**Binomialkoeffizient**

**1) Induktive Definition**

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

$$\binom{0}{k+1} = 0$$

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

| $k$ \ $n$ | 0 | 1 | 2 | 3 | 4 | 5 | ... |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | ... |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | ... |
| 2 | 0 | 0 | 1 | 3 | 6 | 10 | ... |
| 3 | 0 | 0 | 0 | 1 | 4 | 10 | ... |
| 4 | 0 | 0 | 0 | 0 | 1 | 5 | ... |
| 5 | 0 | 0 | 0 | 0 | 0 | 1 | ... |

⇒ **Pascalsches Dreieck** (Blaise Pascal, 1623 – 1662)

```
                    1
                  1   1
                1   2   1
              1   3   3   1
            1   4   6   4   1
          1   5  10  10   5   1
```

Anwendung:
$(a + b)^0 = 1$
$(a + b)^1 = a + b$
$(a + b)^2 = a^2 + 2ab + b^2$
$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
...
**Binomischer Lehrsatz** (Bolzano 1816)
Für alle natürlichen Zahlen $n$ gilt $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$.

**2) Inhaltliche Interpretation (implizite Definition)**
$\binom{n}{k}$ := Anzahl der Möglichkeiten, aus einer Menge mit $n$ Elementen $k$-elementige Teilmengen zu bilden (Anordnung spielt also keine Rolle).
Beispiel: $M = \{a, b, c, d, e\}$, $k = 2$, $|M| = n = 5$.
Es gibt dann also $\binom{5}{2} = 10$ zweielementige Teilmengen, nämlich $\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{a, e\}$, $\{b, c\}$, $\{b, d\}$, $\{b, e\}$, $\{c, d\}$, $\{c, e\}$, $\{d, e\}$.

Zusammenhang zur induktiven Definition:

$\binom{n}{0}$ = Anzahl der Möglichkeiten, aus einer Menge mit $n$ Elementen die Leeremenge (0 Elemente) zu bilden = 1;

$\binom{0}{k+1}$ = Anzahl der Möglichkeiten, aus der Leerenmenge ($k$ + 1)-elementige Mengen zu bilden = 0;

$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$; $M = \{a, b, c, d, e, x\}$, $k + 1 = 3$, $|M| = n + 1 = 6$;

1. Fall: man wählt bei den $k + 1 = 3$ Elementen das $x$ mit aus, dann hat man noch $\binom{n}{k}$ Auswahlmöglichkeiten;
2. Fall: man wählt das $x$ nicht mit aus, dann muss man aus den $n$ Elementen $k + 1$ (also $\binom{n}{k+1}$ Möglichkeiten) Elemente auswählen.

**3) Explizite Definition**

$$\binom{n}{k} = \frac{n!}{(n-k)!*k!} = \frac{(n-k+1)*(n-k+2)*...*n}{1*2*3*...*k}$$ , wobei

$n!$ = 1 * 2 * 3 * ... * $n$ = Anzahl aller Permutationen von $n$ Elementen
= Anzahl aller 1-1-Abbildungen von $M$ auf sich ($|M| = n$).
(Reihenfolge spielt jetzt eine Rolle)

inhaltlich:

Zähler = Anzahl aller Auswahlmöglichkeiten von $k$ Elementen mit Berücksichtigung der Reihenfolge;

Nenner = Anzahl aller Permutationen von $k$ Elementen.

Beispiel: $\binom{17}{5} = \frac{17!}{12!5!} = \frac{13 \cdot 14 \cdot 15 \cdot 16 \cdot 17}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 6188$

### 3.1.8 Der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache

Zu zwei natürlichen Zahlen $m$, $n$ ($n \neq 0$) existieren genau zwei natürliche Zahlen $q$ und $r$, so dass $\boldsymbol{m = q * n + r}$ und $\boldsymbol{0 \leq r < n}$.

**Satz über den größten gemeinsamen Teiler**

Zu zwei natürlichen Zahlen $m$, $n$ ($n \neq 0$) existiert genau eine natürliche Zahl $d$ mit

1) $\boldsymbol{d \mid m}$ **und** $\boldsymbol{d \mid n}$ und
2) für alle $t \in$ IN gilt: ($\boldsymbol{t \mid m}$ **und** $\boldsymbol{t \mid n \Rightarrow t \mid d}$).

Bezeichnung: $\boldsymbol{d}$ **= ggT(**$\boldsymbol{m, n}$**)**

Beispiel: $m = 48$, $n = 360$

$$\left.\begin{array}{ll} 48 & = 2^4 * 3 \\ 360 & = 2^3 * 3^2 * 5 \end{array}\right\} \Rightarrow \text{ggT}(48, 360) = 2^3 * 3 = 24$$

**Definition: *m* und *n* sind teilerfremd**: $\Leftrightarrow \text{ggT}(m, n) = 1$.

Existenzbeweis: **Euklidischer Algorithmus**

$$\begin{array}{ll} m = n * q_1 + r_1 & 0 \le r_1 < n \\ n = r_1 * q_2 + r_2 & 0 \le r_2 < r_1 \\ r_1 = r_2 * q_3 + r_3 & 0 \le r_3 < r_2 \\ \vdots & \\ r_{k-2} = r_{k-1} * q_k + r_k & 0 \le r_k < r_{k-1} \\ r_{k-1} = r_k * q_{k+1} + 0 & \end{array}$$

Behauptungen:

1. Der Algorithmus bricht immer ab. (da die Reste von Schritt zu Schritt immer echt kleiner werden)
2. Der letzte von Null verschiedene Rest, also $r_k$, ist der gesuchte ggT($m$, $n$).
   Beweis:
   1) aus der letzten Zeile folgt, dass $r_k \mid r_{k-1}$, daraus und aus der vorletzten Zeile folgt, dass $r_k \mid r_{k-2}$ usw., schließlich folgt aus der 2. Zeile, dass $r_k \mid n$ und aus der 1. Zeile $r_k \mid m$.
   Mithin ist $r_k$ gemeinsamer Teiler von $m$ und $n$.

   2) Sei nun $t$ irgendein Teiler von $m$ und $n$. Dann folgt aus der ersten Zeile, dass $t$ auch ein Teiler von $r_1$ sein muss, daraus und aus der 2. Zeile folgt nun, dass $t \mid r_2$ und schließlich erhalten wir, dass $t$ auch $r_k$ teilen muss, d.h. $r_k$ ist bezüglich Teilbarkeit der größte aller gemeinsamen Teiler.

   Beispiel: $m = 444$, $n = 756$

$$\begin{array}{rl} 444 = 0 * 756 + & 444 \\ 756 = 1 * 444 + & 312 \\ 444 = 1 * 312 + & 132 \\ 312 = 2 * 132 + & 48 \\ 132 = 2 * 48 + & 36 \\ 48 = 1 * 36 + & 12 \\ 36 = 3 * 12 + & 0 \end{array}$$

   also ist ggT(444, 756) = 12

**Definition: Kleinstes gemeinsames Vielfache**
*v* ist kleinstes gemeinsames Vielfache von natürlichen Zahlen *m* und *n* genau dann, wenn
1) $\boldsymbol{m \mid v}$ **und** $\boldsymbol{n \mid v}$ und
2) für alle natürlichen Zahlen *s* gilt: $(\boldsymbol{m \mid s}$ **und** $\boldsymbol{n \mid s \Rightarrow v \mid s})$.
Bezeichnung: $v = \text{kgV}(m, n)$

Es gilt: $\boldsymbol{\text{kgV}(m, n) = \frac{m \cdot n}{ggT(m, n)}}$

Beispiel: $\text{kgV}(444, 756) = \frac{444 \cdot 756}{12} = 27972$

### 3.1.9 Die Kongruenzrelation

Seien *a*, *b* ganze Zahlen, *m* natürliche Zahl.
$\boldsymbol{a \equiv b \mod m: \Leftrightarrow m \mid (a - b)}$
$\Leftrightarrow$ *a* und *b* lassen bei Division durch *m* denselben Rest

**Eigenschaften der Kongruenzrelation**
a) Reflexivität: Für alle *a* gilt: $a \equiv a \mod m$ (weil $m \mid (a - a) = 0$).
b) Symmetrie: Aus $a \equiv b \mod m$ folgt stets $b \equiv a \mod m$.
c) Transitivität: Aus $a \equiv b \mod m$ und aus $b \equiv c \mod m$ folgt stets $a \equiv c \mod m$.

Aus a) bis c) folgt, dass die Kongruenz eine Äquivalenzrelation ist. Also zerlegt sie die natürlichen Zahlen bezüglich des Moduls *m* in Restklassen [0], [1], ..., [*m*-1].

d) Gilt $a \equiv b \mod m$ und $c \equiv d \mod m$, so ist $a + c \equiv b + d \mod m$.
e) Aus $a \equiv b \mod m$ folgt stets $a^k \equiv b^k \mod m$ für beliebiges *k* aus IN.
Beispiele für die Wirksamkeit dieser Rechengesetze:

- Welchen Rest lässt $n = 28^{64} + 11^{23}$ bei Division durch 8?
  Lösung: Es gelten folgende Kongruenzen:

  | | |
  |---|---|
  | $28 \equiv 4 \mod 8$ | $11 \equiv 3 \mod 8$ |
  | $28^2 \equiv 4^2 \mod 8$ | $11^2 \equiv 1 \mod 8$ |
  | $28^2 \equiv 0 \mod 8$ | $11^{22} \equiv 1 \mod 8$ |
  | $28^{64} \equiv 0 \mod 8$ | $11^{23} \equiv 11 \mod 8$ |
  | | $11^{23} \equiv 3 \mod 8$, |

  also gilt $n \equiv 0 + 3 = 3 \mod 8$, und damit lässt *n* bei Division durch 8 den Rest 3.

- Welchen Rest lässt $n = 23^{144} * 11^{23}$ bei Division durch 7?
  Lösung:

  | | |
  |---|---|
  | $23 \equiv 2 \mod 7$ | $11 \equiv 4 \mod 7$ |
  | $23^3 \equiv 1 \mod 7$ | $11^2 \equiv 2 \mod 7$ |
  | $23^{144} = (23^3)^{48} \equiv 1 \mod 7$ | $11^3 \equiv 1 \mod 7$ |
  | | $11^{23} = 11^{21+2} = (11^3)^7 * 11^2 \equiv 1 * 2 = 2 \mod 7$, |

  also lässt *n* bei Division durch 7 den Rest 2.