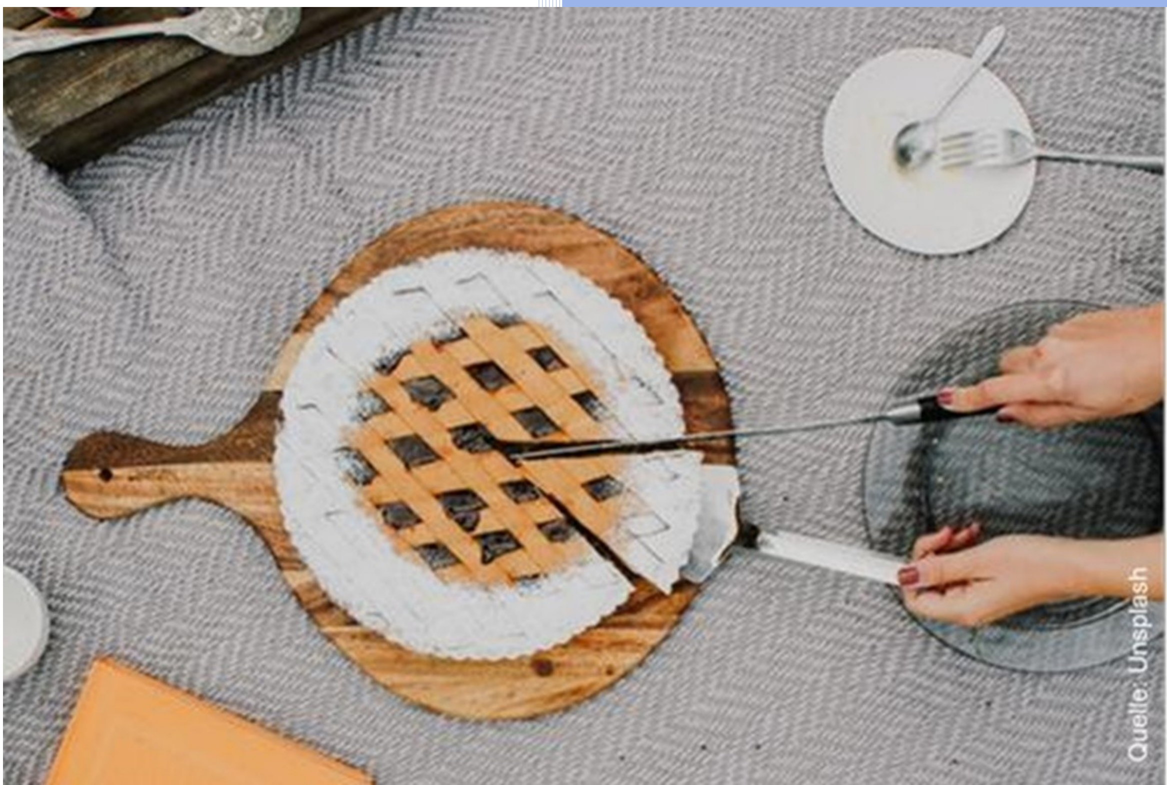
Zahlentheorie – Teil 1
Teilbarkeit



ruhl

ZAHLENTHEORIE – TEIL 1
TEILBARKEIT

INHALT

GRUNDLAGEN

Die Zahlentheorie ist ein Teilgebiet der Mathematik, das sich mit den Eigenschaften der **ganzen Zahlen** beschäftigt.

$Z=\{0,\pm 1,\pm 2,\pm 3,\ldots\}$

$N=\{0,1,2,3,\ldots\}$

$Z^{+¿=N^{+¿=\{1,2,3,\ldots\}¿}¿}$, analog $Z^{-¿¿}$

$Z_0^{+¿=N=\{0,1,2,3,\ldots\}¿}$, analog $Z_0^{-¿¿}$

¿ und $(N,\cdot)$ sind nur kommutative Halbgruppen.

¿ ist eine kommutative Gruppe

$(Z,\cdot)$ ist eine kommutative Halbgruppe

$(Z,+,\cdot)$ ist ein kommutativer Ring mit Einselement. Das einzige, was fehlt: es gibt im Allgemeinen keine multiplikativen Inversen (d.h. die Division funktioniert nicht uneingeschränkt).

TEILBARKEIT UND PRIMFAKTORENZERLEGUNG

Definition: Seien $t, a \in Z$. t teilt a ($t \vee a$), wenn es eine Zahl $b \in Z$ gibt mit $a = b \cdot t$.
t heißt Teiler von a.

z.B.: $6 \vee 18$, da $18 = 3 \cdot 6$ bzw.
$6 \nmid (-20)$, da 20 kein Vielfaches der Zahl 6 ist, und damit auch nicht von -20 .

Die Teilermenge von z.B. $a = 60$ lautet $T_{60} = \{1, 2,3,4,5,6,10,12,15,20,30,60\}$

Die Teiler 1 und 60 (also 1 und a) sind immer Teiler und werden daher **triviale Teiler** genannt.

Aufbau von N (und analog dazu von Z) in ¿:

$$1 = 12 = 1 + 13 = 1 + 1 + 1n = 1 + 1 + \ldots etc.$$

Aufbau von N (und analog dazu von Z) in $(N, \cdot)$:

$$1 = 12 = 1 \cdot 23 = 1 \cdot 34 = 1 \cdot 2 \cdot 25 = 1 \cdot 5 \cdots = \ldots 60 = 1 \cdot 2 \cdot 2 \cdot 3 \cdot 5$$

TEILBARKEITSREGELN

Satz: Seien $a, b, c, d \in Z$.

- $a \vee b \Rightarrow -a | b \text{ und } a | -b$
- $a | b \wedge b | c \Rightarrow a \vee c$
- $a | b \Rightarrow k \cdot a | k \cdot b$ für alle $k \in Z$ ¿ $\{0$ ¿ $\}$
- $a | b \wedge c | d \Rightarrow a \cdot c \vee b \cdot d$
- $a | b \wedge a | c \Rightarrow a \vee (k \cdot b + l \cdot c) \text{mit} \, k, l \in Z$, also auch jede Linearkombination

Beweis: …

Ein physikalischer Vergleich
Alle nat. Zahlen ergeben sich aus der Eins durch Addition. Die Eins ist diesbezüglich sozusagen das erzeugende Atom.
Die Atome der Multiplikation sind die Zahlen $1,2,3,5,7,11, \ldots etc.$ Aus ihnen lassen sich alle Zahlen multiplikativ aufbauen.

Definition: Eine Primzahl p ist eine natürliche Zahl größer 1, die nur die beiden trivialen Teiler 1 und p besitzt. $P = \{2,3,5,7,11,13,17,19,29,31,37,41,43,47, \ldots\}$ … Menge der Primzahlen.

Die Atome der ganzen Zahlen bezüglich der Multiplikation sind die Primzahlen. Die Zerlegung einer ganzen Zahl in Primfaktoren heißt **Primfaktorenzerlegung**.

Beispiel:

60	2
30	2
15	3
5	5
1	

$$60=2\cdot 2\cdot 3\cdot 5$$

Satz (Hauptsatz der Arithmetik): Jede natürliche Zahl $n\in N$ lässt sich (bis auf die Reihenfolge) eindeutig als Produkt von Primzahlpotenzen schreiben,

$$a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$$

wobei $p_i\in P$ (paarweise verschieden), $\alpha_i\in N, 1\leq i\leq s, s\in N$.

Beweis: …

Satz von Euklid: Es gibt unendlich viele Primzahlen.

Beweis: …

Satz (Primzahlsatz):

Im Weiteren sei $\pi(x)$ die Primzahlfunktion, die für beliebige reelle Zahlen x definiert ist als die Anzahl der Primzahlen, die nicht größer sind als x. Formal kann man schreiben:

$$\pi(x)=\left|\{p\in P\vee p\leq x\}\right|$$

Es gibt eine grobe Abschätzung:

$$\pi(x)\approx\frac{x}{\ln(x)}$$

z.B.: Im Bereich von [0 , 1 000] gibt es also etwa 150 Primzahlen.

DER ggT(a,b) – KÜRZEN UND HERAUSHEBEN

Kürzen: $\frac{12}{18}=\frac{6\cdot 2}{6\cdot 3}=\frac{ggT(12,18)\cdot 2}{ggT(12,18)\cdot 3}=\frac{2}{3}$

Herausheben: $12x+18y=ggT(12,18)\cdot(2x+3y)=6\cdot(2x+3y)$

ggT

Primfaktorenzerlegung

Euklidischer Algorithmus

Primfaktorenzerlegung:

60	2	90	2
30	2	45	3
15	3	15	3
5	5	5	5
1		1	

$$ggT(60)=2\cdot 3\cdot 5=30$$

(weitere Beispiele)

KLASSISCHER EUKLIDISCHER ALGORITHMUS

Idee: Der $ggT(a,b)$ $(a>b)$ ist auch $ggT(b,a-b)$! (*Beweis*: …)
Statt $ggT(a,b)$ zu bestimmen, berechnet man den ggT der kleineren Zahlen b und $a-b$.

z.B. $ggT(90,60)$ -> Tabelle

a	b	$a-b$
90	60	30
60	30	30
30	30	0

$ggT(90,60)=30$

z.B. $ggT(693,286)$ -> Tabelle

a	b	$a-b$
693	286	407
407	286	121
286	121	165
165	121	44
121	44	77
77	44	33
44	33	11
33	11	22
22	11	11
11	11	0

$ggT(693,286)=11$

MODERNER EUKLIDISCHER ALGORITHMUS

Dabei werden die im klassischen Algorithmus auftretenden wiederholten Subtraktionen eines Wertes durch eine einzige Division mit Rest ersetzt.

z.B. $ggT(693,286)$ $\rightarrow$ Tabelle

a	$(n)b$	$a-(n)b$
693	2·286	121
286	2·121	44
121	2·44	33
44	1·33	11
33	3·11	0

$ggT(693,286)=11$

z.B. $ggT(53667,25527)$ -> Tabelle

a	$(n)b$	$a-(n)b$
53667	2·25527	2613
25527	9·2613	2010
2613	1·2010	603
2010	3·603	201
201	3·201	0

$ggT(53667{,}25527)=201$

ERWEITERTER EUKLIDISCHER ALGORITHMUS (Euklidischer Algorithmus mit Rückrechnung)

Siehe Tabellen oben!

$$11=ggT(693{,}286) \qquad \text{¿}44-1\cdot 33=44-1\cdot(121-2\cdot 44)=-1\cdot 121+3\cdot 44=\text{¿}$$
$$\text{¿}-1\cdot 121+3\cdot(286-2\cdot 121)=3\cdot 286-7\cdot 121=\text{¿}$$
$$\text{¿}3\cdot 286-7\cdot(693-2\cdot 286)=-7\cdot 693+17\cdot 286$$

$$201=ggT(53677{,}25527) \qquad \text{¿}2010-3\cdot 603=\cdots\cdots=-39\cdot 53667+82\cdot 25527$$

Satz: Mit dem erweiterten euklidischen Algorithmus erhält man $ggT(a,b)$ als ganzzahlige Linearkombination von a und b :
$ggT(a,b)=x\cdot a+y\cdot b$mit $x,y\in\ Z$.

Beweis: Auf Grund der Konstruktion funktioniert das Verfahren immer.