1.2 Primzahlen

Es seien n, m ganze Zahlen.
Dann teilt m die Zahl n (Symb.: $m \mid n$), falls es eine ganze Zahl k gibt mit

$$n = k \cdot m$$

Beachte: Jede Zahl teilt 0 !

Eine nat. Zahl $n > 0$ heißt Primzahl, falls 1 und n die einzigen nat. Zahlen sind, die n teilen.

Die ersten Primzahlen sind: 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...
(üblicherweise wird 1 nicht zu den Primzahlen gezählt.)

Satz 1. (Primzahlzerlegung)
Es sei n eine nat. Zahl, $n \geq 2$. Dann gibt es eindeutig bestimmte Primzahlen $2 \leq p_1 < p_2 < \dots < p_k$ und pos. nat. Zahlen $a_1, \dots, a_k$ mit

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$$

■

Beispiele:

(1.) $24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 3^1$; $k=2$, $p_1=2$, $p_2=3$, $a_1=3$, $a_2=1$

(2.) $36 = 6^2 = (2 \cdot 3)^2 = 2^2 \cdot 3^2$; $k=2$, $p_1=2$, $p_2=3$, $a_1=2$, $a_2=2$

(3.) $111 = 3^1 \cdot 37^1$; $k=2$, $p_1=3$, $p_2=37$, $a_1=a_2=1$

(4.) $113 = 113^1$; $k=1$, $p_1=113$, $a_1=1$

1.3 Divisionsreste

Es seien n eine ganze Zahl, m eine nat. Zahl, $m \geq 2$.
Dann teilt m die Zahl n mit Rest r, $0 \leq r \leq m-1$, falls eine ganze Zahl k existiert mit

$$n = k \cdot m + r$$

Beachte: k, r eindeutig

Definiere Modulo-Funktion:

$\mathrm{mod}(n, m) = r$ gdw. m teilt n mit Rest r

Beispiele:

1. $\mathrm{mod}(7, 3) = 1$, denn: $7 = 2 \cdot 3 + 1$
2. $\mathrm{mod}(-7, 3) = 2$, denn: $-7 = (-3) \cdot 3 + 2$
3. $\mathrm{mod}(9, 3) = 0$, denn: $9 = 3 \cdot 3 + 0$
4. $\mathrm{mod}(-9, 3) = 0$, denn: $-9 = (-3) \cdot 3 + 0$

Satz 2.

Es seien k, n, m ganze Zahlen, $m \geq 2$.

(1.) $\mathrm{mod}(k+n, m) = \mathrm{mod}(\mathrm{mod}(k, m) + \mathrm{mod}(n, m), m)$

(2.) $\mathrm{mod}(k \cdot n, m) = \mathrm{mod}(\mathrm{mod}(k, m) \cdot \mathrm{mod}(n, m), m)$

(3.) $\mathrm{mod}(n^k, m) = \mathrm{mod}(\mathrm{mod}(n, m)^k, m)$

Beispiele:

1. $\mathrm{mod}(5+7, 4)$
   $= \mathrm{mod}(\mathrm{mod}(5, 4) + \mathrm{mod}(7, 4), 4)$
   $= \mathrm{mod}(1+3, 4)$
   $= 0$

$= \mathrm{mod}(12, 4)$

② $\mathrm{mod}(5 \cdot 7, 4)$
$= \mathrm{mod}(\mathrm{mod}(5,4) \cdot \mathrm{mod}(7,4), 4)$
$= \mathrm{mod}(1 \cdot 3, 4)$
$= 3$
$= \mathrm{mod}(35, 4)$

③ $\mathrm{mod}(5^7, 4)$
$= \mathrm{mod}(\mathrm{mod}(5,4)^7, 4)$
$= \mathrm{mod}(1^7, 4)$
$= 1$
$= \mathrm{mod}(78125, 4)$

④ $\mathrm{mod}(13^{73} \cdot 17^{25} + (-2)^{113}, 4)$
$= \mathrm{mod}(\mathrm{mod}(13,4)^{73} \cdot \mathrm{mod}(17,4)^{25} + \mathrm{mod}(-2,4)^{113}, 4)$
$= \mathrm{mod}(1^{73} \cdot 1^{25} + 2^{113}, 4)$
$= \mathrm{mod}(\mathrm{mod}(1,4) + \mathrm{mod}(2^{113}, 4), 4)$
$= \mathrm{mod}(1 + \mathrm{mod}(2^2, 4)^{56} \cdot \mathrm{mod}(2,4), 4)$
$= 1$

Es sei x eine reelle Zahl:

$\lfloor x \rfloor$ = auf größte ganze Zahl $\leq x$

$\lceil x \rceil$ = auf kleinste ganze Zahl $\geq x$

Beispiele:

① $\lfloor \frac{3}{2} \rfloor = 1$, $\lceil \frac{3}{2} \rceil = 2$

② $\lfloor -\frac{3}{2} \rfloor = -2$, $\lceil -\frac{3}{2} \rceil = -1$

Dann gilt: $n = \left\lfloor \frac{n}{m} \right\rfloor \cdot m + \mathrm{mod}(n, m)$

Denn: Für $r = \mathrm{mod}(n, m)$ gibt es k mit $n = k \cdot m + r$

Also gilt: $\left\lfloor \frac{n}{m} \right\rfloor = \left\lfloor \frac{k \cdot m + r}{m} \right\rfloor = \left\lfloor k + \underbrace{\frac{r}{m}}_{<1} \right\rfloor = k$