· elementare Zahlentheorie: · Primzahlen
· Teilbarkeit natürlicher Zahlen

Division mit Rest: · Dividend = Quotient · Divisor + Rest
· $a = q \cdot b + r \rightarrow 0 \leq r < b$
· in Programmieren %
· umrechnen von Dezimalsystem in x-System

Teilbarkeit: $a = q \cdot b \Rightarrow b \mid a \rightarrow b$ Teiler von a
$\rightarrow q$ komplementärer Teiler von a

Für ganze Zahlen $a, b, c, a_1, a_2, b_1, b_2 \in \mathbb{Z}$ gilt

i. $b \mid a \Longrightarrow b \mid (a \cdot c)$
ii. $b \mid a \wedge c \mid b \Longrightarrow c \mid a$
iii. $b \mid a \wedge b \mid c \Longrightarrow b \mid (ka + \ell c)$ für alle ganzen Zahlen k, ℓ
iv. $b_1 \mid a_1 \wedge b_2 \mid a_2 \Longrightarrow (b_1 \cdot b_2) \mid (a_1 \cdot a_2)$
v. $b \mid a \wedge a \mid b \Longrightarrow |a| = |b|$
vi. Für $a, b \in \mathbb{N}$ gilt $b \mid a \Longrightarrow b \leq a$
vii. Ist $c \neq 0$, dann gilt $b \mid a \Longrightarrow cb \mid ca$

Eine natürliche Zahl a (in Dezimaldarstellung) ist genau dann

- durch 10 teilbar, wenn ihre letzte Ziffer eine 0 ist,
- durch 5 teilbar, wenn ihre letzte Ziffer eine 0 oder 5 ist,
- durch 2 teilbar (gerade), wenn ihre letzte Ziffer eine $0, 2, 4, 6$ oder 8 ist,
- durch 4 teilbar, wenn die aus ihren letzten beiden Ziffern gebildete Zahl durch 4 teilbar ist,
- durch 8 teilbar, wenn die aus ihren letzten drei Ziffern gebildete Zahl durch 8 teilbar ist,
- durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist,
- durch 6 teilbar, wenn ihre Quersumme durch 3 teilbar ist und die Zahl a gerade ist,
- durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.

Primzahlen

· häufig als Zwilling (als Paar | Abstand 2)
· unendlich viele

· $p \in \mathbb{N}, p > 1$ heißt Primzahl, wenn sie nur die trivialen Teiler ± 1 und $\pm p$ besitzt

· $p \neq$ prim $\Rightarrow$ zusammengesetzt

Primzahlzerlegung

Wir kennen viele Darstellungen von 144:

$$144 = 2 \cdot 72 = 3 \cdot 48 = 6 \cdot 24 = 8 \cdot 18 = 9 \cdot 16 = 12 \cdot 12$$

Der kleinste Faktor p mit $144 = p \cdot q$ ist eine Primzahl.
Diese Darstellung einer zusammengesetzten Zahl als Produkt einer Primzahl und einer weiteren natürlichen Zahl können wir weiter bearbeiten. Am Ende sind wir an einem Produkt aus lauter Primzahlen angelangt:

$$\begin{aligned} 144 &= 2 \cdot 72 \\ &= 2 \cdot 2 \cdot 36 \\ &= 2 \cdot 2 \cdot 2 \cdot 18 \\ &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 9 \\ &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \end{aligned}$$

Beispiel

Jede natürliche Zahl $n > 1$ ist durch ein Produkt von endlich vielen Primzahlen darstellbar, die nicht notwendig verschieden sind. Bis auf die Reihenfolge der Faktoren ist diese Darstellung, die Primzahlzerlegung, eindeutig.

Fundamentalsatz der Zahlentheorie

Anzahl der Primzahlen

größte bekannte Primzahlen: 51. Mersenne-Primzahl $2^p - 1$

Sieb des Erasthostenes: $n > 1$, kein Vielfaches einer Primzahl p mit $p^2 \leq n \Rightarrow n =$ Primzahl

Beispiel:

- Die Zahl $n = 37$ ist kein Vielfaches der Primzahlen $2, 3$ und 5, die einzigen Primzahlen, deren Quadrat kleiner als 37 ist. Damit ist 37 prim.
- Alle zusammengesetzten Zahlen bis 77 enthalten in ihrer Primzahlzerlegung eine Primzahl, die kleiner oder gleich 7 ist, da $7^2 < 77$ und $11^2 > 77$.

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~

Primzahlen < 30

Algorithmus:
- alle $2 \cdot x$ raus
- nächste freie Zahl 3
- alle $3 \cdot x$ raus
- nächste freie Zahl 5
- alle $5 \cdot x$ raus
- nächste freie Zahl 7
- alle $7 \cdot x$ raus

...

Größter gemeinsamer Teiler

$a, b \in \mathbb{N}$ mit $k | a$ und $k | b$
k größte $\mathbb{N}$

$\boxed{ggT(a,b)}$

$k \Rightarrow$ größter gemeinsamer Teiler von a und b

$\Rightarrow ggT(a,b) = k$

- $ggT(a,b) = 1 \Rightarrow$ relativ prim oder teilerfremd

- ggT in Primzahlzerlegung

Euklidischer Algorithmus:

Für die natürlichen Zahlen $a > b$ wird gesetzt

$$r_0 = a, \quad r_1 = b.$$

größer kleiner $\frac{r_0}{r_1} = q_0$

Durch fortlaufende Division mit Rest erhalten wir

$$\begin{aligned} r_0 &= q_0 r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= q_1 r_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_{n-2} r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n-1} r_n. \end{aligned}$$

Dann ist $ggT(a,b) = r_n$.

Beispiel: $ggT(56,21)$

$56 : 21 = 2 \; R\,14$ $\qquad 56 = 21 \cdot 2 + 14$

$21 : 14 = 1 \; R\,7$ $\qquad 21 = 14 \cdot 1 + 7$

$14 : 7 = 2 \; R\,0$ $\qquad 14 = 7 \cdot 2$

$\Rightarrow ggT(56,21) = 7$

Beispiel: $ggT(144,60)$

$144 : 60 = 2 \; R\,24$ $\qquad 144 = 60 \cdot 2 + 24$

$60 : 24 = 2 \; R\,12$ $\qquad 60 = 24 \cdot 2 + 12$

$24 : 12 = 2 \; R\,0$ $\qquad 24 = 12 \cdot 2$

$\Rightarrow ggT(144,60) = 12$

- jeder gemeinsame Teiler von a und b teilt auch $ggT(a,b)$

Rekursive Berechnung: - $ggT(a,b) = ggT(a-b,b)$

Beispiel:

$$
\begin{aligned}
ggT(133, 91) &= ggT(91, 42) && |\, 91-42 \\
&= ggT(49, 42) && |\, 49-42 \\
&= ggT(42, 7) && |\, 42-7 \\
&= ggT(35, 7) && |\, 35-7 \\
&= ggT(28, 7) && |\, 28-7 \\
&= ggT(21, 7) && |\, 21-7 \\
&= ggT(14, 7) && |\, 14-7 \\
&= ggT(7, 7) && |\, 7-7 \\
&= 7
\end{aligned}
$$

immer größere nach Vorne

Modulare Arithmetik

Sei m eine natürliche Zahl. Zwei ganze Zahlen a und b heißen kongruent modulo m, wenn $m \mid a - b$, d. h. m teilt die Differenz von a und b. Die Bezeichnung lautet kurz

$$a \equiv b \bmod m.$$

Die Zahl m heißt Modul.

Beispiel: $8 \equiv 20 \bmod 4$, denn $4 \mid 12$

$40 \not\equiv 1 \bmod 5$, denn $5 \nmid 39$

wenn $m \mid a$, dann ist $a \equiv 0 \bmod m$

· Modul und Rest: Seien $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ gegeben. Es gilt

$$a \equiv b \bmod m$$

genau dann, wenn a und b bei Division durch den Modul m den gleichen Rest ergeben.

- Rechnen modulo m: Seien $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}$. Aus

$$a \equiv b \bmod m \quad \text{und} \quad c \equiv d \bmod m$$

folgt

$$a \pm c \equiv b \pm d \bmod m,$$
$$a \cdot c \equiv b \cdot d \bmod m.$$

$37 \equiv 17 \bmod 5 \quad \text{und} \quad 12 \equiv 7 \bmod 5$

$\Longrightarrow$

$37 + 12 = 49 \equiv 24 \bmod 5$

$37 - 12 = 25 \equiv 10 \bmod 5$

$\underbrace{37 \cdot 12}_{444} \equiv \underbrace{7 \cdot 17}_{119} \bmod 5$

Beispiel

Eindeutigkeit modulo Rechnung: - jede ganze Zahl a ist zum Modul m zu genau einer der Zahlen $0, 1, \dots, m-1$ kongruent

Kongruenz als Äquivalenzrelation:

Die Kongruenz modulo m ist eine Äquivalenzrelation $\equiv_m$ in den ganzen Zahlen mit den Äquivalenzklassen

$$[r] = \{k \cdot m + r \ : \ k \in \mathbb{Z}\}$$

von Zahlen, die bei Division durch m den gleichen Rest r $(0 \leq r \leq m-1)$ lassen.

Teilbarkeit durch 3 und 9

Bemerkung (Teilbarkeit durch 3 und 9)

MIt Hilfe von Modulo-Division kann man die Teilbarkeitsregel für die 3 beweisen. Sei

$$n = a_0 \cdot 10^0 + a_1 \cdot 10^1 + \cdots + a_k \cdot 10^k$$

mit den Ziffern $a_i, 0 \leq a_i \leq 9$. Dann gilt für die Zehnerpotenzen

$$\begin{aligned} 1 = 10^0 &\equiv 1 \bmod 3 \\ 10 = 10^1 &\equiv 1 \bmod 3 \\ 100 = 10^2 &\equiv 1 \bmod 3 \end{aligned} \qquad \begin{aligned} 1000 = 10^3 &\equiv 1 \bmod 3 \\ &\vdots \\ 10^i &\equiv 1 \bmod 3 \end{aligned}$$

damit ist

$$\begin{aligned} n &\equiv a_0 \cdot 10^0 + a_1 \cdot 10^1 + \cdots + a_k \cdot 10^k \bmod 3 \\ n &\equiv a_0 + a_1 + \cdots + a_k \bmod 3 \end{aligned}$$

Eine Zahl ist also genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist. Der Beweis für die Teilbarkeit durch 9 verläuft genauso.

$1234 \equiv 1 \bmod 3$

$1+2+3+4$

$= 10 \equiv 1 \bmod 3$

quersumme $= 9$ oder 3