Thema: 1.2 elem. Zahlentheorie

-> ganze u. natürl. Zahlen

Definition: li $\Longleftrightarrow$ re

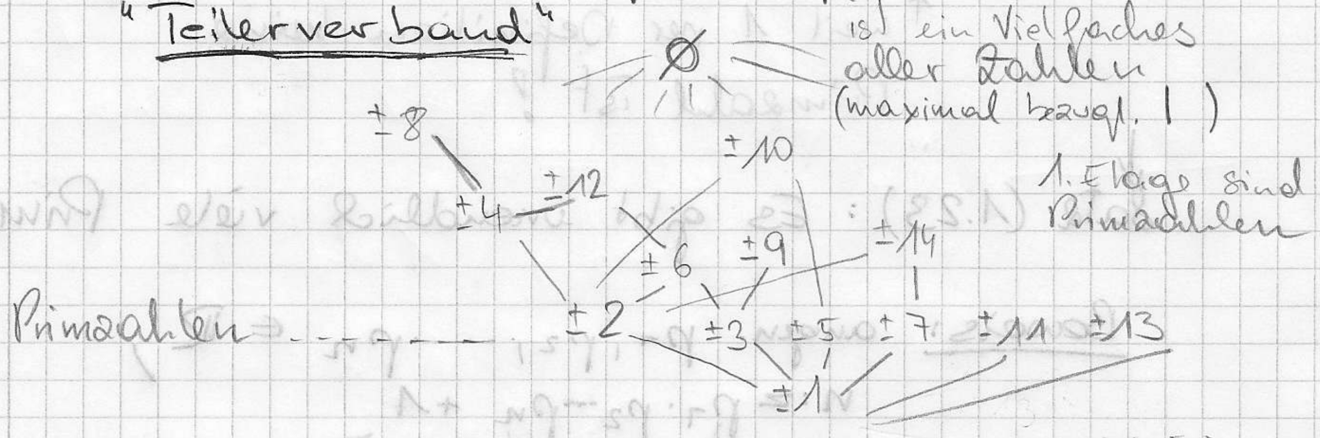
wird neu definiert

a) Teilbarkeit

Wann kann ich eine ganze Zahl dividieren

Seien a, b ganze Zahlen
b teilt a, i.Z. $b \mid a$:$\Longleftrightarrow$ Es gibt ein $c \in \mathbb{Z}$ mit Eigenschaft $b \cdot c = a$

"Teilerverband"



zB: $\pm 4 = ggT(8, 12)$ größter gem. Teiler
$\pm 12 = kgV(4, 6)$ kl. gemeinsames Vielfaches

b) d ist ggT von a und b :$\Longleftrightarrow$
(i) $d \mid a$ und $d \mid b$
(ii) $d' \mid a$ und $d' \mid b \Rightarrow d' \mid d$
$8, 12 \to 4, 2 \quad 2 \mid 4$

c) kgV

v ist kgV von a und b $:\Leftrightarrow$

(i) $a \mid v$ und $b \mid v$

(ii) $a \mid v'$ und $b \mid v' \Rightarrow v \mid v'$

d) Primzahl

$p \in \mathbb{N}$ ist Primzahl, $p \in \mathbb{P} :\Leftrightarrow$

$p \geq 2$ und $a \mid p \Rightarrow a \in \{1, -1, p, -p\}$

↑ weil 1 per Definition keine Primzahl ist!

Satz (1.23): Es gibt unendlich viele Primzahlen

__Beweis:__ angen. $p_1, p_2, \dots p_n \in \mathbb{P}$,

$n := \underbrace{p_1 \cdot p_2 \cdots p_n}_{\text{Vielfaches der Zahl } p_i} + 1$

bei Division bekomm ich 1 Rest wenn ich durch p_i dividiere

$\Rightarrow p_i \nmid k, \; i = 1, \dots, n$

k besitzt mind. einen Primteiler $p := p_{n+1} \neq p_i$

d.h. zu endlich vielen Primzahlen gibt es (eine) weitere $\Rightarrow$ Behauptung

Division mit Rest: (Satz 1.15)

Quotient (Vielfaches von b)

von a durch b: $a = q \cdot b + r$

Rest

$0 \leq r < b$

Iteration ⇒ Euklidischer Algorithmus

Satz 1.16 Bsp 1.17

Bsp: $a = 59$, $b = 11$

$\boxed{59} = 11 \cdot 5 + 4 \Rightarrow 4 = 59 - 11 \cdot 5$

$11 = 4 \cdot 2 + 3 \Rightarrow 3 = 11 - 4 \cdot 3$

$4 = 3 \cdot 1 + \boxed{1} \Rightarrow 1 = 4 - 3 \cdot 1$

$3 = 1 \cdot 3 + 0$

muss Teiler sein

ggT

$4 = 59 - 11 \cdot 5$

$3 = 11 - 4 \cdot 2$

$1 = 4 - 3 \cdot 1 = 4 - (11 - 4 \cdot 2) \cdot 1 = 3 \cdot 4 - 11 =$

jeder Teiler ist Teiler von 1 (dieser Zahl)

$3 \cdot 4 - 11 = 3 \cdot (59 - 11 \cdot 5) - 11 = 3 \cdot 59 - 16 \cdot 11$

$\Rightarrow 1 = ggT(59, 11)$

Eukl. Alg. zeigt, dass es immer einen ggT gibt!

Allgemein: (Satz 1.18)

Je zwei Zahlen $a, b \in \mathbb{Z}$ besitzen ein ggT, der mit Hilfe des Euklidschen Alg. ermittelt werden kann.
Über dies gilt das der $ggT(a,b) = x \cdot a + y \cdot b$ mit $x, y \in \mathbb{Z}$

Folgerung (Satz 1.20) - Euklidisches Lemma

$$p \in \mathbb{P},\ p \mid \underbrace{a_1 \cdot a_2 \cdots a_r}_{\in \mathbb{N}},\ r \geq 1 \Rightarrow p \mid a_j \text{ für ein } j \in \{1, 2, \dots r\}$$

$r > 2$ Induktion

Beweis: (für $r = 2$)

Angenommen: $p \mid a_1 \cdot a_2$, $p \nmid a_1$

jetzt möchte ich sagen, dass es $p \mid a_2$ sein muss

$$\Rightarrow ggT(p, a_1) = 1 = x \cdot a_1 + y \cdot p \quad x, y \in \mathbb{Z}$$

Multiplikation mit a_2

$$\Rightarrow a_2 = \underbrace{x \cdot a_1 \cdot a_2}_{p \mid \cdot} + \underbrace{y \cdot p \cdot a_2}_{p \mid \cdot} \Rightarrow p \mid a_2$$

beide Summanden sind Vielfaches von p

Was kann ich mit $\mathbb{Z}$:

→ Ist es eine Primzahl

→ wenn nein kann ich sie als Produkt von Primfaktoren darstellen

$$72 = 2 \cdot 36$$
$$2 \cdot 2 \cdot 18$$
$$2 \cdot 2 \cdot 2 \cdot 9$$
$$2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$$

Fundamentalsatz der Zahlentheorie

(Satz 1.21) Σ ← Sigma

Die Primfaktorzerlegung für $n \geq 1$ ist (bis auf die Reihenfolge der Faktoren eindeutig, d.h. in ~~$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$~~ Produkt

Produkt

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

(in dieser Darstellung ...)
sind die $\nu_p^{(n)}$ durch n eindeutig bestimmt.

Beweis - Induktionsbeweis:

hier will ich was zeigen $n = 1$
dann überleg ich mir wie sichs weiter verhält

Beweis:

$n=1$ leeres Produkt $1 = \prod_{p \in \mathbb{P}} p^{0} \quad v_p^{(1)}$

$n=2$ $\quad v_2^{(2)}=1, \; v_p^{(2)}=0 \;\; \forall p \neq 2$ eindeutig

Induktionsannahme: Diese Aussage gelte für $k = 1, 2, 3, \dots n$

$n+1 = p_1 \cdot \dots p_m = p_1' \cdot \dots p_m' \Rightarrow p_i, p_j' \in \mathbb{P}$

$p_m \mid p_1' \dots p_m' \overset{S\,1.20}{\Longrightarrow} p_m \mid p_j'$ für ein j,

$p_m \mid n+1$

o.B.d.A $j = m'$ // ohne Beschränkung / der Allgemeinheit

Wir haben eine Primzahl p_m gefunden, die p_j' teilt.

$\overrightarrow{p_m'}$ $p_m = p_m'$ kürzen: $n' = \dfrac{n+1}{p_m} = p_1 \cdots p_{r-1} = p_1' \cdots p_{r-1}'$

Induktionsannahme

$p'_{n'-1} \Longrightarrow m = m'$ und Faktoren müssen übereinst.

$\Rightarrow m = m'$, (OBdA) $p_1 = p'_1,\ p_2 = p'_2, \ldots, p_{m-1} = p'_{m'-1}$

$\Rightarrow$ Satz 1.24

$$a = \prod_{p \in \mathbb{P}} p^{\nu_p(a)}, \quad b = \prod_{p \in \mathbb{P}} p^{\nu_p(b)} \Rightarrow$$

$$\Rightarrow a \mid b \Leftrightarrow \forall p \in \mathbb{P}: \nu_p(a) \leq \nu_p(b)$$

$$ggT(a,b) = \prod_{p \in \mathbb{P}} p^{\min\{\nu_p(a), \nu_p(b)\}}$$

$$kgV(a,b) = \prod_{p \in \mathbb{P}} p^{\max\{\nu_p(a), \nu_p(b)\}}$$

$$\Rightarrow ggT(a,b) \cdot kgV(a,b) = a \cdot b$$

Kongruenzen: zB modulo 5 (= m)

Restklassen modulo 5

$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
⋮	⋮	⋮	⋮	⋮
-10	-9	-8	-7	-6
-5	-4	-3	-2	-1
0	1	2	3	$\boxed{4}$
5	6	7	8	$\boxed{9}$
10	11	12	13	14
⋮	⋮	⋮	⋮	⋮

Zahlen aus Klasse 1

Klasse 3

also $\overline{1} + \overline{3} = \overline{4}$ ← landen immer in Kl. $\overline{4}$

$\overline{1} \cdot \overline{3} = \overline{3}$ etc

<u>allg.:</u>

$$* \quad \left\{ \begin{array}{l} a_1 = k_1 \cdot m + r_1 \\ a_2 = k_2 \cdot m + r_2 \end{array} \right\} \Rightarrow \begin{array}{l} a_1 + a_2 = (k_1 + k_2) m + (r_1 + r_2) \\ a_1 \cdot a_2 = (k_1 r_2 + r_1 k_2 + k_1 k_2 m) m + r_1 \cdot r_2 \end{array}$$

⇒ Restklassen der Ergebnisse hängen nur von den Restklassen r_1 und r_2 von a_1, a_2 ab!

Definition:

Sei $m \in \mathbb{N}$, $m \geq 1$ „Modul"

$a, b \in \mathbb{Z}$ heißen kongruent modulo m

i.Z. $a \equiv b \mod m$, falls sie bei Division durch m denselben Rest liefern

($\Leftrightarrow m \mid a-b$)

$\bar{a} = a + m \cdot \mathbb{Z} = \{a + mk \mid k \in \mathbb{Z}\}$

$\bar{a}$ heißt Restklasse von a modulo m.

$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ = Menge der Restklassen

Wegen ⊛ sind die Operationen

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{a} - \bar{b} = \overline{a-b}$$

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

für Restklassen „wohldefiniert", d.h. unabhängig von der Wahl der Repräsentanten a, b der Klassen $\bar{a}, \bar{b}$.

Rechenregeln vererben sich von $\mathbb{Z}$ auf $\mathbb{Z}_m$ entsprechend.

Inverses $\frac{1}{3} = 3$

$\pm 1 = \pm 1$

Inverse Elemente bezügl. der Multiplikation

$\overline{a} \cdot \overline{b} = \overline{1}$ bedeutet (Inverses Element von a: $\overline{b}$)

$$a \cdot b - m \cdot k = 1 \quad \text{mit } k \in \mathbb{Z}$$

Das ist genau dann möglich wenn $\mathrm{ggT}(a, m) = 1$

Vergl. Satz 1.18

In diesem Fall nennt man $\overline{a}$ eine prime Restklasse modulo m

$4 \to \overline{1}, \overline{3}$

$\varphi(m)$ = Anz. der primen Restklassen modulo m

Eulersche φ-Funktion

zB $m \in \mathbb{P}$ zB 5, sind alle ausser $\emptyset$ Restkl.

$m \in \mathbb{P} \Rightarrow$ alle Restklassen $\overline{a} \neq \overline{0}$ besitzen Inverse

Inverse $\Rightarrow \varphi(p) = p - 1$

Allg. Satz 1.34:

$$m = p_1^{e_1} \cdots p_r^{e_r} \; ; \; e_i \geq 1$$

$$\Rightarrow \varphi(m) = m\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

ohne Beweis...

Anwendungen von Kongruenzen:

- Codierungstheorie
- Teilbarkeitsregeln
- Kryptographie (RSA-Verfahren)

Nur zur Info