$(\mathbb{Z}, +, \cdot)$	ganze Zahlen (Ring)	*integer (number)*
$d \mid n :\Leftrightarrow (\exists q)\ n = dq$	d teilt n	$(d, n, q \in \mathbb{Z})$
$d \mid n$	d Teiler von n	*divisor*
$1, -1, +n, -n$	unechte Teiler von n	
$1, -1$	Einheiten in $\mathbb{Z}$	*units*
$\tau(n) := \sum_{d\mid n} 1$	Teilerfunktion	
		Anzahl der positiven Teiler
p prim $:\Leftrightarrow\ \tau(p) = 2$	Primzahl	*prime (number)*
	($\neq 1$, keine echten Teiler)	

(Division mit Rest)		$(\exists k, r)$ *(eindeutig!)*
$(\forall n, q)\ n = kq + r$	$0 \leq r < n$	*positiv kleinster Rest*
$(\forall n, q)\ n = kq + r$	$-\frac{(n-1)}{2} < r \leq \frac{(n-1)}{2})$	*absolut kleinster Rest*

einige Eigenschaften:

	$a \mid b \wedge b \mid c\ \Rightarrow\ a \mid c$	transitiv
	$a \mid b \wedge b \mid a\ \Rightarrow\ a = \pm b$	
also:	$(\mathbb{N}, \mid)$ (teilweise) geordnet	*partial order, poset*
ferner:	$a \mid b\ \Rightarrow\ a \mid bc$	
	$a \mid b \wedge a \mid c\ \Rightarrow\ a \mid (b + c)$	

Definition:

	$a \equiv b \bmod m :\Leftrightarrow\ m \mid (a - b)$	**kongruent**
es gilt	$a \equiv a\ (m)$	reflexiv
	$a \equiv b\ \Rightarrow\ b \equiv a$	symmetrisch
	$a \equiv b \wedge b \equiv c\ \Rightarrow\ a \equiv c$	transitiv
	$a \equiv a' \wedge b \equiv b'\ \Rightarrow\ a + b \equiv a' + b'$	
und	$a \equiv a' \wedge b \equiv b'\ \Rightarrow\ ab \equiv a'b'$	

allgemein:

Eine Relation ist eine **Kongruenzrelation**,
wenn sie mit der *Struktur* verträglich ist.

(gewählt zu einem der schönsten Sätze der Mathematik)
sowie: ein Beweis aus „The Book“ (nach Pal Erdős)

(Euklid) Es gibt unendlich viele Primzahlen.

denn: zu jedem $n \in \mathbb{N}$ gibt es eine Primzahl $p > n$

$N := n! + 1$ ist durch kein k $(2 \leq k \leq n)$ teilbar,

also sind alle Teiler (inklusive Primteiler) $> n$.

(a, b) größter gemeinsamer Teiler
greatest common divisor

$[a, b]$ kleinstes gemeinsames Vielfaches
least common multiple

$(a, b) = 1$ a und b relativ prim

es gilt: Verband $(\mathbb{N}, |)$ *lattice*

$d \mid a \wedge d \mid b \;\Rightarrow\; d \mid (a, b)$ Infimum $a \cap b$

$a \mid m \wedge b \mid m \;\Rightarrow\; [a, b] \mid m$ Supremum $a \cup b$

sowie $ab = (a, b)[a, b]$

Euklidischer Algorithmus *zur Bestimmung von* (a, b)

wegen $(a, b) = (a, a - b)$ *gilt* *obdA.* $a > b$

$(a, b) = (b, r) =: (a_1, b_1)$ *für* $a = bq + r$

nach endlich vielen Schritten:

$$(a, b) = \cdots = (a_n, 0) = a_n$$

Einsetzen ergibt: $b_1 = r = a - bq$ *etc.*

$(a, b) = a_n = \lambda a + \mu b$ $(\lambda, \mu \in \mathbb{Z})$

$$(a, b) = \min\{n > 0 \mid n \in a\mathbb{Z} + b\mathbb{Z}\}$$

$(a, b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ *(Hauptideal)*

Der größte gemeinsame Teiler von zwei oder mehr Zahlen ist
die kleinste positive (ganzzahlige) Linearkombination dieser Zahlen.

(Fundamentallemma(-satz) der Zahlentheorie)

$$a \mid bc \wedge (a,b) = 1 \;\Rightarrow\; a \mid c$$

Beweis: Euklidischer Algorithmus $\Rightarrow$ ($\mathbb{Z}$ euklidisch)

$$1 = \lambda a + \mu b \;\Rightarrow\; c = c(\lambda a + \mu b) = (\lambda c)a + \mu(bc) \;\Rightarrow\; a \mid c \qquad \blacksquare$$

(Spezialfall) p prim, $p \mid bc \;\Rightarrow\; p \mid b \vee p \mid c$ p Primelement

(Definition) p irreduzibel (unzerlegbar)

p prim, $(d \mid p)$ d.h. $dd' = p \;\Rightarrow$ *d oder d'* Einheit

ZPE = **Z**erlegung **P**rimzahlen **e**indeutig

(Prim(zahl)zerlegung) ($\mathbb{Z}$ ist ein ZPE-Ring.)

Jede natürliche (*ganze*) Zahl n kann als Produkt von Primzahlen,

$n = p_1 p_2 \cdots p_k$, geschrieben werden, und

die Darstellung ist bis auf die Reihenfolge (*und Einheiten*) eindeutig.

(Normalform) *(eindeutig)*

$$n = \pm p_1^{e(1)} p_2^{e(2)} \cdots p_r^{e(r)} \qquad (e(r) \geq 1,\; p_1 < p_2 < \cdots < p_r)$$

$$n = \pm 2^{e_2(n)} \cdots p(k)^{e_{p(k)}(n)} \cdots = (\pm 1) \prod_{p \text{ prim}} p^{e_p(n)} \qquad (e_{p(k)}(n) \geq 0)$$

(Teiler) $d \mid n \;\Leftrightarrow\; e_p(d) \leq e_p(n)$ $(\forall p)$

$$e_p((m,n)) = \min(e_p(m), e_p(n)) \qquad e_p([m,n]) = \max(e_p(m), e_p(n))$$

$$(m,n) = \prod_{p \text{ prim}} p^{\min(e_p(m), e_p(n))} \qquad [m,n] = \prod_{p \text{ prim}} p^{\max(e_p(m), e_p(n))}$$

Anzahl der Teiler (in $\mathbb{N}$) *Summe der Teiler*

$$\tau(n) := \textstyle\sum_{d \mid n} 1 \qquad \sigma(n) := \textstyle\sum_{d \mid n} d$$

$$\tau(n) = \prod_{p \text{ prim}} (e_{p(n)} + 1) \qquad \sigma(n) = \prod (1 + p + \cdots p^{e_p(n)})$$

($\sigma(n) = 2n \;\Leftrightarrow$: n vollkommen (Euklid)) $$= \prod_{p \text{ prim}} \frac{p^{e_p(n)+1} - 1}{p - 1}$$

Jede natürliche Zahl (größer 1)
ist kann als Produkt von Primzahlen geschrieben werden
und die Faktoren sind bis auf die Reihenfolge eindeutig bestimmt.

Beweis: sei $n \geq 2$

Existenz Induktion nach n

Induktionsanfang: $n = 2$ $2 = 2$

Induktionsannahme: $k < n \Rightarrow k = p_1 p_2 \cdots p_s$

Induktionschritt:

entweder n hat keine echten Teiler $\Rightarrow n$ prim $n = n$

oder $n = n_1 n_2$ mit $1 < n_1, n_2 < n$

Induktionsannahme $\Rightarrow n_1 = p_1 p_2 \cdots p_s$

und $\Rightarrow n_2 = q_1 q_2 \cdots q_t$

$\Rightarrow n = p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t$ ■

Eindeutigkeit

Induktionsanfang: $n = 2$ $2 = 2$

Induktionsannahme:

$k < n$ und $k = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$

$\Rightarrow s = t$ und die p_i sind eine Permutation der q_j

Induktionschritt: $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$

es gilt $p_1 \mid (q_1 q_2 \cdots q_t)$

also (Fundamentalsatz)

p_1 teilt einen der Faktoren (q_{j_0})

$p_1 \mid q_{j_0}$ $\Rightarrow p_1 = q_{j_0}$ da: q_{j_0} prim und $p_1 > 1$

also $n > \frac{n}{p_1} = \frac{n}{q_{j_0}} = p_2 \cdots p_s = q_1 q_2 \cdots q_{j_0-1} q_{j_0+1} \cdots q_t$

und laut Induktionsannahme folgt:

die p_i und die q_j sind dieselben Faktoren

(Variante) sei zusätzlich *oBdA.* $p_1 \leq p_2 \leq \cdots p_s$,

$q_1 \leq q_2 \leq \cdots q_t$ und $p_1 \leq q_1$

$\Rightarrow p_1 \leq q_1 \leq q_{j_0} = p_1 \Rightarrow p_1 = q_1 (= q_{j_0})$

also: $n > p_2 p_3 \cdots p_s = \frac{n}{p_1} = \frac{n}{q_1} = q_2 q_3 \cdots q_t$

und daher laut Induktionsvoraussetzung:

$(s-1) = (t-1)$ und $p_2 = q_2, p_3 = q_3, \ldots, p_s = q_s (= q_t)$ ■