2.1. Natürliche Zahlen

Die Menge

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

der natürlichen Zahlen wird formal durch die Peano–Axiome definiert:

(A1) $1 \in \mathbb{N}$

(A2) $n \in \mathbb{N} \Rightarrow (n+1) \in \mathbb{N}$

(A3) $n \neq m \Rightarrow (n+1) \neq (m+1)$

(A4) $n \in \mathbb{N} \Rightarrow (n+1) \neq 1$

(A5) Für $A \subset \mathbb{N}$ gilt das Vollständigkeitsaxiom :

$$1 \in A \wedge (\forall n : [n \in A \Rightarrow (n+1) \in A]) \Rightarrow A = \mathbb{N}$$

Bemerkung: Die Nachfolgeabbildung $n \to (n+1)$ ist eine injektiv.

Beweisprinzip der vollständigen Induktion.

Dabei ist die Gültigkeit einer Aussage $A(n)$ für alle $n \in \mathbb{N}$ zu beweisen, d.h. es ist zu zeigen

$$\forall\, n \in \mathbb{N} : A(n)$$

wobei $A(n)$ eine Aussageform ist, die von $n \in \mathbb{N}$ abhängt.

Beweisschritte der vollständigen Induktion.

(I1) Induktionsanfang: $n = 1$, d.h. zeige $A(1)$.

(I2) Induktionsannahme: Es gelte $A(n)$.

(I3) Induktionsschluss: $n \to n+1$

Zeige die Implikation $A(n) \Rightarrow A(n+1)$.

Sind (I1)-(I3) durchführbar, so gilt die Aussage $A(n)$ für alle $n \in \mathbb{N}$.

Beispiel 1 zur vollständigen Induktion I.

Bestimme die Anzahl t_n der Teilmengen einer Menge mit n Elementen,

$$A_n = \{a_1, a_2, \ldots, a_n\}$$

Vorgehen: Betrachte zunächst kleine $n \in \mathbb{N}$, z.B. $n = 1, 2, 3$.

1. $n = 1$:
   Die Menge $A_1 = \{a_1\}$ besitzt die Teilmengen $\emptyset, \{a_1\}$, d.h. $t_1 = 2$.
2. $n = 2$:
   Die Menge $A_2 = \{a_1, a_2\}$ besitzt die vier Teilmengen

   $$\emptyset, \{a_1\}, \{a_2\}, \{a_1, a_2\}$$

   und somit gilt $t_2 = 4$.
3. $n = 3$: Die Menge $A_3 = \{a_1, a_2, a_3\}$ besitzt $t_3 = 8$ Teilmengen.

Vermutung: Es gilt $t_n = 2^n$ für alle $n \in \mathbb{N}$.

Beispiel 1 zur vollständigen Induktion II.

Satz: Eine n–elementige Menge $A = \{a_1, \ldots, a_n\}$ besitzt 2^n Teilmengen.

Beweis: durch vollständige Induktion über n.

- Induktionsanfang ($n = 1$): Es gilt $t_1 = 2 = 2^1$.
- Induktionsannahme: Es gelte $t_n = 2^n$ für $n \in \mathbb{N}$.
- Induktionsschluss ($n \to n + 1$):

Zu zeigen: $A_{n+1} = \{a_1, \ldots, a_n, a_{n+1}\}$ hat 2^{n+1} Teilmengen.

Schreibe $\mathcal{P}(A_{n+1}) = K_1 \cup K_2$ für die Potenzmenge von A_{n+1}, wobei

$$T \in K_1 \iff a_{n+1} \notin T$$
$$T \in K_2 \iff a_{n+1} \in T$$

Nach Induktionsannahme besitzen K_1 und K_2 genau $t_n = 2^n$ Elemente.

Weiterhin gilt nach Konstruktion $K_1 \cap K_2 = \emptyset$.

Somit hat $\mathcal{P}(A_{n+1})$ insgesamt $t_{n+1} = t_n + t_n = 2^n + 2^n = 2^{n+1}$ Elemente.

Beispiel 2 zur vollständigen Induktion I.

Bestimme die Anzahl p_n der verschiedenen Anordnungen (Permutationen) für die Elemente einer n–elementigen Menge $A_n = \{1, 2, \ldots, n\}$

Vorgehen: Betrachte zunächst kleine $n \in \mathbb{N}$, z.B. $n = 1, 2, 3$.

1. $n = 1$:
   Das Element in $A_1 = \{1\}$ besitzt nur eine Anordnung (1), d.h. $p_1 = 1$.
2. $n = 2$: Für die Elemente in $A_2 = \{1, 2\}$ gibt es zwei Anordnungen
   $$(1, 2), (2, 1).$$
   Somit gilt $p_2 = 2$.
3. $n = 3$: Für die Elemente in $A_3 = \{1, 2, 3\}$ gibt es sechs Anordnungen
   $$(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1).$$
   Somit gilt $p_3 = 6$.

Vermutung: Es gilt $p_n = n! = 1 \cdot 2 \cdot \ldots \cdot n$ für alle $n \in \mathbb{N}$.

Beispiel 2 zur vollständigen Induktion II.

Satz: Es gibt $p_n = n!$ Permutationen für das n–Tupel $(1, 2, \ldots, n)$.

Beweis: durch vollständige Induktion über n.

- Induktionsanfang $(n = 1)$: Es gilt $p_1 = 1$.
- Induktionsannahme: Es gelte $p_n = n!$ für $n \in \mathbb{N}$.
- Induktionsschluss $(n \to n + 1)$:

Es gibt nach Induktionsannahme je $n!$ Permutationen für die $(n+1)$–Tupel

$$\left\{ \begin{array}{c} (i_1, i_2, \ldots, i_{n-1}, i_n, n+1), \\ (i_1, i_2, \ldots, i_{n-1}, n+1, i_n), \\ \vdots \\ (i_1, n+1, i_2, \ldots, i_{n-1}, i_n), \\ (n+1, i_1, i_2, \ldots, i_{n-1}, i_n) \end{array} \right\} \underbrace{i_1, \ldots, i_n}_{\text{paarweise verschieden}} \in \{1, \ldots, n\}$$

und somit gilt $p_{n+1} = \underbrace{n! + \ldots + n!}_{(n+1)-fach} = (n+1) \cdot n! = (n+1)!$.

Beispiel 2 zur vollständigen Induktion III.

Folgerung: Eine n–elementige Menge $\{a_1, \ldots, a_n\}$ besitzt genau

$$\binom{n}{m} = \frac{n!}{m!\,(n-m)!}, \quad \text{für } n, m \in \mathbb{N}_0 : 0 \leq m \leq n$$

m–elementige Teilmengen. Dabei setzt man $0! = 1$.

Klassisches Beispiel: Zahlenlotto. Es gibt

$$\binom{49}{6} = \frac{49!}{6!\,43!} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 13983816$$

Möglichkeiten, aus einer 49–elementigen Menge eine 6–elementige Teilmenge auszuwählen.
Mit anderen Worten: Die Wahrscheinlichkeit, beim (klassischen) Zahlenlotto "6 aus 49" die 6 richtigen Zahlen zu tippen, beträgt

$$\frac{1}{\binom{49}{6}} = \frac{1}{13983816} = 0.000000071511238420185 16\ldots$$

Einschub: Summen, Produkte und Potenzen I.

Definition:

Allgemeine Summen und Produkte.

$$\sum_{k=m}^{n} b_k := b_m + b_{m+1} + \cdots + b_n \quad (\text{falls } m \leq n)$$

$$\sum_{k=m}^{n} b_k := 0 \quad (\text{falls } m > n, \text{ leere Summe})$$

$$\prod_{k=m}^{n} b_k := b_m \cdot b_{m+1} \cdot \ldots \cdot b_n \quad (\text{falls } m \leq n)$$

$$\prod_{k=m}^{n} b_k := 1 \quad (\text{falls } m > n, \text{ leeres Produkt})$$

Einschub: Summen, Produkte und Potenzen II.

Definition:

Potenzen.

$$a^n := \begin{cases} \prod_{k=1}^{n} a & : \text{ für } n \geq 0 \\ 1/(a^{-n}) & : \text{ für } n < 0 \end{cases}$$

Potenzgesetze.

$$a^n \cdot a^m = a^{n+m}$$

$$(a^n)^m = a^{n \cdot m}$$

Binomialkoeffizienten und deren Eigenschaften I.

Definition:

Die (natürlichen) Zahlen $\binom{n}{m}$ nennt man Binomialkoeffizienten.

Satz:

a) Für $n, m \in \mathbb{N}$, $0 < m \leq n$, gilt die Rekursionsformel

$$\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1}$$

wobei

$$\binom{n}{0} = \binom{n}{n} = 1$$

b) Für $n \in \mathbb{N}_0$ und $a, b \in \mathbb{R}$ gilt der Binomische Lehrsatz

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Binomialkoeffizienten und deren Eigenschaften II.

Beweis zu Teil a): Es gilt $(n, m \in \mathbb{N}, 0 < m \leq n)$

$$\begin{aligned}
\binom{n}{m} + \binom{n}{m-1} &= \frac{n!}{m!\,(n-m)!} + \frac{n!}{(m-1)!\,(n-m+1)!} \\
&= \frac{n!\,(n-m+1) + n!\,m}{m!\,(n+1-m)!} \\
&= \frac{n!\,(n+1-m+m)}{m!\,(n+1-m)!} \\
&= \frac{(n+1)!}{m!\,(n+1-m)!} \\
&= \binom{n+1}{m}
\end{aligned}$$

Beweis: Binomischer Lehrsatz I.

Beweis zu Teil b): durch vollständige Induktion über n.

- Induktionsanfang ($n = 0$): Es gilt

$$(a+b)^0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix} a^0 b^0 = 1$$

- Induktionsannahme: Für $n \geq 0$ gelte

$$(a+b)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} a^k \, b^{n-k}$$

- Induktionsschluss ($n \to n+1$):

$$\begin{aligned} (a+b)^{n+1} &= (a+b)(a+b)^n \\ &= (a+b) \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} a^k \, b^{n-k} \end{aligned}$$

Beweis: Binomischer Lehrsatz II.

$$
\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}\, a^k\, b^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n}\binom{n}{k} a^k b^{n+1-k} \\
&= \sum_{j=1}^{n+1}\binom{n}{j-1} a^j b^{n+1-j} + \sum_{k=0}^{n}\binom{n}{k} a^k b^{n+1-k} \\
&= \binom{n}{0} a^0 b^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k} + \binom{n}{k-1}\right] a^k b^{n+1-k} + \binom{n}{n} a^{n+1} b^0 \\
&= \binom{n+1}{0} a^0 b^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k} a^k b^{n+1-k} + \binom{n+1}{n+1} a^{n+1} b^0 \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k} a^k b^{n+1-k}
\end{aligned}
$$

Rekursive Berechnung der Binomialkoeffizienten.

Pascalsches Dreieck

					1							
				1		1						
			1		2		1					
		1		3		3		1				
	1		4		6		4		1			
1		5		10		10		5		1		
...	...	...	...	...	...	...	...	...	...	...	...	...

Beispiel:

$$
\begin{aligned}
(a+b)^5 &= 1 \cdot a^0 b^5 + 5 \cdot a^1 b^4 + 10 \cdot a^2 b^3 + 10 \cdot a^3 b^2 + 5 \cdot a^4 b^1 + 1 \cdot a^5 b^0 \\
&= a^5 + 5a^4 b + 10a^3 b^2 + 10a^2 b^3 + 5ab^4 + b^5
\end{aligned}
$$

2.2. Primzahlen

Definition: Eine natürliche Zahl $m \in \mathbb{N}$ heißt Teiler von $n \in \mathbb{N}$, falls ein $k \in \mathbb{N}$ existiert mit

$$n = k \cdot m$$

Man schreibt dann auch $m|n$.

Jede Zahl besitzt offensichtlich die beiden Teiler 1 und n, denn es gilt stets

$$n = n \cdot 1 = 1 \cdot n$$

Existiert für $n > 1$ kein weiterer Teiler, so nennt man n eine Primzahl.
Die ersten Primzahlen lauten

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Bemerkung: Es gibt unendliche viele Primzahlen.

Hauptsatz der Zahlentheorie.

Satz: Jede natürliche Zahl $n \in \mathbb{N}$ läßt sich als Produkt von Primzahlpotenzen schreiben,

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k}$$

wobei p_j Primzahl und $r_j \in \mathbb{N}_0$ für $1 \leq j \leq k$.

Beweis: durch Induktion über n.

- Induktionsanfang ($n = 1$): Es gilt $1 = 2^0$.
- Induktionsannahme: Alle $k \leq n$ besitzen Primfaktorzerlegung.
- Induktionsschluss ($n \to n+1$):

Fall 1: Sei $n+1$ eine Primzahl. Dann gilt $n+1 = (n+1)^1$.

Fall 2: Sei $n+1$ keine Primzahl. Dann gibt es $k, m \leq n$ mit $n+1 = k \cdot m$.

Somit besitzt $n+1$ eine Primfaktorzerlegung, da k und m je eine besitzen.

Der ggT und das kgV.

Definition: Seien $n, m \in \mathbb{N}$ zwei natürliche Zahlen. Dann heißt

$$\mathrm{ggT}(n,m) := \max\{k \mid k \text{ teilt } n \text{ und } m\}$$

der größte gemeinsame Teiler (ggT) von n und m. Weiterhin heißt

$$\mathrm{kgV}(n,m) := \min\{k \mid n \text{ und } m \text{ teilen } k\}$$

das kleinste gemeinsame Vielfache (kgV) von n und m.

Beobachtung: Für

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k} \quad \text{und} \quad m = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_k^{s_k}$$

mit Primfaktoren $p1, \ldots, p_k$ und Exponenten $r_1, \ldots, r_k, s_1, \ldots, s_k \geq 0$ gilt

$$\mathrm{ggT}(n,m) = p_1^{\min(r_1,s_1)} \cdot p_2^{\min(r_2,s_2)} \cdot \ldots \cdot p_k^{\min(r_k,s_k)}$$

$$\mathrm{kgV}(n,m) = p_1^{\max(r_1,s_1)} \cdot p_2^{\max(r_2,s_2)} \cdot \ldots \cdot p_k^{\max(r_k,s_k)}$$

Beispiel zu ggT und kgV.

Beispiel: Für

$$\begin{aligned} n &= 525 = 2^0 \cdot 3^1 \cdot 5^2 \cdot 7^1 \\ m &= 180 = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^0 \end{aligned}$$

gilt

$$\begin{aligned} \mathrm{ggT}(525, 180) &= 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 15 \\ \mathrm{kgV}(525, 180) &= 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 6300 \end{aligned}$$

und

$$n \cdot m = 525 \cdot 180 = 15 \cdot 6300 = \mathrm{ggT} \cdot \mathrm{kgV}$$

Beobachtung: Für alle $n, m \in \mathbb{N}$ gilt

$$n \cdot m = \mathrm{ggT}(n, m) \cdot \mathrm{kgV}(n, m)$$

Der Euklidische Algorithmus.

Für $n, m \in \mathbb{N}$ läßt sich der ggT mit dem Verfahren der iterierten Division bestimmen.

Vorüberlegung: Zu $n, m \in \mathbb{N}$, $n \geq m$, existieren eindeutige $q, r \in \mathbb{N}_0$ mit

$$n = q \cdot m + r, \quad \text{wobei } 0 \leq r < m.$$

(Euklidischer) Algorithmus:

INPUT: $n, m \in \mathbb{N}$ mit $n \geq m$.

- Setze $r_0 = n$, $r_1 = m$ und $j = 1$;
- **REPEAT**
  - $r_{j-1} = q_j \cdot r_j + r_{j+1}$, wobei $0 \leq r_{j+1} < r_j$;
  - Setze $j = j + 1$;

  UNTIL $(r_{j+1} = 0)$

OUTPUT: $r_j = ggT(n, m)$.

Beispiel zum Algorithmus und $\mathbb{Z}$–Kombination.

Beispiel: Für $n = 3054$ und $m = 1002$ liefert der Euklidische Algorithmus:

$$\begin{aligned} 3054 &= 3 \cdot 1002 + 48 \\ 1002 &= 20 \cdot 48 + 42 \\ 48 &= 1 \cdot 42 + 6 \\ 42 &= 7 \cdot \boxed{6} + 0 \end{aligned}$$

$\Longrightarrow$ ggT(3054,1002) $= 6$, kgV(3054,1002) $= 3054 \cdot 1002/6 = 510018$.

$\mathbb{Z}$–Kombination des ggT(n, m) von n und m.

$$\begin{aligned} 6 &= 48 - 1 \cdot 42 = 48 - 1 \cdot (1002 - 20 \cdot 48) = 21 \cdot 48 - 1002 \\ &= 21 \cdot (3054 - 3 \cdot 1002) - 1002 = 21 \cdot 3054 - 64 \cdot 1002 \end{aligned}$$

Die $\mathbb{Z}$–Kombination von $n = 3054$ und $m = 1002$ ist gegeben durch

$$\text{ggT}(3054, 1002) = 6 = 21 \cdot 3054 - 64 \cdot 1002$$