

Teilbarkeit

Seien $a, b \in \mathbb{Z}$. Dann gilt:

$$a \mid b \quad (\text{a teilt } b) \Leftrightarrow \exists m \in \mathbb{Z} : a \cdot m = b.$$

1. $4 \mid 20$, 因为存在整数 $m = 5$, 使得 $4 \cdot 5 = 20$.

2. $3 \mid 9$, 因为存在整数 $m = 3$, 使得 $3 \cdot 3 = 9$.

3. $5 \mid 25$, 因为存在整数 $m = 5$, 使得 $5 \cdot 5 = 25$.

Modulare Arithmetik

Für $a, b \in \mathbb{Z}$ und $c \in \mathbb{N}_{\geq 2}$ ist a Kongruent zu b modulo c , falls $a - b$ durch c teilbar ist.

↳ $a \equiv b \pmod{c}$ [manchmal auch $a \equiv_c b$]
⇒ $c \mid a - b$

Bemerkung: \equiv ist Äquivalenzrelation auf \mathbb{Z} .

↳ insb. also: $x \equiv_c y$ und $y \equiv_c z \Rightarrow x \equiv_c z$.

$$14 \mid 28$$

1. $17 \equiv 5 \pmod{12}$, 因为 $17 - 5 = 12$, 且 12 能被 12 整除。
2. $20 \equiv 2 \pmod{9}$, 因为 $20 - 2 = 18$, 且 18 能被 9 整除。
3. $35 \equiv 7 \pmod{14}$, 因为 $35 - 7 = 28$, 且 28 能被 14 整除。

Modulooperation

$z \bmod m :=$ Rest bei Division $\frac{z}{m}$.

↳ $\forall z \in \mathbb{Z} \exists q_z \in \mathbb{Z} \exists r_z \in \{0, \dots, m-1\} : z = q_z \cdot m + r_z$

↳ Rest ist immer ≥ 0

↳ Rest ist eindeutig!

Rechenregeln

Für $a, b, m \in \mathbb{Z}$ und $m \geq 2$ gilt

1) $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

2) $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$

Für $a, b, c, d, m \in \mathbb{Z}$ mit $m \geq 2$ gilt

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

$$\Rightarrow 1) (a+c) \equiv (b+d) \pmod{m}$$

$$\Rightarrow 2) (a \cdot c) \equiv (b \cdot d) \pmod{m}$$

Aufgabe 1

(i) Zeigen Sie, dass für alle Zahlen $n \in \mathbb{N}$ gilt: Wenn n^2 gerade ist, dann ist auch n gerade.

$$\begin{aligned} z \in \mathbb{Z} \text{ ist gerade} &\Leftrightarrow \exists k \in \mathbb{Z} : a = z \cdot k \quad (\Leftrightarrow a \bmod z = 0) \\ \text{ungerade} &\Leftrightarrow \exists k \in \mathbb{Z} : a = z \cdot k + 1 \quad (\Leftrightarrow a \bmod z = 1) \end{aligned}$$

Kontraposition: n ungerade $\Rightarrow n^2$ ungerade

$$\begin{aligned} \hookrightarrow n &= z \cdot k + 1 \\ \Rightarrow n^2 &= (z \cdot k + 1)^2 = 4k^2 + 4k + 1 \\ &= z(2k^2 + 2k) + 1 \end{aligned}$$

Analog zeigt man: n gerade $\Rightarrow n^2$ gerade

$$\Rightarrow n \text{ gerade} \Leftrightarrow n^2 \text{ gerade}$$

(ii) Zeigen Sie, dass für alle Zahlen $n \in \mathbb{N}$ gilt: Wenn n^2 ungerade ist, dann gibt es eine Zahl $m \in \mathbb{N}$, sodass $n^2 = 8m + 1$.

$$\cdot n^2 \text{ ungerade} \Rightarrow n \text{ ungerade}$$

$$\hookrightarrow \exists k \in \mathbb{N} : n = z \cdot k + 1$$

$$\cdot \text{Also: } n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1.$$

Wenn $k^2 + k$ gerade ist, dann sind wir fertig, denn:

$$\exists m \in \mathbb{N} : k^2 + k = 2m \Rightarrow n^2 = 4(2m) + 1 = 8m + 1.$$

\rightsquigarrow zz: $k^2 + k$ ist gerade

Fall 1: k gerade $\Rightarrow k^2$ gerade

$$\Rightarrow k^2 + k \text{ gerade}$$

Fall 2: k ungerade $\Rightarrow k^2$ ungerade

$$\Rightarrow k + k^2 \text{ gerade}$$

Aufgabe 2

(i) Beweisen Sie, dass für Primzahlen $p \geq 5$ gilt: $p^2 - 1$ ist ganzzahlig durch 24 teilbar.

Hinweis: Versuchen Sie zu zeigen, dass die Faktoren einer Produktdarstellung von $p^2 - 1$ mehrfach durch 2 und einmal durch 3 teilbar ist.

$$p \in \mathbb{N}_{\geq 2} \text{ ist Primzahl} \Leftrightarrow \forall m \in \mathbb{N}^+: m \mid p \Rightarrow m \in \{2, p\}$$

Aus der VL: Jedes $n \in \mathbb{N}_{\geq 2}$ hat eine eindeutige Primfaktorzerlegung.

$$\hookrightarrow 24 = 2 \cdot 2 \cdot 2 \cdot 3 = 8 \cdot 3$$

Wenn wir zeigen können, dass $2^3 \mid p^2 - 1$ und $3 \mid p^2 - 1$, dann folgt aus der Eindeutigkeit der PFZ, dass $p^2 - 1 = 2^3 \cdot 3 \cdot q$, $q \in \mathbb{N}$ und somit $\underbrace{2^3 \cdot 3}_{=24} \mid p^2 - 1$

Achtung: 1.A. gilt nicht $a|x \wedge b|x \Rightarrow a \cdot b|x$.

Da $p \geq 5$ gilt, ist p ungerade $\Rightarrow p^2$ ungerade

$$\hookrightarrow \text{Nach 1(ii): } \exists m \in \mathbb{N}: p^2 = 8 \cdot m + 1$$

$$\Rightarrow p^2 - 1 \text{ durch 8 teilbar}$$

Weiter ist $p^2 - 1 = (p-1)(p+1)$.

Unter beliebigen drei aufeinanderfolgenden Zahlen gibt es (genau) eine Zahl, die durch 3 teilbar ist.

\hookrightarrow Beweis: Sei $n \in \mathbb{N}$ mit $n = k \cdot 3 + \ell$ für $k \in \mathbb{N}$ und $\ell \in \{0, 1, 2\}$.

Falls $\ell = 0 \Rightarrow 3 \mid n$

Falls $\ell = 1 \Rightarrow n+2 \equiv_3 k \cdot 3 + \ell + 2 \equiv_3 k \cdot 3 + 3 \equiv_3 0$.

Falls $\ell = 2 \Rightarrow n+1 \equiv_3 k \cdot 3 + \ell + 1 \equiv_3 k \cdot 3 + 3 \equiv_3 0$.

Nun sind $p-1, p, p+1$ solche Zahlen und wegen $3 \nmid p$ ($p \geq 5$)

ist $3 \mid (p-1)$ oder $3 \mid (p+1)$

$$\Rightarrow 3 \mid (p-1)(p+1)$$

$\Rightarrow p^2 - 1$ ist durch 3 teilbar.

(i) Wir können $p^2 - 1$ umschreiben als $(p-1)(p+1)$. Da $p \geq 5$ Primzahl ist, ist die Zahl insbesondere ungerade. Nach 1(ii) folgt, dass $p^2 - 1 = 8m$ ist für ein $m \in \mathbb{N}$ und somit ist $p^2 - 1$ durch 8 teilbar.

Außerdem ist jede dritte natürliche Zahl durch 3 teilbar, also genau eine aus $(p-1), p, (p+1)$. Weil p eine Primzahl ist und $p \neq 3$, muss also $3 \mid (p-1)$ oder $3 \mid (p+1)$ und damit $3 \mid (p-1)(p+1)$ gelten.

Zudem wissen wir, dass jede zweite Zahl durch 2 teilbar ist. Da $\frac{p-1}{2} > 1$, gilt also $2 \mid \frac{p-1}{2}$ oder $2 \mid \frac{p+1}{2}$ und damit $2 \mid \frac{p-1}{2} \cdot \frac{p+1}{2}$. Insgesamt erhalten wir $2 \cdot 2 \cdot 3 \mid (p-1)(p+1)$, also $24 \mid (p-1)(p+1)$.

(ii) Zeigen Sie: Für $n \in \mathbb{N}$ (also $n > 0$) gilt $n^5 - n \equiv 0 \pmod{30}$.

Nach Def.: $n^5 - n \equiv 0 \pmod{30} \Leftrightarrow 30 \mid (n^5 - n)$

↪ PFZ von 30: $30 = 2 \cdot 3 \cdot 5$

$$\hookrightarrow n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = n(n-1)(n+1)(n^2 + 1)$$

$n-1, n, n+1$ sind Faktoren und drei aufeinanderfolgende Zahlen

$$\Rightarrow 2 \mid (n^5 - n) \text{ und } 3 \mid (n^5 - n)$$

Wir untersuchen, ob $n^5 - n$ durch 5 teilbar ist.

$$n^5 - n = n(n-1)(n+1)(n^2 + 1)$$

1. Fall: $n \equiv 0 \pmod{5}$

Dann ist n durch 5 teilbar und somit auch $n(n-1)(n+1)(n^2 + 1)$.

2. Fall: $n \equiv 1 \pmod{5}$

Dann ist $n-1$ durch 5 teilbar und somit auch $n(n-1)(n+1)(n^2 + 1)$.

3. Fall: $n \equiv 2 \pmod{5}$

Dann gilt $n^2 \equiv 2^2 \pmod{5}$ und somit $n^2 + 1 \equiv 4 + 1 \pmod{5}$. Also ist $n^2 + 1$ durch 5 teilbar und somit auch $n(n-1)(n+1)(n^2 + 1)$.

4. Fall: $n \equiv 3 \pmod{5}$

Dann gilt $n^2 \equiv 3^2 \pmod{5}$ und somit $n^2 + 1 \equiv 9 + 1 \pmod{5}$. Also ist $n^2 + 1$ durch 5 teilbar und somit auch $n(n-1)(n+1)(n^2 + 1)$.

5. Fall: $n \equiv 4 \pmod{5}$

Dann ist $n+1$ durch 5 teilbar und somit auch $n(n-1)(n+1)(n^2 + 1)$.

Für $a, b, c, d, m \in \mathbb{Z}$ mit $m \geq 2$ gilt

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

$$\Rightarrow 1) (a+c) \equiv (b+d) \pmod{m}$$

$$\Rightarrow 2) (a \cdot c) \equiv (b \cdot d) \pmod{m}$$

(iii) Beweisen Sie: Jede zusammengesetzte Zahl n (d.h. jede Zahl, die keine Primzahl ist) hat einen Primfaktor p mit $p \leq \sqrt{n}$.

Sei $n \in \mathbb{N}$ zusammengesetzt.

$$\Rightarrow \exists a, b \in \mathbb{N}_{\geq 2} : n = a \cdot b.$$

$$\text{Ang. es gilt } a, b > \sqrt{n} \Rightarrow n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n \quad \text{F}$$

Sei also obdA $a \leq \sqrt{n}$.

Fall 1: a ist prim \Rightarrow fertig.

Fall 2: a ist zusammengesetzt

Dann hat a eine PFZ aus Primzahlen die kleiner als a sind

\Rightarrow Das sind aber auch Primfaktoren von n .

(iii) Wenn n zusammengesetzt ist, so kann man n schreiben als $n = a \cdot b$, und mindestens eine der beiden Zahlen a und b ist kleiner oder gleich \sqrt{n} , da andernfalls $a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$ gilt. Ist diese Zahl keine Primzahl, so kann sie weiter zerlegt werden, wobei alle ihre Primfaktoren kleiner gleich \sqrt{n} und auch Primfaktoren von n sind. Andernfalls ist die Zahl selbst ein gesuchter Primfaktor.

Legendre's formula

Sei $n \in \mathbb{N}_{\geq 2}$ und p eine Primzahl.

Dann ist der größte Exponent $e \in \mathbb{N}$ mit $p^e \mid n!$ gegeben durch

$$e = E(n, p) := \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \quad (\text{nur endlich viele Summanden von Null verschieden})$$

\hookrightarrow ist also $n! = p^e \cdot q_1^{e_1} \cdot \dots \cdot q_k^{e_k}$ die PFZ von n mit $p \neq q_i \forall i$, so ist $e = E(n, p)$.

Beweis: • $\left\lfloor \frac{n}{p^i} \right\rfloor$ ist die Anzahl von Zahlen $1 \leq j \leq n$, die durch p^i teilbar sind.

• $\left\lfloor \frac{n}{p^2} \right\rfloor$ " ", die durch p^2 teilbar sind

• ...

$\Rightarrow \left\lfloor \frac{n}{p^i} \right\rfloor$ Faktoren steuern jeweils Faktor p bei $\Rightarrow p^{\left\lfloor \frac{n}{p^i} \right\rfloor} \mid n!$

\Rightarrow von diesen $\left\lfloor \frac{n}{p^i} \right\rfloor$ Faktoren gibt es $\left\lfloor \frac{n}{p^2} \right\rfloor$ Faktoren, die jeweils ein weiteres p als Faktor beisteuern

$\Rightarrow \dots$

$$\begin{aligned} \text{Bsp. } p=2 : 10! &= \underbrace{1 \cdot 2}_{2} \cdot \underbrace{3 \cdot 4}_{2} \cdot \underbrace{5 \cdot 6}_{2} \cdot \underbrace{7 \cdot 8}_{2} \cdot \underbrace{9 \cdot 10}_{2} \rightsquigarrow \left\lfloor \frac{10}{2} \right\rfloor = 5 \\ &= 2^5 \cdot \underbrace{1 \cdot 1 \cdot 3}_{2} \cdot \underbrace{2 \cdot 5}_{2} \cdot \underbrace{3 \cdot 7}_{2} \cdot \underbrace{4 \cdot 9}_{2} \cdot 5 \rightsquigarrow \left\lfloor \frac{10}{4} \right\rfloor = 2 \\ &= 2^7 \cdot \underbrace{1 \cdot 1 \cdot 3 \cdot 1 \cdot 5}_{2} \cdot \underbrace{3 \cdot 7 \cdot 2}_{2} \cdot 9 \cdot 5 \rightsquigarrow \left\lfloor \frac{10}{8} \right\rfloor = 1 \\ &= 2^8 \cdot 1 \cdot 1 \cdot 3 \cdot 1 \cdot 5 \cdot 3 \cdot 7 \cdot 1 \cdot 9 \cdot 5 \Rightarrow e = 5+2+1 = 8 \end{aligned}$$

und tatsächlich gilt: $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$

Wir zeigen: Das Produkt von n aufeinanderfolgenden natürlichen Zahlen ist durch $n!$ teilbar.

Sei $k \in \mathbb{N}$. Dann ist $\frac{(k+n)!}{k!} = (k+1) \cdot (k+2) \cdot \dots \cdot (k+n)$ sowie

$$l = E(n+k, p) - E(k, p) \Leftrightarrow p^l \mid (k+1) \cdot (k+2) \cdot \dots \cdot (k+n) \text{ und } l \text{ maximal.}$$

$$\hookrightarrow \text{PFZ: } (n+k)! = p^e \cdot q_1^{e_1} \cdot \dots \cdot q_k^{e_k}, \quad k! = p^{\tilde{e}} \cdot \tilde{q}_1^{\tilde{e}_1} \cdot \dots \cdot \tilde{q}_k^{\tilde{e}_k} \quad \text{mit } p \neq q_i, \quad p \neq \tilde{q}_i \quad \forall i$$

$$\Rightarrow \frac{(n+k)!}{k!} = p^{e-\tilde{e}} \cdot q, \quad \text{für } q \in \mathbb{N} \text{ mit } \text{ggT}(p, q) = 1 \text{ und } l = e - \tilde{e} \text{ maximal}$$

Weiter folgt aus $[a+b] \geq [a] + [b]$ $\forall a, b \in \mathbb{R}$ auch

$$E(n+k, p) - E(k, p) = \sum_{i=1}^{\infty} \left\lfloor \frac{k+n}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor \geq \sum_{i=1}^{\infty} \left\lfloor \frac{k}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = E(n, p).$$

Also gilt für alle Primzahlen p und $\forall i \in \mathbb{N}$:

$$p^i \mid n! \Rightarrow p^i \mid (k+1) \cdot (k+2) \cdot \dots \cdot (k+n)$$

und somit $n! \mid (k+1) \cdot (k+2) \cdot \dots \cdot (k+n)$.

Aufgabe 3

Beweise, mit einem zahlentheoretischen Argument, dass $\binom{n}{m}$ eine natürliche Zahl ist, für $n, m \in \mathbb{N}, m \leq n$.

Tipp: Betrachte wie viele Zahlen von 1 bis m durch 2 bzw. 3 bzw. 4 teilbar sind.

$$\binom{n}{m} = \frac{n!}{m!(n-m)!} = \frac{\prod_{i=1}^m (n-m+i)}{m!} = \frac{(k+1)(k+2) \cdots (k+m)}{m!} \xleftarrow[m \text{ aufeinanderfolgende Zahlen}]{} = \frac{\prod_{i=1}^m (n-m+i)}{\prod_{i=1}^m i} \xleftarrow[k \cdot z \leq x \leq m]{} \in \mathbb{N} \text{ nach Voraussetzung}$$

$$\Rightarrow \binom{n}{m} \in \mathbb{N}.$$

Insbesondere zeigen wir: Für jede natürliche Zahl z gilt: Die Anzahl an Faktoren von $\prod_{i=1}^m i$, die durch z teilbar sind ist kleiner oder gleich der Anzahl an Faktoren von $\prod_{i=1}^m (n-m+i)$, die durch z teilbar sind.

Sei k die Anzahl an Zahlen $x \in \{i \in \mathbb{N} \mid 1 \leq i \leq m\}$, sodass $z|x$. Dann gilt $m \geq k \cdot z$. Sei $n-m \equiv a \pmod{z}$, dann gilt

$$n-m-a+j \cdot z \equiv 0 \pmod{z} \text{ für } j \in \mathbb{N}$$

Zudem gilt für $1 \leq j \leq k$, dass $n-m+1 \leq n-m-a+j \cdot z \leq n$. Da gilt, dass $|\{n-m-a+j \cdot z \mid 1 \leq j \leq k\}| = k$ existieren somit mindestens k Zahlen zwischen $n-m+1$ und n , die durch z teilbar sind.

Aufgabe 4

Führe den erweiterten euklidischen Algorithmus für folgender Zahlenpaare aus:

- (i) 12, 18,
- (ii) 111, 201 und
- (iii) ~~12, 1355~~, 1355.
2949

$$\begin{array}{rcl} 2949 - 2 \cdot 1355 & = & 239 \Rightarrow 160 = 1355 - 5 \cdot 239 = 1355 - 5(2949 - 2 \cdot 1355) = -5 \cdot 2949 + 11 \cdot 1355 \\ 1355 - 5 \cdot 239 & = & 160 \Rightarrow 79 = 2949 - 2 \cdot 1355 - 1(-5 \cdot 2949 + 11 \cdot 1355) = 6 \cdot 2949 - 13 \cdot 1355 \\ 239 - 1 \cdot 160 & = & 79 \Rightarrow 2 = -5 \cdot 2949 + 11 \cdot 1355 - 2(6 \cdot 2949 - 13 \cdot 1355) = -17 \cdot 2949 + 37 \cdot 1355 \\ 160 - 2 \cdot 79 & = & 2 \Rightarrow 1 = 6 \cdot 2949 - 13 \cdot 1355 - 39(-17 \cdot 2949 + 37 \cdot 1355) \\ 79 - 39 \cdot 2 & = & 1 = 669 \cdot 2949 - 7456 \cdot 1355 \end{array}$$

$$\Rightarrow \text{ggT}(2949, 1355) = 1 = 669 \cdot 2949 - 7456 \cdot 1355$$

(i)

$$\begin{aligned} 18 - 1 \cdot 12 &= 6 \\ 12 - 2 \cdot 6 &= 0 \\ 6 &= 1 \cdot 18 - 1 \cdot 12 \end{aligned}$$

(ii)

$$\begin{aligned} 201 - 1 \cdot 111 &= 90 \Rightarrow 21 = 111 - 90 = 111 - (201 - 111) = 2 \cdot 111 - 201 \\ 111 - 1 \cdot 90 &= 21 \Rightarrow 6 = 201 - 111 - 4 \cdot (2 \cdot 111 - 201) = 5 \cdot 201 - 8 \cdot 111 \\ 90 - 4 \cdot 21 &= 6 \Rightarrow 3 = 2 \cdot 111 - 201 - 15 \cdot 201 + 27 \cdot 111 = 28 \cdot 111 - 16 \cdot 201 \\ 21 - 3 \cdot 6 &= 3 \\ 6 - 2 \cdot 3 &= 0 \\ 3 &= 1 \cdot 21 - 3 \cdot 6 \\ 3 &= 13 \cdot 21 - 3 \cdot 90 \\ 3 &= 13 \cdot 111 - 16 \cdot 90 \\ 3 &= 29 \cdot 111 - 16 \cdot 201 \end{aligned}$$

Aufgabe 3

Beweise, mit einem zahlentheoretischen Argument, dass $\binom{n}{m}$ eine natürliche Zahl ist, für $n, m \in \mathbb{N}, m \leq n$.

Tipp: Betrachte wie viele Zahlen von 1 bis m durch 2 bzw. 3 bzw. 4 teilbar sind.

$$\binom{n}{m} = \frac{n!}{m!(n-m)!} = \frac{\prod_{i=1}^m (n-m+i)}{m!} = \frac{(k+1)(k+2) \cdots (k+m)}{m!} \leftarrow m \text{ aufeinanderfolgende Zahlen}$$

$\underbrace{\quad}_{\in \mathbb{N} \text{ nach Vorüberlegung}}$

$$\Rightarrow \binom{n}{m} \in \mathbb{N}.$$

Aufgabe 4

Führe den erweiterten euklidischen Algorithmus für folgender Zahlenpaare aus:

- (i) 12, 18,
- (ii) 111, 201 und
- (iii) ~~2949~~, 1355.

~~2949~~

$$\begin{array}{rcl} 2949 & - & 2 \cdot 1355 = 239 \\ 1355 & - & 5 \cdot 239 = 160 \\ 239 & - & 1 \cdot 160 = 79 \\ 160 & - & 2 \cdot 79 = 2 \\ 79 & - & 39 \cdot 2 = 1 \end{array} \Rightarrow \begin{aligned} 160 &= 1355 - 5 \cdot 239 = 1355 - 5(2949 - 2 \cdot 1355) = -5 \cdot 2949 + 11 \cdot 1355 \\ 79 &= 2949 - 2 \cdot 1355 - 1(-5 \cdot 2949 + 11 \cdot 1355) = 6 \cdot 2949 - 13 \cdot 1355 \\ 2 &= -5 \cdot 2949 + 11 \cdot 1355 - 2(6 \cdot 2949 - 13 \cdot 1355) = -17 \cdot 2949 + 37 \cdot 1355 \\ 1 &= 6 \cdot 2949 - 13 \cdot 1355 - 39(-17 \cdot 2949 + 37 \cdot 1355) \\ &= 669 \cdot 2949 - 7456 \cdot 1355 \end{aligned}$$

$$\Rightarrow \text{ggT}(2949, 1355) = 1 = 669 \cdot 2949 - 7456 \cdot 1355$$