Zahlentheorie

Teilbarkeit

Sind $x, y \in \mathbb{Z}$ ganze Zahlen, so sagen man, dass x ein Teiler von y ist, falls es ein $k \in \mathbb{Z}$ gibt mit $x \cdot k = y$. In diesem Fall schreibt man $x \mid y$.

$x \mid y \; : \; \exists k \in \mathbb{Z} \quad y = x \cdot k$

$T(y)$ bezeichnet die Menge aller natürlichen Zahlen, welche Teiler von y sind.

$T(y) = \{ x \in \mathbb{N} \mid x \mid y \}$

z.B. $T(0) = \mathbb{N}$, $\forall_z \in \mathbb{Z} \; (1 \in T(z))$, $T(-32) = \{1, 2, 4, 8, 16, 32\}$

kgV und ggT

Seien $x, y \in \mathbb{Z}$. Kleinstes gemeinsames Vielfaches von x und y

$kgV(x,y) := \min \{ k \in \mathbb{N} \mid x \mid k \wedge y \mid k \}$

z.B. $kgV(12,40) = 120$, $kgV(-7,12) = 84$

Seien $x \neq 0$ oder $y \neq 0$. Grösster gemeinsamer Teiler von x und y

$ggT(x,y) := \max \{ k \in \mathbb{N} \mid k \mid x \wedge k \mid y \}$

z.B. $ggT(12,40) = 4$, $ggT(-7,12) = 1$

Zusammenhang zwischen $ggT(x,y)$ und $kgV(x,y)$

$ggT(x,y) \cdot kgV(x,y) = |x \cdot y|$

z.B. $ggT(12,40) \cdot kgV(12,40) = 4 \cdot 120 = 480$

$\longrightarrow |12 \cdot 40| = 480$

Euklidischer Algorithmus

Zur Bestimmung des $ggT(x,y)$

z.B. $ggT(27, -96)$ — Dividiere grössere (negativ ignoriert) Zahl durch die kleinere Zahl

$-96 = (-4) \cdot 27 + 12$

$27 = 2 \cdot 12 + 3 \longrightarrow ggT(27,-96) = 3$

$12 = 4 \cdot 3 + 0$ — oberhalb Rest 0

Zwei ganze Zahlen x, y sind Teilerfremd, wenn $ggT(x,y) = 1$

z.B. $ggT(37, 75)$

$75 = 2 \cdot 37 + 1 \longrightarrow ggT(37,75) = 1$

$37 = 1 \cdot 37 + 0$

Erweiterter Euklidischer Algorithmus (Lemma von Bézout)

Finden einer ganzzahligen Lösung für die Gleichungsform:

$ax + by = ggT(a,b) \quad , x, y \in \mathbb{Z}$ und $x, y \neq 0$

(!) Diophantische Gleichung = Gleichung in der nur ganzzahlige Lösungen gesucht

z.B. $ggT(168, 133) = 168x + 133y$

$168 = 1 \cdot 133 + 35 \qquad \Rightarrow \; 35 = 168 + (-1) \cdot 133$

$133 = 3 \cdot 35 + 28 \qquad \Rightarrow \; 28 = 133 + (-3) \cdot 35 = 133 + (-3) \cdot (168 + (-1) \cdot 133)$

$= 133 + (-3) \cdot 168 + 3 \cdot 133$

$= 4 \cdot 133 + (-3) \cdot 168$

$35 = 1 \cdot 28 + 7 \qquad \Rightarrow \; 7 = 35 + (-1) \cdot 28 = 168 + (-1) \cdot 133 + (-1) \cdot (4 \cdot 133 + (-3) \cdot 168)$

$= 168 + (-1) \cdot 133 + (-4) \cdot 133 + 3 \cdot 168$

$= 4 \cdot 168 + (-5) \cdot 133$

$28 = 4 \cdot 7 + 0 \qquad ggT(168,133) = 7$

$\hookrightarrow x = 4, \; y = -5, \; \mathbb{L}_{x,y} = \{(4,-5)\}$

Hat genau dann eine ganzzahlige Lösung, wenn $c = n \cdot ggT(a,b)$

z.B. $168x + 133y = 7'000$, $7'000 = 1'000 \cdot ggT(168,133)$ ✓

$168x + 133y = 10$, $10 = \underbrace{\tfrac{10}{7}}_{\notin \mathbb{Z}} \cdot ggT(168,133)$ ✗

Kongruent modulo Relation

Wenn zwei ganze Zahlen a und b bei Division durch $n \in \mathbb{N}$ denselben Rest haben, so sagt man, a und b sind kongruent modulo n. $a \equiv b \pmod{n}$, $a \equiv_n b$ (n heisst Modul)

z.B. $17 \equiv_5 22$, $6 \equiv_5 1$

Rechenregeln wenn $a \equiv_n b$ und $c \equiv_n d$: $a + c \equiv_n b + d$, $a \cdot c \equiv_n b \cdot d$

Restklassen

Klassen mit demselben Rest bei der Division durch eine Zahl

z.B. $17 \equiv_5 22 \longrightarrow [2]_5$ oder $\bar{2}$ von $\mathbb{Z}/5 = \{\dots, 17, 22, \dots\}$

Menge aller Restklassen : $\mathbb{Z}/n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$

Rechenregeln : $a \cdot [x]_n := [ax]_n$, $[x]_n - [y]_n := [x-y]_n$, $([x]_n)^k = [x^k]_n$

z.B. $3a - 2b^4 + 4a^2 b$, $a = [7]_{15}$, $b = [2]_{15}$

$3 \cdot \bar{7} - 2 \cdot \bar{2}^4 + 4 \cdot \bar{7}^2 \cdot \bar{2}$

$= \overline{21} - \overline{32} + \overline{392}$

$= \overline{381} = \bar{6} \longrightarrow 381 : 15 = 25.4$, $381 - (25 \cdot 15) = 6$

Primzahlen

Eine natürliche Zahl $p > 1$, die nur durch sich selbst und durch 1 teilbar ist. (1 ist keine Primzahl)

Es gilt : $T(p) = \{1, p\}$, $|T(p)| = 2$, Menge aller Primzahlen : $\mathbb{P}$

Primfaktorzerlegung : $60 = 10 \cdot 6 = 2 \cdot 5 \cdot 2 \cdot 3 = 2^2 \cdot 3 \cdot 5$, $8 = 2^3$

$\hookrightarrow kgV(60,8) = 2^3 \cdot 3 \cdot 5 = 120$ (!) grösste Primfaktoren

Fakultät Anzahl Nullen am Ende : $15! = 1 \cdot 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \longrightarrow 3$ Nullen (Exponent bei 5)

Prime Restklassen

Restklassen welche teilerfremd zu n sind. $\mathbb{Z}^*_{/n}$

z.B. $\mathbb{Z}^*_{/8} = \{1, 3, 5, 7\}$

Additive Inverse

Von negativer Restklasse zu positiver.

z.B. $-\overline{496}$ in $\mathbb{Z}/3211$

$3211 - 496 = \overline{2715}$

Multiplikative Inverse

Existiert nur wenn k und n teilerfremd ($ggT(k,n)=1$).

$k \cdot r + n \cdot x = 1$, $[a]_n \cdot [a^{-1}]_n = [1]_n$

z.B. $\overline{123}^{-1}$ in $\mathbb{Z}/3211$ $\rightarrow$ $ggT(123, 3211) = 1$

$3211 = 26 \; 123 + 13 \;\Rightarrow\; 13 = 3211 - 26 \cdot 123$

... lösen mit erweiterter euklidischer Algorithmus

$= 19 \cdot 3211 + (-496) \cdot 123$

$[123^{-1}]_{3211} = [-496]_{3211} = [2715]_{3211}$

$\hookrightarrow$ Wenn negative Restklasse, muss noch additive Inverse berechnet werden, bei positiver Restklasse ist es bereits das Ergebnis.

Lösbarkeit von Gleichungen

$\bar{a} \cdot x = \bar{b}$ ist in $\mathbb{Z}/n$ lösbar, wenn a und n teilerfremd sind. Es gibt genau $t = ggT(a,n)$ Lösungen wenn t auch b teilt, ansonsten gibt es keine.

z.B. $\bar{5}x - \bar{2} = \bar{4}$ für $\mathbb{Z}/9$ $\longrightarrow$ $ggT(5,9) = 1$

$\bar{5}x - \bar{2} = \bar{4} \quad | + \bar{2}$

$\bar{5}x = \bar{6} \quad | \cdot \bar{5}^{-1} = \bar{2}$ $\longrightarrow$ $\bar{5} \cdot \bar{2} = \bar{9} + \bar{1}$

$x = \overline{12} = \bar{3}$

$\mathbb{L}_x = \{\bar{3}\}$

Verknüpfungstabelle

z.B. $\mathbb{Z}/4$

+	0	1	2	3
0	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
1	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
2	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
3	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

	0	1	2	3
0	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
1	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
2	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
3	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Chinesischer Restsatz

z.B. $x \equiv_3 2$, $x \equiv_5 3$, $x \equiv_7 2$

0. $ggT(3,5) = ggT(3,7) = ggT(5,7) = 1$
1. $N_1 = 5 \cdot 7 = 35$, $N_2 = 3 \cdot 7 = 21$, $N_3 = 3 \cdot 5 = 15$, $n = 3 \cdot 5 \cdot 7 = 105$
2. $[N_1]_3 = [35]_3 = [2]_3 \qquad [2^{-1}]_3 = [2]_3 = [r_1]_3$

   $[N_2]_5 = [21]_5 = [1]_5 \qquad [1^{-1}]_5 = [1]_5 = [r_2]_5$

   $[N_3]_7 = [15]_7 = [1]_7 \qquad [1^{-1}]_7 = [1]_7 = [r_3]_7$
3. $x = \sum_{i=1}^{3} y_i \cdot N_i \cdot r_i = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$

   $233 : 105 = 2.21$, $233 - (2 \cdot 105) = 23$

Lösungsmenge: $[233]_{105} = [23]_{105} = \{23 + k \cdot 105 : k \in \mathbb{Z}\}$

Kleine Satz von Fermat

Ist p eine Primzahl, dann gilt für alle teilerfremde ganze Zahlen: $a^{p-1} \equiv_p 1$

z.B. $p = 13$, $a = 6$ $\longrightarrow$ $6^{12} \equiv_{13} 1$

Sind p und a teilerfremd und ist $a^{p-1} - 1$ nicht durch n teilbar, dann kann p keine Primzahl sein.

z.B. $p = 9$, $a = 2$ $\longrightarrow$ $ggT(9,2) = 1$, $2^8 - 1 = 255$ ist nicht durch 9 teilbar $\longrightarrow$ 9 ist keine Primzahl