Brückenkurs – Tag 4 – „Fancy Friday“

3 Binomialkoeffizienten

$k \in \mathbb{N}_0 : \binom{x}{k} = \frac{x \cdot (x-1) \cdot (x-2) \ldots (x-k+1)}{k!}$

Dabei gilt:

$$\binom{n}{0} = 1, \quad \binom{0}{0} = 1, \quad \binom{0}{k} = 0$$

Spezialfall $0 \leq k \leq n \in \mathbb{N}_0$

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \in \mathbb{Q}$$

Durch Experiment: $\in \mathbb{N}_0$

Aufgabe $\binom{x}{k} = \binom{x-1}{k-1} + \binom{x-1}{k}$ für $k \geq 1$

[Beispiel für rekursive Berechnung von $\binom{5}{3}$]

$$\binom{5}{3} = \binom{4}{2} + \binom{4}{3} = \binom{3}{1} + \binom{3}{2} + \binom{3}{2} + \binom{3}{3} = \cdots = \binom{0}{\ldots} + \cdots + \binom{0}{\ldots}$$

Satz Seien $k, n \in \mathbb{N}_0$. Dann ist die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge M durch $\binom{n}{k}$ gegeben.

Beweis mit Induktion über n $n = 0$: $M = \emptyset$. Anzahl der k-elementigen Teilmengen von $M = \begin{cases} 1 & \text{für } k = 0 \\ 0 & \text{für } k > 0 \end{cases} \overset{stimmt}{=} \binom{0}{k}$ $n \Rightarrow n+1$: Sei $M = \{a_0, a_1, \ldots, a_n\}$ $(n+1)$-elementig. Dann ist $M' := a_1, \ldots, a_n$ n-elementig.

Sei $L \subseteq M$ eine k-elementige Teilmenge. Dann ist entweder $L = a_0 \cup L'$ mit $L' \subseteq (k-1)$-elementig oder $L \subseteq M'$, k-elementig. und alle k-elementigen Teilmengen $L \subseteq M$ entstehen eindeutig auf diese Weise.

Damit ist die Anzahl der k-elementigen Teilmengen von $M \overset{IV}{=} \binom{n}{k-1} + \binom{n}{k} \overset{Aufg.}{=} \binom{n+1}{k}$

Fall $k = 0$ trivial, daher $k > 0$.

q.e.d.

3.1 Anwendung

$$(x+y)^n = \Sigma_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k$$

Beispiel

$$(x+y)^2 = \binom{2}{0} x^2 y^0 + \binom{2}{1} x^1 y^1 + \binom{2}{2} x^0 y^2 = x^2 + 2xy + y^2$$

$$(x+y)^3 = \binom{3}{0} x^3 y^0 + \binom{3}{1} x^2 y^1 + \binom{3}{2} x^1 y^2 + \binom{3}{3} x^0 y^3 = x^3 + 3x^2 y + 3xy^2 + y^3$$

Begründung

$$(x+y)^n = (x+y)(x+y)\ldots(x+y) = \Sigma n\text{-fache Produkte} = \Sigma_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Verständnisfrage: Was ist $\Sigma_{k=0}^{n} \binom{n}{k}$? $= |P(M)| = 2^n =$ Anzahl der Teilmengen einer n-elementigen Menge

4 Der euklidische Algorithmus

Im Folgenden: $d, n \in \mathbb{N}_0$

4.1 Definition

Die Zahl d **teilt** n, geschrieben $d|n$, falls $n = b \cdot d$ für ein $b \in \mathbb{Z}$.

Beispiele $2|100$, $11|165$, $-13|169$, 5X21.

4.2 Regeln

1. $1|n,\ n|n,\ d|0$
2. $0|d \implies d = 0,\ d|1 \implies d = \pm 1$
3. $d|n, n|m \implies d|m$
4. $d|a, d|b \implies d|(ax + bx)$ für alle $x, y \in \mathbb{Z}$
5. $bd|bn,\ b \neq 0 \implies d|n$
6. $d|n,\ n \neq 0 \implies |d| \leq |n|$ Jedes $n \neq 0$ hat nur endlich viele Teiler; insbesondere 1.
7. $d|n,\ n|d \implies d = \pm n$

Beweis von 4. Es gelte also $d|a, d|b$ d.h. $a = sd, b = td$ für $s, t \in \mathbb{Z}$ Damit ist $ax+by = sdx+tdy = (sx+ty)\cdot d$, also $d|ax + by$

Konsequenz Aus diesen Regeln ergibt sich, dass jede Zahl endlich viele Teiler hat, also haben je zwei $a, b \in \mathbb{Z}$ einen größten gemeinsamen Teiler, $ggT(a, b)$, wobei $ggT(0, 0) := 0$.

Es gilt

- $ggT(a, b)|a,\ \ ggT(a, b)|b.$
- $d|a,\ \ d|b \implies d|ggT(a, b).$

Beispiel $ggT(11, 14) = 1,\ ggT(21, 14) = 7,\ ggT(110, 140) = 10,\ ggT(210, 140) = 70.$

4.3 Satz: Division mit Rest

$a, b \in \mathbb{Z}$, $b \neq 0$. Dann existieren eindeutige $q, r \in \mathbb{Z}$ mit $a = bq + r$ mit $0 \leq r < |b|$.

Beweis $R = \{a - bq \mid q \in \mathbb{Z}\} \cap \mathbb{N}_0$ ist nicht leer. Diese besitzt ein kleinstes Element, welches das gesuchte $r = a - bq$ für das gewünschte q ist.
Bleibt zu zeigen: $r < |b|$. Dies folgt aus der Minimalität von $r \in R$.
q.e.d.

Folgerung Seien $a, b \in \mathbb{Z}$, $d = ggT(a, b)$. Dann $(d) := \{d \cdot n \in \mathbb{Z}\} = \{ax + by|x, y \in \mathbb{Z}\} =: (a, b)$.
Insbesondere läßt sich d in der Form $d = ax + by$ für gewisse $x, y \in \mathbb{Z}$ schreiben. (Beispiel: $ggT(9, 6) = 3 = 9 \cdot 1 + 6 \cdot (-1)$)

Beweis „$\supseteq$“ $ax + by \in (d) \Leftrightarrow d|(ax + by)$ (wg. 4. und $d|a$, $d|b$)
„$\subseteq$“ Es reicht zu zeigen, dass $d \in (a, b)$. Der Fall $a = 0$ ist einfach: Also sei $a \neq 0$.
Die Menge $M := ax + by|x, y \in \mathbb{Z} \cap \mathbb{N}_{\geq 1}$ ist nicht leer; damit besitzt sie ein kleinstes Element $m \geq 1$. Wir wissen schon (4.), dass $d|m$. Division mit Rest liefert $a = mq + r,\ 0 \leq r < m$.

Annahme $r > 0$. Dann ist $r = a - mq \in M$ **! Widerspruch !** Also $r = 0$, also $a = mq$, daher $m|a$.
Analog (mit b anstelle von a) erhalten wir $m|b$, also ist m gemeinsamer Teiler von a und b. Damit $m \leq d$. Zusammen mit $d \leq m$ folgt $d = m$. Somit $d \in (a, b)$.
$m \mid a, m \mid b \overset{iv}{\implies} m \mid ggT(a, b)$ □

4.4 Praktische Bestimmung des ggT

$$\begin{array}{rcrcrcr} 117 & = & 3 & \cdot & 33 & + & 18 \\ 33 & = & 1 & \cdot & 18 & + & 15 \\ 18 & = & 1 & \cdot & 15 & + & 3 \\ 15 & = & 5 & \cdot & 3 & + & 0 \end{array}$$

Verbleibende Zahl $3 = ggT(117, 33)$.

4.5 Satz über den euklidischen Algorithmus

Seien $a, b \in \mathbb{N}_0$, $a \geq b \neq 0$.

$$\begin{array}{rcrcrcl}
a & = & q_1 & \cdot & b & + & r_1 \quad 0 \leq r_1 < b \\
b & = & q_2 & \cdot & r_1 & + & r_1 \quad 0 \leq r_2 < r_1 \\
r_1 & = & q_3 & \cdot & r_2 & + & r_1 \quad 0 \leq r_3 < r_2 \\
 & & & & \vdots & & \\
r_{n-2} & = & q_n & \cdot & r_{n-1} & + & r_1 \quad 0 \leq r_1 < b \\
r_{n-1} & = & q_{n+1} & \cdot & r_n & + & 0
\end{array}$$

5 Primzahlen

5.1 Definition

Ein $p \in \mathbb{N}_0$ heißt **Primzahl**, wenn sie genau zwei positive Teiler besitzt.

5.2 Lemma von Euklid

Seien p eine Primzahl, $a, b \in \mathbb{Z}$. Dann: $p \,|\, (a \cdot b) \implies p \,|\, a \wedge p \,|\, b$

5.2.1 Beweis

Sei $d = ggT(p, a)$. Dann $d|p$. Nach Voraussetzung ist dann $d = 1$ oder $d = p$.

Fall 1: $d = p$ Dann $p|a$, da $p = ggT(p, a)$.

Fall 2: $d = 1$ Damit ist $1 = px + ay$ mit $x, y \in \mathbb{Z}$.
$\overset{b}{\implies} b = bpx + aby \overset{p|ab}{\implies} p|b$
□

5.3 Fundamentalsatz der Arithmetik

Satz Jede natürliche Zahl $n \geq 1$ besitzt eine eindeutige Primfaktorzerlegung („PFZ“), d.h. es existieren eindeutig bestimmte Zahlen $\nu_p(n) \in \mathbb{N}_0$ mit

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$$

Beispiel $60 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0 \ldots$ hier bspw.: $\nu_3(60) = 1$

Beweis

Existenz Sei $M = \{n \in \mathbb{N} \text{ mit } n \geq 1 \text{ ohne } PFZ\}$. Zu zeigen: $M = \emptyset$. Sei $n \in M$.
Dann ist jedenfalls n keine Primzahl, also existieren $2 \leq a, b < n$ mit $n = ab$. Damit muss $a \in M \vee b \in M$. Insbesondere ist n in M nicht kleinstes Element.
Also hat M kein kleinstes Element und $M = \emptyset$.

Eindeutigkeit Sei $n = p_1 \cdot p_2 \ldots p_r = q_1 \cdot q_2 \ldots q_s$ mit p_i, q_j Primzahlen.
$p_1 \,|\, p_1 \ldots p_r \implies p_1 \,|\, q_1 \ldots q_s \overset{Euklid}{\implies} p_1 \,|\, q_j$ für ein j. Da p_1, q_j Primzahlen $\implies p_1 = q_j$. Dann kürze mit $p_1 (= q_j)$ und mache mit p_2 weiter, ...