Zahlentheorie ist die Mathematik der ganzen Zahlen.

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

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

Diophantische Gleichungen

Gegeben $a, b, c \in \mathbb{N}$, gesucht $x, y \in \mathbb{Z}$ mit: $ax + by = c$

Wir schreiben Lösungen als Zahlenpaar $(x|y)$.

Beispiele:

$x + 3y = 10$ $\quad (x|y) = (7|1), (4|2), (1|3)$

$3x + 7y = 1$ $\quad (x|y) = (-2|1), (5|-2)$

$5x + 5y = 1$ $\quad$ Keine Lösung, da linke Seite durch 5 teilbar, rechte nicht.

Teiler und Primzahlen

Definition:

1) Seien $x \in \mathbb{Z}$, $n \in \mathbb{N}$. k heißt Teiler von x, geschrieben $k|x$, falls es ein $q \in \mathbb{Z}$ gibt, so dass gilt: $x = q \cdot k$.

2) Seien $a, b \in \mathbb{N}$. Dann ist der größte gemeinsame Teiler von a und b definiert durch:

$ggT(a,b) = \max\{k \in \mathbb{N} \mid k|a \wedge k|b\}$

Beispiele:

$3|12$, denn $12 = 3 \cdot 4$

$2|-8$, denn $-8 = 2 \cdot (-4)$

$a = 70$, $b = 98$

Teiler von $a = \{1, 2, 5, 7, 10, 14, 35, 70\}$

Teiler von $b = \{1, 2, 7, 14, 49, 98\}$

gemeinsame Teiler von a und $b = \{1, 2, 7, 14\}$

$ggT(a,b) = 14$

Definition:

Eine natürliche Zahl $p > 1$ heißt Primzahl oder prim, wenn sie genau zwei Teiler hat: die 1 und sich selbst.

Beispiele:

$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Hauptsatz der elementaren Zahlentheorie

Jede natürliche Zahl $n > 1$ lässt sich, bis auf die Reihenfolge der Faktoren, eindeutig als Produkt von Primzahlen darstellen.

Beispiele:

$70 = 2 \cdot 5 \cdot 7$
$98 = 2 \cdot 7 \cdot 7$
$\Rightarrow ggT(70, 98) = 2 \cdot 7 = 14$

$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$
$756 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7$
$\Rightarrow ggT(360, 756) = 2 \cdot 2 \cdot 3 \cdot 3 = 36$

Der $ggT(a,b)$ besteht aus allen gemeinsamen Primfaktoren von a und b.
Also: Jeder gemeinsame Teiler von a und b ist auch Teiler von $ggT(a,b)$.

Definition: Einen Ausdruck der Form $ax + by$ mit $a, b \in \mathbb{N}$ und $x, y \in \mathbb{Z}$ nennen wir Vielfachsumme von a und b.

Satz
Ist k ein gemeinsamer Teiler von a und b, dann teilt k auch jede Vielfachsumme von a und b, also:
$k|a \wedge k|b \Rightarrow k|(ax+by)$ für $a, b, k \in \mathbb{N}$, $x, y \in \mathbb{Z}$

Beweis:
$k|a \Rightarrow \exists k_1 \in \mathbb{Z}: a = q_1 \cdot k$
$k|b \Rightarrow \exists k_2 \in \mathbb{Z}: b = q_2 \cdot k$
$\Rightarrow ax + by = q_1 kx + q_2 ky = k(\underbrace{q_1 x + q_2 y}_{\in \mathbb{Z}})$
$\Rightarrow k|(ax+by)$ q.e.d.

Satz
Besitzt die Gleichung $ax + by = c$ eine Lösung $(x|y)$, so folgt: $ggT(a,b) | c$

Beweis:
Gilt $ax + by = c$, dann ist c eine Vielfachsumme von a und b. Nach dem letzten Satz folgt also: $ggT(a,b) | c$ q.e.d.

Satz (Teilen mit Rest)
Seien $a, b \in \mathbb{N}$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{N}_0$, so dass gilt:
$a = q \cdot b + r$ mit $0 \leq r < b$.

Beispiele:
$a = 13, b = 4$: $\underset{a}{13} = \underset{q \cdot b}{3 \cdot 4} + \underset{r}{1}$
$a = 223, b = 25$: $223 = 8 \cdot 25 + 23$

Satz
Seien $a, b \in \mathbb{N}$ und $a = q \cdot b + r$ (Teilen mit Rest).
Dann gilt: $ggT(a,b) = ggT(b,r)$

Beweis:
Wir zeigen zunächst: $ggT(a,b) \leq ggT(b,r)$ (I)
dann: $ggT(b,r) \leq ggT(a,b)$
Aus (I) und (II) folgt dann die Behauptung

(I):

$ggT(a,b) \mid a$
$ggT(a,b) \mid b$
$\Rightarrow ggT(a,b) \mid a - q \cdot b = r$ (Satz über Vielfachsumme)

$ggT(a,b) \mid r$
$\Rightarrow ggT(a,b) \leq ggT(b,r)$ (↑ Definition von ggT)

(II):

$ggT(b,r) \mid b$
$ggT(b,r) \mid r$
$\Rightarrow ggT(b,r) \mid q \cdot b + r = a$

$ggT(b,r) \mid a$
$\Rightarrow ggT(b,r) \leq ggT(a,b)$ q.e.d.

Der Euklidsche Algorithmus zur Bestimmung des ggT

$a = 126, \; b = 98$

126	98	
98	28	= Rest von 126 : 98
28	14	= Rest von 98 : 28
14	0	= Rest von 28 : 14
ggT	fertig	

$ggT(126, 98) = 14$

$a = 28, \; b = 52$

28	52
52	28
28	24
24	4
4	0

$ggT(28, 52) = 4$

Satz

Zu beliebig gewählten natürlichen Zahlen a,b gibt es ganze Zahlen x,y, so dass gilt:
$ax + by = ggT(a,b)$

Beweis:
Beschreibung eines Verfahrens, wie x und y gefunden werden (an einem Beispiel).

Erweiterter Euklidscher Algorithmus

$a = 110, \; b = 32$

$110 = 3 \cdot 32 + 14$
$32 = 2 \cdot 14 + 4$
$14 = 3 \cdot 4 + 2$
$4 = 2 \cdot 2 + 0$
(2 = ggT, 0 = fertig)

$2 = -32 \cdot 3 + 7 \cdot (110 - 3 \cdot 32) = 7 \cdot 110 - 24 \cdot 32$
$2 = 14 - 3 \cdot (32 - 2 \cdot 14) = -3 \cdot 32 + 7 \cdot 14$
$2 = 14 - 3 \cdot 4$

Ergebnis: $110 \cdot 7 + 32(-24) = 2$
$a \cdot x + b \cdot y = ggT(a,b)$

Tabellenschreibweise:

a	b	q	r	x	y	
110	32	3	14	7	-24	$= (-3-(7\cdot 3))$
32	14	2	4	-3	7	$= (1-(-3\cdot 2))$
14	4	3	2	1	-3	$= (0-(1\cdot 3))$
4	2	2	0	0	1	

ggT — fertig — Start für ↑

Weiteres Beispiel:

$a = 99$, $b = 78$

a	b	q	r	x	y
99	78	1	21	-11	14
78	21	3	15	3	-11
21	15	1	6	-2	3
15	6	2	3	1	-2
6	3	2	0	0	1

Ergebnis: $99\cdot(-11) + 78\cdot 14 = 3$

Satz

Seien $a, b, c \in \mathbb{N}$, $x, y \in \mathbb{Z}$. Dann gilt:

$ax + by = c$ hat Lösung $\Leftrightarrow$ $ggT(a,b) \mid c$

Beweis:

„$\Rightarrow$": früher Satz

„$\Leftarrow$": Der Erweiterte Euklidsche Algorithmus liefert $x_0, y_0 \in \mathbb{Z}$ mit $ax_0 + by_0 = ggT(a,b)$.

$ggT(a,b) \mid c \Rightarrow \exists k \in \mathbb{Z}: ggT(a,b)\cdot k = c \rightarrow ax_0k + by_0k = ggT(a,b)\cdot k = c$

$\Rightarrow (kx_0 \mid ky_0)$ ist Lösung. q.e.d.

Satz

(i) Ist $(x_0|y_0)$ Lösung von $ax+by=c$, dann sind alle Zahlenpaare $(x|y) = (x_0+kb \mid y_0-ka)$ mit $k \in \mathbb{Z}$ Lösungen.

(ii) Gilt $ggT(a,b) = 1$, dann sind dadurch alle Lösungen gegeben.

Beweis:

(i): $ax + by = a(x_0+kb) + b(y_0-ka) = ax_0 + akb + by_0 - bka = ax_0 + by_0 = c$.

(ii): Sei $(x|y)$ irgendeine Lösung und $ggT(a,b) = 1$.

$0 = c - c = (ax+by) - (ax_0+by_0) = a(x-x_0) + b(y-y_0)$

$\Rightarrow a(x-x_0) = -b(y-y_0)$. (1)

Da $ggT(a,b) = 1$, sind alle Primfaktoren von a in $(y-y_0)$ enthalten.

$\Rightarrow a \mid (y-y_0) \Rightarrow \exists k \in \mathbb{Z}: a\cdot k = y - y_0 \Rightarrow y = y_0 + ak$ (2) { das ist die gewünschte Darstellung für y

(2) einsetzen in (1): $a(x-x_0) = -b(y_0+ak-y_0) = -bak \quad |:a$

$x - x_0 = -bk$

$x = x_0 - bk$ { Das ist gewünschte Darstellung für x

q.e.d.