomorphie

Zwei Gruppen $(G, \circ)$ und $(H, \diamond)$ sind isomorph, falls es eine Bijektion π gibt, bezüglich derer sie sich ähnlich verhalten. *(Informeller kann ich das leider nicht ausdrücken.)*

Gruppen – Isomorphie

Zwei Gruppen $(G, \circ)$ und $(H, \diamond)$ sind isomorph, falls es eine Bijektion π gibt, bezüglich derer sie sich ähnlich verhalten. *(Informeller kann ich das leider nicht ausdrücken.)*

Formell: Die Gruppen $(G, \circ)$ und $(H, \diamond)$ sind isomorph, wenn es eine Bijektion $\pi : G \to H$ gibt, so dass gilt:

$$\forall a, b \in G : \pi(a \circ b) = \pi(a) \diamond \pi(b)$$

Beispiel $(\mathbb{R}, +)$ und $(\mathbb{R}^+, \cdot)$.

Gruppen – Isomorphie

Zwei Gruppen $(G, \circ)$ und $(H, \diamond)$ sind isomorph, falls es eine Bijektion π gibt, bezüglich derer sie sich ähnlich verhalten. *(Informeller kann ich das leider nicht ausdrücken.)*

Formell: Die Gruppen $(G, \circ)$ und $(H, \diamond)$ sind isomorph, wenn es eine Bijektion $\pi : G \to H$ gibt, so dass gilt:

$$\forall a, b \in G : \pi(a \circ b) = \pi(a) \diamond \pi(b)$$

Beispiel $(\mathbb{R}, +)$ und $(\mathbb{R}^+, \cdot)$.
Der Isomorphismus ist hier e^x:

$$e^{a+b} = e^a \cdot e^b = e^{a+b}$$

Was ist der inverse Isomorphismus?

Gruppen – Isomorphie

Zwei Gruppen $(G, \circ)$ und $(H, \diamond)$ sind isomorph, falls es eine Bijektion π gibt, bezüglich derer sie sich ähnlich verhalten. *(Informeller kann ich das leider nicht ausdrücken.)*

Formell: Die Gruppen $(G, \circ)$ und $(H, \diamond)$ sind isomorph, wenn es eine Bijektion $\pi : G \to H$ gibt, so dass gilt:

$$\forall a, b \in G : \pi(a \circ b) = \pi(a) \diamond \pi(b)$$

Beispiel $(\mathbb{R}, +)$ und $(\mathbb{R}^+, \cdot)$.
Der Isomorphismus ist hier e^x:

$$e^{a+b} = e^a \cdot e^b = e^{a+b}$$

Was ist der inverse Isomorphismus?$\to log(x)$

$$log(a \cdot b) = log(a) + log(b)$$

Gruppen – Isomorphie

Welche der beiden Funktionen ist ein Isomorphismus von $(\mathbb{Z}_4, +)$ nach $(\mathbb{Z}_5^*, \cdot)$?

$$\pi_a(x) = 3^x \bmod 5 \qquad \pi_a(x) = 4^x \bmod 5$$

Gruppen – Isomorphie

Welche der beiden Funktionen ist ein Isomorphismus von $(\mathbb{Z}_4, +)$ nach $(\mathbb{Z}_5^*, \cdot)$?

$\pi_a(x) = 3^x \bmod 5$

$3^{(a+b) \bmod 4} \bmod 5$	0	1	2	3
0	1	3	4	2
1	3	4	2	1
2	4	2	3	2
3	2	1	3	4

$\pi_a(x) = 4^x \bmod 5$

$4^{(a+b) \bmod 4} \bmod 5$	0	1	2	3
0	1	4	1	4
1	4	1	4	1
2	1	4	1	4
3	4	1	4	1

$((3^a \cdot 3^b) \bmod 5) \bmod 5$	0	1	2	3
0	1	3	4	2
1	3	4	2	1
2	4	2	3	2
3	2	1	3	4

$((4^a \cdot 4^b) \bmod 5) \bmod 5$	0	1	2	3
0	1	4	1	4
1	4	1	4	1
2	1	4	1	4
3	4	1	4	1

Gruppen – Isomorphie

Welche der beiden Funktionen ist ein Isomorphismus von $(\mathbb{Z}_4, +)$ nach $(\mathbb{Z}_5^*, \cdot)$?

$\pi_a(x) = 3^x \bmod 5$

$3^{(a+b) \bmod 4} \bmod 5$	0	1	2	3
0	1	3	4	2
1	3	4	2	1
2	4	2	3	2
3	2	1	3	4

$\pi_a(x) = 4^x \bmod 5$

$4^{(a+b) \bmod 4} \bmod 5$	0	1	2	3
0	1	4	1	4
1	4	1	4	1
2	1	4	1	4
3	4	1	4	1

$((3^a \cdot 3^b) \bmod 5) \bmod 5$	0	1	2	3
0	1	3	4	2
1	3	4	2	1
2	4	2	3	2
3	2	1	3	4

$((4^a \cdot 4^b) \bmod 5) \bmod 5$	0	1	2	3
0	1	4	1	4
1	4	1	4	1
2	1	4	1	4
3	4	1	4	1

Ein Isomorphismus muss bijektiv sein. Damit ist π_b kein Isomorphismus!

Section 3

Rest

k-glatte Zahlen

Eine Zahl heißt k-glatt, wenn für alle ihre Primfaktoren p_i gilt: $p_i \leq k$.

k-glatte Zahlen

Eine Zahl heißt k-glatt, wenn für alle ihre Primfaktoren p_i gilt: $p_i \leq k$.
Beispiele:
$15 =$

k-glatte Zahlen

Eine Zahl heißt k-glatt, wenn für alle ihre Primfaktoren p_i gilt: $p_i \leq k$.
Beispiele:
$15 = 3 \cdot 5. \rightarrow 15$ ist also 5-glatt.

k-glatte Zahlen

Eine Zahl heißt k-glatt, wenn für alle ihre Primfaktoren p_i gilt: $p_i \leq k$.
Beispiele:
$15 = 3 \cdot 5. \rightarrow 15$ ist also 5-glatt.
$14 =$

k-glatte Zahlen

Eine Zahl heißt k-glatt, wenn für alle ihre Primfaktoren p_i gilt: $p_i \leq k$.
Beispiele:
$15 = 3 \cdot 5. \rightarrow 15$ ist also 5-glatt.
$14 = 2 \cdot 7. \rightarrow 14$ ist also 7-glatt, nicht aber 5-glatt.

k-glatte Zahlen

Eine Zahl heißt k-glatt, wenn für alle ihre Primfaktoren p_i gilt: $p_i \leq k$.
Beispiele:
$15 = 3 \cdot 5. \rightarrow 15$ ist also 5-glatt.
$14 = 2 \cdot 7. \rightarrow 14$ ist also 7-glatt, nicht aber 5-glatt.
$1024 =$

k-glatte Zahlen

Eine Zahl heißt k-glatt, wenn für alle ihre Primfaktoren p_i gilt: $p_i \leq k$.
Beispiele:
$15 = 3 \cdot 5. \rightarrow 15$ ist also 5-glatt.
$14 = 2 \cdot 7. \rightarrow 14$ ist also 7-glatt, nicht aber 5-glatt.
$1024 = 2^{10}. \rightarrow 1024$ ist also 2-glatt.

k-glatte Zahlen

Eine Zahl heißt k-glatt, wenn für alle ihre Primfaktoren p_i gilt: $p_i \leq k$.
Beispiele:
$15 = 3 \cdot 5. \rightarrow 15$ ist also 5-glatt.
$14 = 2 \cdot 7. \rightarrow 14$ ist also 7-glatt, nicht aber 5-glatt.
$1024 = 2^{10}. \rightarrow 1024$ ist also 2-glatt.
$3072 =$

k-glatte Zahlen

Eine Zahl heißt k-glatt, wenn für alle ihre Primfaktoren p_i gilt: $p_i \leq k$.
Beispiele:
$15 = 3 \cdot 5. \rightarrow 15$ ist also 5-glatt.
$14 = 2 \cdot 7. \rightarrow 14$ ist also 7-glatt, nicht aber 5-glatt.
$1024 = 2^{10}. \rightarrow 1024$ ist also 2-glatt.
$3072 = 2^{10} \cdot 3. \rightarrow 3072$ ist also 3-glatt.

CRC - Prüfsummen

CRC Prüfsummen sind eine weit verbreitete Methode um Übertragungs- oder Speicherfehler zu erkennen. Hierfür wird ein Polynom aus $\mathbb{Z}_2$[x] vom Grad n benötigt. Um eine s-bit lange Nachricht zu übertragen benötigen wir $s + n$ Bits $(c_{s+n-1}, \ldots, c_0)$.
Prüfsumme erzeugen:

1. Wir schreiben unsere Nachricht in die Bits $(c_{s+n-1}, \ldots, c_n)$
2. Die Bits der Prüfsumme $(c_{n-i}, \ldots c_0)$ füllen wir zuerst mit 0.
3. Nun teilen wir unsere temporäre Nachricht (C') durch das Polynom. Der Rest dieser Division ist unsere Prüfsumme und wir schreiben sie in $(c_{n-1}, \ldots, c_0)$.

Beispiel: Nachricht = 101101, Polynom $P = x^3 + x + 1 = 1011$

$C' = 101101\_\_\_$

$C' = 101101000$

101101000 / 1011 = 100001
Rest 011
$C = 101101011$

CRC - Prüfsummen

Gegeben $P = 1011, \quad C = 101101011$

Überprüfen der Korrektheit:
Wir teilen die Empfangene Nachricht C durch P. Wenn wir einen Rest erhalten, so liegt ein Fehler vor. Erhalten wir keinen Rest, so gehen wir davon aus, dass kein Fehler aufgetreten ist.
Korrekte Übertragung:
101101011 / 1011 = 100001 Rest 0 $\rightarrow$ kein Fehler

CRC - Prüfsummen

Gegeben $P = 1011$, $C = 101101011$

Überprüfen der Korrektheit:
Wir teilen die Empfangene Nachricht C durch P. Wenn wir einen Rest erhalten, so liegt ein Fehler vor. Erhalten wir keinen Rest, so gehen wir davon aus, dass kein Fehler aufgetreten ist.
Korrekte Übertragung:
101101011 / 1011 = 100001 Rest 0 $\rightarrow$ kein Fehler

Fehlerhafte Übertragung im dritten Bit:
101101111 / 1011 = 100001 Rest 100 $\rightarrow$ Fehler

CRC - Prüfsummen

Gegeben $P = 1011$, $C = 101101011$

Überprüfen der Korrektheit:
Wir teilen die Empfangene Nachricht C durch P. Wenn wir einen Rest erhalten, so liegt ein Fehler vor. Erhalten wir keinen Rest, so gehen wir davon aus, dass kein Fehler aufgetreten ist.
Korrekte Übertragung:
101101011 / 1011 = 100001 Rest 0 $\rightarrow$ kein Fehler

Fehlerhafte Übertragung im dritten Bit:
101101111 / 1011 = 100001 Rest 100 $\rightarrow$ Fehler

Fehlerhafte Übertragung im 2., 3. und 5. Bit:
101111101 / 1011 = 100011 Rest 0 $\rightarrow$ kein Fehler

Wenn $C \oplus C'$ ein Vielfaches von P ist, können Fehler nicht erkannt werden!

Hinweise

Klausur: 21.09.2020 9.00 Uhr

- Bitte vorher da sein
- Corona Maßnahmen beachten
- Ein zweiseitig handbeschriebenes Blatt
- KEIN Taschenrechner!

Lest die Aufgaben sorgfältig

Überprüft eure Rechnungen

- Übt Kopf- und schriftliches Rechnen
- Erspart Schusselfehler und vorallem Zeit