Teilbarkeit und Primzahlen

Fragen?

Formel für Primzahlen? Nein!

Test, ob eine Zahl eine Primzahl ist? Ja, z.B. Miller-Rabin-Test

- Teilermenge $T(a) := \{x \in \mathbb{N} \mid x|a\}$, z.B. $T(\underbrace{12}_{a}) = \{1, 2, 3, 4, 6, \underbrace{12}_{a}\}$

$|T(a)| \geq 2$ für $a > 1$.

Wegen $1|a$ $(1 \cdot a = a)$ gilt $1 \in T(a)$

Wegen $a|a$ $(a \cdot 1 = a)$ gilt $a \in T(a)$

$\Rightarrow T(a) = \{1, \ldots, a\} \Rightarrow |T(a)| \geq 2$

$\neq$ wegen $a>1$

$x=1$

d.h. $\exists x \in \mathbb{Z}: a \cdot x = a$

- Zeigen Sie: $\forall a, b \in \mathbb{N}: a|b \Leftrightarrow T(a) \subseteq T(b)$.

"$\Rightarrow$" Geg: $a|b$, d.h. $\exists q \in \mathbb{Z}: a \cdot q \overset{(*)}{=} b$.

Zzg: $T(a) \subseteq T(b)$, $\forall x: x \in T(a) \Rightarrow x \in T(b)$

Sei $x \in T(a)$, d.h. $x|a$ d.h. $\exists \tilde{q} \in \mathbb{Z}: x \cdot \tilde{q} \overset{(**)}{=} a$

Zzg: $x \in T(b)$, d.h. $x|b$ d.h.

Zzg: $\exists \tilde{\tilde{q}} \in \mathbb{Z}: x \cdot \tilde{\tilde{q}} = b$

(**) in (*): $\underbrace{(x \cdot \tilde{q}) \cdot q}_{} = b$

$x \cdot \underbrace{(\tilde{q} \cdot q)}_{=: \tilde{\tilde{q}}} = b$.

* **Teilbarkeit.** Wahr oder falsch? Warum?

1. $3 \mid 12$ ✓ $\exists q \in \mathbb{Z}: 3 \cdot q = 12$ wahr, denn es gibt $q = 4$ mit $3 \cdot 4 = 12$.
2. $2 \mid 7$ ✗ $\forall q \in \mathbb{Z}: 2 \cdot q \neq 7$. Annahme: $2 \cdot q = 7 \overset{:2}{\Rightarrow} q = \frac{7}{2} = 3{,}5 \notin \mathbb{Z}$ ↯ $(q \in \mathbb{Z})$
   [ODER: 7 nicht gerade!, ODER: 7 Primzahl!]
3. $1 \mid 8$ ✓ $1 \cdot \underbrace{8} = 8$
4. $0 \mid 5$ ✗ $\underbrace{0 \cdot \underbrace{q}}_{0} \neq 5$
5. $8 \mid 0$ ✓ $8 \cdot \underbrace{0} = 0$
6. $\forall a \in \mathbb{N} : 0 \mid a$ ✗ Gegenbsp. 4.: $0 \nmid 5 = a$
7. $\forall a \in \mathbb{N} : a \mid 0$ ✓ $a \cdot \underbrace{0} = 0$
8. $\forall a \in \mathbb{N} : a \mid a$ ✓ $a \cdot \underbrace{1} = a$

Eigener Lösungsversuch.

1. $3 \mid 12$
2. $2 \mid 7$
3. $1 \mid 8$
4. $0 \mid 5$
5. $8 \mid 0$
6. $\forall a \in \mathbb{N} : 0 \mid a$
7. $\forall a \in \mathbb{N} : a \mid 0$
8. $\forall a \in \mathbb{N} : a \mid a$

Gerade und ungerade Zahlen.

$$2\mathbb{Z} := \{2n \mid n \in \mathbb{Z}\} = \{\ldots, \overset{n=-2}{-4}, \overset{n=-1}{-2}, \overset{n=0}{0}, \overset{n=1}{2}, \overset{n=2}{4}, \ldots\} \quad \text{gerade Zahlen}$$
$$2\mathbb{Z}+1 := \{2n+1 \mid n \in \mathbb{Z}\} = \{\ldots, -3, -1, \underset{n=0}{1}, \underset{n=1}{3}, 5, \ldots\} \quad \text{ungerade Zahlen}$$

Zeigen Sie, dass eine gerade Zahl durch 2 teilbar ist und ungerade Zahlen *nicht* durch 2 teilbar sind.

Hinweis: Def. der Teilbarkeit! $x \mid a :\Longleftrightarrow \exists q \in \mathbb{Z}: x \cdot q = a$

Lösung.

- Sei $a \in 2\mathbb{Z}$ eine gerade Zahl d.h. $a = 2 \cdot n$ für ein $n \in \mathbb{Z}$, d.h. $2 \mid a$.
- Sei $a \in 2\mathbb{Z}+1$ eine ungerade Zahl, d.h. $a = 2n+1$ für ein $n \in \mathbb{Z}$. ~~Beh~~: $2 \nmid a$.

Ann: $2 \mid a$, d.h. $\exists q \in \mathbb{Z}: 2 \cdot q = \underbrace{a}_{2n+1} \Rightarrow \underbrace{2q - 2n}_{2(q-n)} = 1$ d.h. $2 \mid 1$ ↯ $(2 > 1)$

Eigener Lösungsversuch.

Exkurs zur Unendlichkeit: Hilberts Hotel

Stellen Sie sich ein Hotel mit unendlich vielen Zimmern vor. Die Zimmer-Nummern seien durch $\mathbb{N}$ gegeben:

Zimmer-Nummer:	1	2	3	4	5	...

Auf einmal kommt ein Bus mit unendlich vielen Gästen, aber schön durch nummeriert:

Gast-Nummer:	1	2	3	4	5	...

Wie kann man die Gäste verteilen? Na klar, Gast-Nr. n kommt auf Zimmer n. Dies kann man schön mit einer Zuordnung/Funktion schreiben als

$$\mathrm{id}_{\mathbb{N}} = f : \underset{\text{Gast-Nr.}}{\mathbb{N}} \to \underset{\text{Zimmer-Nr.}}{\mathbb{N}},\ n \mapsto n.$$

z.B. Gast-Nr. 5 $\mapsto$ Zimmer-Nr. 5

Soweit so gut. Jetzt kommt aber noch ein Bus mit unendlich vielen Gästen. Was nun?

Bus 1, Gast-Nr: 1 2 3 ..., Bus 2, Gast-Nr: 1 2 3 ...

ungerade Zimmer-Nr. | gerade Zimmer-Nr.

Zimmer-Nummer:	1	2	3	4	5	...

Dies kann man schön mit einer Zuordnung/Funktion schreiben als

Bus-Nr. | Gast-Nr. | Zimmer-Nr.

$$f : \{1, 2\} \times \mathbb{N} \to \mathbb{N},\ (n_{\text{Bus}}, n_{\text{Gast}}) \mapsto \begin{cases} 2 \cdot n_{\text{Gast}} - 1 & \text{falls } n_{\text{Bus}} = 1 \\ 2 \cdot n_{\text{Gast}} & \text{falls } n_{\text{Bus}} = 2 \end{cases}$$

z.B. $(\underset{\text{Bus}}{1}, 5) \mapsto 2 \cdot 5 - 1 = 9$ ← Zimmer

Auch gemeistert! Aber oje, jetzt kommen unendlich viele Busse mit unendlich vielen Gästen!!! Was nun?

Zimmer-Nr.

Bus 1, Gast-Nr:	1^{1}	2^{2}	3^{6}	4^{7}	...
Bus 2, Gast-Nr:	1^{3}	2^{5}	3^{8}	4	...
Bus 3, Gast-Nr:	1^{4}	2^{9}	3	4	...
Bus 4, Gast-Nr:	1^{10}	2	3	4	...
⋮	⋮				

Cantor'sche Diagonalverfahren

Bemerkung: $|\mathbb{R}|$-viele Gäste kann man nicht mehr in $|\mathbb{N}|$-vielen Zimmern unterbekommen!
d.h. $\neg(\exists f : \mathbb{R} \to \mathbb{N}$ bijektiv$)$

Teilermenge und Primfaktorzerlegung. Betrachten Sie folgende Zahlen:

$$18, \quad 24, \quad 256, \quad 333, \quad 341, \quad 10^{100}.$$

Googol

Bestimmen Sie jeweils die Teilermenge und Primfaktorzerlegung.

Lösung.

18: $T(18) = \{1, 2, 3, 6, 9, 18\} = \{2^i \cdot 3^j \mid 0 \le i \le 1,\ 0 \le j \le 2\}.$

$$18 = 2 \cdot \underbrace{9}_{\underbrace{3 \cdot 3}_{\text{Prim.}}} = 2^1 \cdot 3^2$$

24: $T(24) = \{1, 2, 3, 4, 6, 8, 12, 24\} = \{2^i 3^j \mid 0 \le i \le 3,\ 0 \le j \le 1\}$

$$24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$$

256: $T(256) = \{1, 2, 4, 8, 16, 32, 64, 128, 256\} = \{2^i \mid 0 \le i \le 8\}$

$$256 = 2^8$$

? Probieren!

333: $T(333) = \{1, 3, 9, 37, 111, 333\}$

$$333 = 3 \cdot \underbrace{111}_{3 \cdot 37} = 3^2 \cdot \underset{\mathbb{P}}{\underset{\cap}{37}}$$

341: $T(341) = \{1, 11, 31, 341\}$

$$341 = \underset{\mathbb{P}}{\underset{\cap}{31}} \cdot \underset{\mathbb{P}}{\underset{\cap}{11}}$$

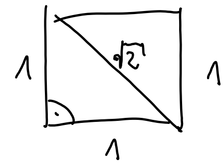
10^{100}: $T(10^{100}) = \{2^i 5^j \mid 0 \le i, j \le 100\}$

$101 \times 101 = 10.201$ Teiler

$$10^{100} = (2 \cdot 5)^{100} = 2^{100} \cdot 5^{100}$$

Eigener Lösungsversuch.

* $\sqrt{2}$ **ist irrational.** Zeigen Sie: $\sqrt{2} \notin \mathbb{Q}$



Hinweis: Nehmen Sie $\sqrt{2} = \frac{a}{b}$ mit $a, b \in \mathbb{N}$ und a, b haben keinen gemeinsamen Primfaktor (vollständig gekürzt!), und führen Sie dies zum Widerspruch!

Lösung.

$$\underline{\text{Ann:}}\ \sqrt{2} = \frac{a}{b} \overset{(\,)^2}{\Longrightarrow} 2 = \frac{a^2}{b^2} \overset{\cdot b^2}{\Longrightarrow} \boxed{2b^2 = a^2} \Longrightarrow 2 \mid a^2 = a \cdot a \Longrightarrow 2 \mid a$$

4

$$\overset{(\,)^2}{\Longrightarrow} 4 \mid a^2 \Longrightarrow \cancel{4}\,2 \mid \underbrace{b^2}_{= b\cdot b} \Longrightarrow 2 \mid b \ \lightning\ \text{(2 ist gemeinsamer Teiler von } a \text{ und } b\text{!)}$$

Eigener Lösungsversuch.

Ein einfacher Primzahltest.

Frage: Ist 76.457 eine Primzahl?

Naiver Test: Teste Teilbarkeit $d \mid 76.457$ für alle $2 \leq d \leq 76.457$.

Bessere Vorgehensweise: Teste nur mit Primzahlen $d \leq \sqrt{76.457} = 276, 5\ldots$, also folgender Algorithmus

- Teste $d = 2 \mid 76.457$. Ja? keine Primzahl, Nein? iteriere mit nächster Primzahl $d = 3 \leq 276$
- Teste $d = 3 \mid 76.457$. Ja? keine Primzahl, Nein? iteriere mit nächster Primzahl $d = 5 \leq 276$
- Teste $d = 5 \mid 76.457$. Ja? keine Primzahl, Nein? iteriere mit nächster Primzahl $d = 7 \leq 276$
- ...

Falls wir bei $d > 276$ angekommen sind, haben wir eine Primzahl!

Zur Implementierung brauchen wir aber zwei Dinge:

modulo = Rest bei Division mit Rest

- Teilbarkeits-Test $d|n \iff$ n%d==0 (in C-Code)

nächstes mal!

- Primzahlliste bis 276 $\rightarrow$ Wikipedia oder später mit Sieb des Erathostenes

Primzahltest in C. Schreiben Sie eine Funktion in C, die prüft ob ein übergebenes $n \in \mathbb{N}$ eine Primzahl ist.

Lösung. $\rightarrow$ C-Datei