

$$m = q \cdot n + r$$

$$r = m - q \cdot n$$

Nach diesen Gleichung haben
die Paar (m, n) und (n, r)
den selben ggT.

Beispiel: Berechnung ggT(816, 294)

$$816 = 2 \cdot 294 + 228$$

$$294 = 1 \cdot 228 + 66$$

$$228 = 3 \cdot 66 + 30$$

$$66 = 2 \cdot 30 + 6$$

$$30 = 5 \cdot 6 + 0$$

Ausgabe: ggT(816, 294) = 6

Beispiel:

$$7 \bmod 5 = 2 = 12 \bmod 5$$
$$\Rightarrow 7 \text{ und } 12 \text{ sind kons.} \\ \text{mod. } 5$$

Angenommen

$$a \bmod m = b \bmod m$$

Dann ex. q_a und q_b sowie r mit

$$a = q_a \cdot m + r \quad \text{und} \quad b = q_b \cdot m + r$$

$$a - b = q_a \cdot m + r - q_b \cdot m - r \\ = q_a \cdot m - q_b \cdot m$$

$$\Rightarrow m | a - b.$$

Umgekehrt gelte $m | a - b$.

Dann ex. q_a und q_b mit

$$a = q_a \cdot m$$

Dann ex. q mit $a - b = q \cdot m$

Außerdem ex. q_a, r_a, q_b, r_b mit

$$a = q_a \cdot m + r_a, \quad b = q_b \cdot m + r_b.$$

$$m \mid a - b = q_a \cdot m + r_a - q_b \cdot m - r_b$$

$$= (q_a - q_b) \cdot m + (r_a - r_b).$$

$\Rightarrow r_a - r_b$ ist durch m teilbar.

Wissen: $0 \leq r_a, r_b < m$

$$\Rightarrow -m < r_a - r_b < m$$

$$\Rightarrow r_a - r_b = 0$$

$$\Rightarrow r_a = r_b \Rightarrow$$

$$a \bmod m = b \bmod m.$$

Beispiel: (1) $23 \equiv 8 \pmod{5}$

$$23 = 4 \cdot 5 + 3, \quad 8 = 1 \cdot 5 + 3$$

$$23 - 8 = 15 \text{ ist durch } 5 \text{ teilbar.}$$

(2) $-7 \equiv 2 \pmod{3}$

$$-7 - 2 = -9 \text{ ist durch } 3 \text{ teilbar}$$

$$-7 = -3 \cdot 3 + 2$$

$$2 = 0 \cdot 3 + 2$$

(3) $8227 \not\equiv 11 \pmod{3}$

$$8227 - 11 = 8216 \text{ ist nicht durch } 3 \text{ teilbar.}$$

Beispiel: $a = 12, m = 5$

$$[a]_m = \{ \dots, -3, 2, 7, 12, 17, \dots \}$$

Restklassen mod 5:

$$[0]_m = \{ \dots, -5, 0, 5, 10, \dots \}$$

$$[1]_m = \{ \dots, -4, 1, 6, 11, \dots \}$$

$$[2]_m = \{ \dots, -3, 2, 7, 12, \dots \}$$

$$[3]_m = \{ \dots, -2, 3, 8, 13, \dots \}$$

$$[4]_m = \{ \dots, -1, 4, 9, 14, \dots \}$$

$$[5]_m = [0]_m.$$

$$3. \quad a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}$$

$$\Rightarrow a \equiv c \pmod{m}$$

$$5. \quad a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$$

$$\Rightarrow m | a - b \wedge m | c - d.$$

$$\text{Dann gilt } m | (a + c) - (b + d)$$

$$= \underbrace{(a - b)}_{m \text{ teilt}} + \underbrace{(c - d)}_{m \text{ teilt}}$$

$$\Rightarrow a + c \equiv b + d \pmod{m}$$

Zu 6.: $\text{ggT}(c, m) = 1$,

$$c \cdot a \equiv c \cdot b \pmod{m}.$$

$$\Rightarrow m \mid c \cdot a - c \cdot b = c \cdot (a - b)$$

$$\Rightarrow m \mid a - b$$

(gilt nur, da $\text{ggT}(c, m) = 1$)

Beispiel: $8 \cdot 3 \equiv 8 \cdot 6 \pmod{6}$

aber $3 \not\equiv 6 \pmod{6}$.

Hier ist $\text{ggT}(8, 6) = 2 \neq 1$.

Beachte: $a \equiv b \pmod{m}$

$$\Rightarrow c \cdot a \equiv c \cdot b \pmod{m}$$

f.a. $c \in \mathbb{Z}$.

$$a \equiv b \pmod{m} \Rightarrow m \mid a - b$$

$$\Rightarrow m \mid c \cdot (a - b) = c \cdot a - c \cdot b$$

$$\Rightarrow c \cdot a \equiv c \cdot b \pmod{m}.$$

$$\lceil \lceil \sqrt{2} \rceil \rceil = \lceil 1,4\dots \rceil = 2$$

$$\lfloor \sqrt{2} \rfloor = \lfloor 1,4\dots \rfloor = 1$$

$$\lceil \pi \rceil = \lceil 3,14\dots \rceil = 4$$

$$\lfloor \pi \rfloor = \lfloor 3,14\dots \rfloor = 3$$

$$\lceil 1 \rceil = 1$$

$$\lfloor 2 \rfloor = 2$$

$$\lceil -\pi \rceil = \lceil -3,14\dots \rceil = -3$$

$$\lfloor -\pi \rfloor = -4$$

$$m = q \cdot n + r, \quad q = \lfloor \frac{m}{n} \rfloor$$

$$r = m - q \cdot n = m - \lfloor \frac{m}{n} \rfloor \cdot n$$

Beispiel: $M = \{1, 2, 3, 4, 5\}$

$$M_1 = \{1\}, M_2 = \{2, 4\}$$

$$M_3 = \{3, 5\}.$$

$$M_1 \cap M_2 = \emptyset = M_2 \cap M_3 = M_1 \cap M_3$$

$$|M| = 5, |M_1| = 1, |M_2| = 2 = |M_3|$$

$$5 = 1 + 2 + 2$$

$$M_1 \cup \dots \cup M_n = \bigcup_{i=1}^n M_i$$

Sind M_1, \dots, M_n disjunkt,
so gilt

$$\left| \bigcup_{i=1}^n M_i \right| = \sum_{i=1}^n |M_i|$$

$$A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) :$$

$$a_1 \in A_1 \wedge \dots \wedge a_n \in A_n\}$$

Beispiel: $A_1 = \{1, 2, 3\}$, $A_2 = \{0, 1\}$,
 $A_3 = \{a, b\}$

$$A_1 \times A_2 \times A_3 = \{(1, 0, a), (1, 0, b), \\ (1, 1, a), (1, 1, b), \\ (2, 0, a), (2, 0, b), (2, 1, a), (2, 1, b), \\ (3, 0, a), (3, 0, b), (3, 1, a), (3, 1, b)\}$$

$$M = \{a_1, a_2, \dots, a_n\}$$

$(\underbrace{\cdot, \cdot, \dots, \cdot}_{k\text{-Tupel}})$

Nach der Multiplikationsregel
gibt es n^k k -Tupel von Elementen
von M .

$$|M^k| = |\underbrace{M \times \dots \times M}_k \text{ Faktoren}| = |M| \cdot |M| \cdot \dots \cdot |M| = |M|^k$$

$$M = \{a, b, c, d, e, f\}$$

Es gibt 6^3 3-Tupel über M .

über M : von Elementen aus M .

$(\underbrace{\cdot, \dots, \cdot}_{k\text{-Tupel}})$

$$n \cdot (n-1) \cdot \dots \cdot (n-(k-1))$$

n^k

$$n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$$

$$n^{\underline{k}} = n!$$

$$n^{\underline{k}} = n \cdot (n-1) \cdot \dots \cdot (n-k+1)$$

$$= \frac{n!}{(n-k)!} = \frac{n(n-1) \cdot \cancel{\dots} \cdot \cancel{2} \cdot \cancel{1}}{(n-k) \cdot (n-k-1) \cdot \cancel{\dots} \cdot \cancel{2} \cdot \cancel{1}}$$

$$\frac{n!}{(n-k)!} = \frac{n(n-1) \cdot \dots \cdot (n-k+1) \cdot \cancel{(n-k)} \cdot \cancel{(n-k-1)} \cdot \dots \cdot \cancel{2} \cdot \cancel{1}}{(n-k) \cdot (n-k-1) \cdot \dots \cdot \cancel{2} \cdot \cancel{1}}$$

$$= n \cdot (n-1) \cdot \dots \cdot (n-k+1) = n^{\underline{k}}$$

Beispiel:

$$7^{\underline{3}} = 7 \cdot 6 \cdot 5$$

$$\frac{7!}{(7-3)!} = \frac{7 \cdot 6 \cdot 5 \cdot \cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot \cancel{1}}{\cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot \cancel{1}} = 7^{\underline{3}}$$

$$M = \{a_1, a_2, \dots, a_n\}$$

$\pi \downarrow$ \downarrow \dots \downarrow
 a_3 a_5 a_7

Sei M endlich.

Dann ist $f: M \rightarrow M$ genau dann injektiv, wenn f surjektiv ist.

Beispiel:

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\underline{\pi(1) = 3, \pi(2) = 1, \pi(3) = 2}$$

$$M = \{a_1, a_2, \dots, a_n\}$$

$$\underbrace{\{a_2, a_3, a_1, \dots, a_7\}}_{k \text{ Elemente.}}$$

Sei M eine n -elementige Menge.
 Dann gibt jedes k -Tupel
 über M ohne Wiederholungen
 Anlass zu einer k -elementigen
 Teilmenge.

$$(a_1, a_2, \dots, a_k) \mapsto \{a_1, \dots, a_k\}.$$

Es gibt für (a_1, \dots, a_k)

$k!$ k -Tupel mit denselben
 Komponenten a_1, \dots, a_k , evtl.
 in anderer Reihenfolge.

Anzahl k -Tupel über M ohne Wied.:

$$\text{Es gibt also } \frac{n^k}{k!} \text{ } k\text{-elementige}$$

Teilmenge von M .

Beispiel: $K = \{1, 2, 3\}$, $k = 2$.

$$S^2 = \left\{ \begin{array}{l} (1, 2) \\ (2, 1) \\ (1, 3) \\ (3, 1) \\ (2, 3) \\ (3, 2) \end{array} \right\} \quad \left\{ \begin{array}{l} \{1, 2\} \\ \{1, 3\} \\ \{2, 3\} \end{array} \right\} \quad \frac{3^2}{2!}$$

$\binom{n}{k}$ wird gelesen: „n über k“.

Wollen zeigen:

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

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

$$\binom{n}{0} = \frac{n!}{0! (n-0)!} = \frac{n!}{n!} = 1$$

$$\binom{n}{n} = \frac{n!}{n! (n-n)!} = \frac{n!}{n!} = 1$$

$$\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 1 & & 1 & & \\
 & 1 & & 2 & & 1 & \\
 1 & 3 & & 3 & & 1 & \\
 1 & 4 & & 6 & & 4 & 1 \\
 1 & 5 & 10 & 10 & 5 & 1 &
 \end{array}$$

Beachte: $\binom{n}{k} = \binom{n}{n-k}$

$$\begin{aligned}
 \binom{n}{k} &= \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!} \\
 &= \binom{n}{n-k}
 \end{aligned}$$

Achtung: $(a+b)^n \neq a^n + b^n$

Beispiel:	1	$\binom{0}{2}$
	1	$\binom{1}{2}$
	1	$\binom{2}{2}$
	1	$\binom{3}{2}$

$$(a+b)^1 = a + b$$

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

$$(a+b)^3 = a^3 + 3 \cdot a^2 b^1 + 3 a^1 b^2 + b^3$$

$$(a+b)^4 = a^4 + 4 a^3 b + 6 a^2 b^2 + 4 a b^3 + b^4$$

Beweis des Satzes:

Ind. Anf.: $(a+b)^0 = 1 \cdot a^0 b^0$.

Ind. Schritt: Annahme: gilt für n .

$$(a+b)^{n+1} = (a+b)^n \cdot (a+b)$$

$$\stackrel{IH.}{=} \left(\sum_{i=0}^n \binom{n}{i} a^{n-i} b^i \right) \cdot (a+b)$$

$$= \left(\sum_{i=0}^n \binom{n}{i} a^{n-i} b^i \right) \cdot a + \left(\sum_{i=0}^n \binom{n}{i} a^{n-i} b^i \right) \cdot b$$

$$= \sum_{i=0}^n \binom{n}{i} a^{n+1-i} b^i + \sum_{i=0}^n \binom{n}{i} a^{n-i} b^{i+1}$$

$$= \sum_{i=0}^n \binom{n}{i} \underline{a^{n+1-i} b^i} + \sum_{i=1}^{n+1} \binom{n}{i-1} \underline{a^{n+1-i} b^i}$$

$$= a^{n+1} + \sum_{i=0}^n \underbrace{\left(\binom{n}{i} + \binom{n}{i-1} \right)}_{\binom{n+1}{i}} a^{n+1-i} b^i + b^{n+1}$$

$$= \sum_{i=0}^{n+1} \binom{n+1}{i} a^{n+1-i} b^i \quad \square$$