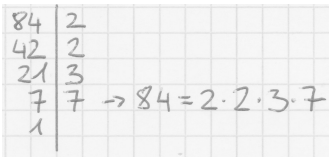
Fundamentalsatz der Arithmetik

Als Kinder lernen wir – so oder so ähnlich wie im Bild rechts dargestellt – die Primfaktorzerlegung.



Tatsächlich steckt hinter dieser Methode der
Fundamentalsatz der Arithmetik:

1) Existenz der Primfaktorzerlegung: Jede natürliche Zahl $n \geq 2$ ist ein Produkt von Primzahlen.

2) Eindeutigkeit der Primfaktorzerlegung: Diese Primfaktorzerlegung ist für jede natürliche Zahl $n \geq 2$ eindeutig bis auf die Reihenfolge der Faktoren.

Jedes Produkt von Primzahlen, das *nicht* genau aus den vier Faktoren 2, 2, 3 und 7 besteht, ist also *ungleich* 84.

Einen Beweis für den Fundamentalsatz der Arithmetik findest du am Ende dieses Arbeitsblatts.

Vielfachheiten

Meist sortieren wir die Primfaktoren aufsteigend und schreiben gleiche Primfaktoren als Potenz.

Zum Beispiel: $1176 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7 = 2^3 \cdot 3^1 \cdot 7^2$

Wir sagen auch: „Die **Vielfachheit** der Primzahl 2 in 1176 ist 3.“

Folge von Vielfachheiten

Die Primfaktorzerlegung jeder natürlichen Zahl $n \geq 1$ hat eine Folge $(v_1, v_2, v_3, \ldots)$ von Vielfachheiten:

$$n = 2^{v_1} \cdot 3^{v_2} \cdot 5^{v_3} \cdot 7^{v_4} \cdot 11^{v_5} \cdot 13^{v_6} \cdot \ \cdots$$

v_i ist die Vielfachheit der i-ten Primzahl.

Die Vielfachheiten sind ganze Zahlen $v_i \geq 0$, wobei nur *endlich* viele $v_i \neq 0$ sind.

Zum Beispiel: $1176 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^2 \cdot 11^0 \cdot 13^0 \cdot \ \cdots \implies (v_n) = (3, 1, 0, 2, 0, 0, \ldots)$

Umgekehrt liefert jede solche Folge die Primfaktorzerlegung einer natürlichen Zahl:

$$(v_n) = (3, 1, 0, 2, 0, 0, \ldots) \implies 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^2 \cdot 11^0 \cdot 13^0 \cdot \ \cdots = 1176$$

Wir schreiben dafür auch kurz: $1176 \cong (3, 1, 0, 2, 0, 0, \ldots)$

Codierung & Decodierung

a) Zerlege 1400 in Primfaktoren. Gib die zugehörige Folge von Vielfachheiten an.

$1400 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 7 = 2^3 \cdot 5^2 \cdot 7^1 \implies 1400 \cong (3, 0, 2, 1, 0, 0, \ldots)$

b) Welche natürliche Zahl steckt hinter der Folge $(0, 4, 2, 0, 0, \ldots)$ von Vielfachheiten?

$2^0 \cdot 3^4 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot \ \cdots = 2025$

Vielfachheiten & Multiplikation

Die natürliche Zahl $a \geq 1$ hat die Folge von Vielfachheiten $(v_1, v_2, v_3, \ldots)$. $a \cong (v_1, v_2, v_3, \ldots)$
Die natürliche Zahl $b \geq 1$ hat die Folge von Vielfachheiten $(w_1, w_2, w_3, \ldots)$. $b \cong (w_1, w_2, w_3, \ldots)$

Welche Folge von Vielfachheiten hat dann die Zahl $a \cdot b$?

$$a \cdot b = 2^{v_1} \cdot 2^{w_1} \cdot 3^{v_2} \cdot 3^{w_2} \cdot 5^{v_3} \cdot 5^{w_3} \cdot \ \cdots = 2^{v_1+w_1} \cdot 3^{v_2+w_2} \cdot 5^{v_3+w_3} \cdot \ \cdots$$

Also hat $a \cdot b$ die Folge von Vielfachheiten $(v_1 + w_1, v_2 + w_2, v_3 + w_3, \ldots)$.

Vielfachheiten & Teilbarkeit MmF

Es gilt $a \cong (v_1, v_2, v_3, \ldots)$ und $b \cong (w_1, w_2, w_3, \ldots)$.

Mit den beiden Folgen von Vielfachheiten können wir unmittelbar prüfen, ob a ein Teiler von b ist:

$$\boldsymbol{a \mid b \iff v_1 \leq w_1 \quad \text{und} \quad v_2 \leq w_2 \quad \text{und} \quad v_3 \leq w_3 \quad \text{und} \quad \cdots}$$

In diesem Fall gibt es eine natürliche Zahl k mit $b = a \cdot k$. Welche Folge von Vielfachheiten hat k?

$k \cong (w_1 - v_1, w_2 - v_2, w_3 - v_3, \ldots) \implies a \cdot k \cong (w_1, w_2, w_3, \ldots) \cong b$ ✓

Vielfachheiten & ggT/kgV MmF

Ermittle die Primfaktorzerlegung vom $\mathrm{ggT}(a, b)$ und vom $\mathrm{kgV}(a, b)$.

a) $a = 2^3 \cdot 3^5 \cdot 7^1, \quad b = 2^2 \cdot 3^1 \cdot 5^4$

$\mathrm{ggT}(a, b) = 2^2 \cdot 3^1$

$\mathrm{kgV}(a, b) = 2^3 \cdot 3^5 \cdot 5^4 \cdot 7^1$

b) $a = 3^5 \cdot 11^2, \quad b = 2^3 \cdot 5^2 \cdot 7^4$

$\mathrm{ggT}(a, b) = 1$

$\mathrm{kgV}(a, b) = 2^3 \cdot 3^5 \cdot 5^2 \cdot 7^4 \cdot 11^2$

Vielfachheiten & ggT/kgV MmF

Es gilt $a \cong (v_1, v_2, v_3, \ldots)$ und $b \cong (w_1, w_2, w_3, \ldots)$.

Mit den beiden Folgen können wir also $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ unmittelbar berechnen:

1) $\boldsymbol{\mathrm{ggT}(a, b) \cong (\min\{v_1, w_1\}, \min\{v_2, w_2\}, \min\{v_3, w_3\}, \ldots)}$

2) $\boldsymbol{\mathrm{kgV}(a, b) \cong (\max\{v_1, w_1\}, \max\{v_2, w_2\}, \max\{v_3, w_3\}, \ldots)}$

$\min\{v_1, w_1\}$ ist die kleinere der beiden Zahlen. („Minimum“). $\max\{v_1, w_1\}$ ist die größere der beiden Zahlen. („Maximum“)

$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = a \cdot b$ MmF

Erkläre, warum $\boldsymbol{\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = a \cdot b}$ gilt.

Allgemein gilt: $\min\{v_i, w_i\} + \max\{v_i, w_i\} = v_i + w_i$

$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b)$ und $a \cdot b$ haben also die gleiche Folge von Vielfachheiten und sind somit gleich.

Vielfachheiten & Teilerfremdheit MmF

Es gilt $a \cong (v_1, v_2, v_3, \ldots)$ und $b \cong (w_1, w_2, w_3, \ldots)$.

Wie kannst du mit den beiden Folgen unmittelbar prüfen, ob a und b teilerfremd sind?

Teilerfremd heißt, dass a und b keinen gemeinsamen Teiler außer 1 haben, also $\mathrm{ggT}(a, b) = 1$.

a und b sind genau dann teilerfremd, wenn $\min\{v_i, w_i\} = 0$ für alle i gilt.
Es darf also *nicht dieselbe* Primzahl in *beiden* Primfaktorzerlegungen vorkommen.

Gemeinsame Faktoren kürzen MmF

Erkläre, warum die beiden Zahlen $\frac{a}{\text{ggT}(a,b)}$ und $\frac{b}{\text{ggT}(a,b)}$ teilerfremd sind.

$a \cong (v_1, v_2, v_3, \ldots) \quad b \cong (w_1, w_2, w_3, \ldots)$
$\implies \frac{a}{\text{ggT}(a,b)} \cong (v_1 - \min\{v_1, w_1\}, v_2 - \min\{v_2, w_2\}, \ldots)$
$\implies \frac{b}{\text{ggT}(a,b)} \cong (w_1 - \min\{v_1, w_1\}, w_2 - \min\{v_2, w_2\}, \ldots)$

Für alle i gilt $v_i - \min\{v_i, w_i\} = 0$ oder $w_i - \min\{v_i, w_i\} = 0$.
Die beiden Zahlen sind also teilerfremd.

Wo sind die Primfaktoren? MmF

Begründe die folgende Aussage: $\left.\begin{array}{l} n \mid a \cdot b \\ \text{ggT}(n, a) = 1 \end{array}\right\} \implies n \mid b$

$a \cong (v_1, v_2, v_3, \ldots) \quad b \cong (w_1, w_2, w_3, \ldots) \quad n \cong (x_1, x_2, x_3, \ldots)$

$$\implies \left.\begin{array}{ll} x_i \leq v_i + w_i & \text{für alle } i \\ \min\{x_i, v_i\} = 0 & \text{für alle } i \end{array}\right\} \overset{(\star)}{\implies} x_i \leq w_i \quad \text{für alle } i$$

$(\star)$ ist korrekt, weil $x_i = 0$ oder $v_i = 0$ gilt. In beiden Fällen folgt $x_i \leq w_i$.

Division MmF

Begründe die folgenden beiden Äquivalenzen:

$$\boldsymbol{a \mid b \cdot c} \overset{\textbf{1)}}{\iff} \frac{a}{\text{ggT}(a,b)} \mid \frac{b}{\text{ggT}(a,b)} \cdot c \overset{\textbf{2)}}{\iff} \boldsymbol{\frac{a}{\text{ggT}(a,b)} \mid c}$$

Diese Eigenschaft wird sich am Arbeitsblatt – Kongruenz und Restklassen als nützlich erweisen.

1) Es gilt: $b \cdot c = a \cdot k \iff \frac{b}{\text{ggT}(a,b)} \cdot c = \frac{a}{\text{ggT}(a,b)} \cdot k$

2) $\Longrightarrow$
$\frac{a}{\text{ggT}(a,b)}$ und $\frac{b}{\text{ggT}(a,b)}$ sind teilerfremd.

Aus $\frac{a}{\text{ggT}(a,b)} \mid \frac{b}{\text{ggT}(a,b)} \cdot c$ folgt deshalb $\frac{a}{\text{ggT}(a,b)} \mid c$.

$\Longleftarrow$
Aus $A \mid B$ folgt immer $A \mid B \cdot C$.

Lemma von Euklid  MmF

Das **Lemma von Euklid** ist eine grundlegende Aussage der Zahlentheorie:

„Wenn eine Primzahl ein Produkt von zwei Zahlen teilt, dann teilt sie mindestens einen der Faktoren."

$$p \mid a \cdot b \implies p \mid a \quad \text{oder} \quad p \mid b \quad \text{für alle Primzahlen } p \text{ und } a, b \in \mathbb{Z}$$

Das Lemma von Euklid gilt dann auch für Produkte mit endlich vielen Faktoren:

$$p \mid a \cdot \underbrace{(b \cdot c)}_{\in \mathbb{Z}} \implies p \mid a \quad \text{oder} \quad p \mid b \cdot c \implies p \mid a \quad \text{oder} \quad p \mid b \quad \text{oder} \quad p \mid c$$

„Wenn eine Primzahl p ein Produkt teilt, dann teilt p mindestens einen der Faktoren."

Lemma von Euklid (Beweis)

Wir beweisen das **Lemma von Euklid** ohne die Eindeutigkeit der Primfaktorzerlegung zu verwenden. Tatsächlich ist die Eindeutigkeit der Primfaktorzerlegung eine Folgerung aus dem Lemma von Euklid.

Warum folgt also aus $p \mid a \cdot b$, dass die Primzahl p eine der Zahlen a oder b teilen muss?
Wenn p ein Teiler von a ist, dann ist nichts mehr zu begründen.
Wenn p *kein* Teiler von a ist, dann gilt $\mathrm{ggT}(p,a) = 1$, da p eine Primzahl ist.

1) Der Euklidische Algorithmus liefert ganze Zahlen r und s, für die gilt: $p \cdot r + a \cdot s = \underbrace{\mathrm{ggT}(p,a)}_{=1}$

2) Wir multiplizieren mit b auf beiden Seiten der Gleichung: $p \cdot r \cdot b + a \cdot b \cdot s = b$

3) Da p ein Teiler von $a \cdot b$ gibt es eine ganze Zahl k mit $a \cdot b = k \cdot p$.

Wir setzen ein: $p \cdot r \cdot b + k \cdot p \cdot s = b \implies p \cdot \underbrace{(r \cdot b + k \cdot s)}_{\in \mathbb{Z}} = b$

Wenn p kein Teiler von a ist, dann muss also p ein Teiler von b sein.

Existenz der Primfaktorzerlegung (Beweis)

Warum kann jede natürliche Zahl $n \geq 2$ als Produkt vom Primfaktoren geschrieben werden?

Indirekter Beweis: Angenommen, es gibt eine natürliche Zahl ≥ 2, die *keine* Primfaktorzerlegung hat.

1) Wähle unter allen solchen Zahlen die *kleinste* Zahl m, die *keine* Primfaktorzerlegung (PFZ) hat.

2) Dann kann m *keine* Primzahl sein. Denn jede Primzahl hat eine PFZ, nämlich sich selbst.

3) Also gibt es natürliche Zahlen a und b mit $m = a \cdot b$ und $1 < a, b < m$. Sonst wäre m eine Primzahl.

4) Dann müssen aber a und b jeweils eine PFZ haben. m ist ja die *kleinste* Zahl ≥ 2 ohne PFZ.

5) Dann hat aber auch m eine PFZ: $m = a \cdot b = \underbrace{(\text{PFZ von } a) \cdot (\text{PFZ von } b)}_{\text{PFZ von } m}$ ↯ Widerspruch zu **1)**

Die Annahme war also falsch. *Jede* natürliche Zahl $n \geq 2$ muss eine Primfaktorzerlegung haben.

Eindeutigkeit der Primfaktorzerlegung (Beweis)

Warum ist die PFZ jeder natürlichen Zahl $n \geq 2$ eindeutig bis auf die Reihenfolge der Faktoren?

Indirekter Beweis: Angenommen, es gibt eine natürliche Zahl ≥ 2 mit verschiedenen PFZ.

1) Wähle unter allen solchen Zahlen die *kleinste* Zahl m, die verschiedene PFZ hat:

$$m = p_1 \cdot p_2 \cdot \ldots \cdot p_r = P_1 \cdot P_2 \cdot \ldots \cdot P_s$$

2) Dann kann m *keine* Primzahl sein. Denn jede Primzahl hat eine *eindeutige* PFZ, nämlich sich selbst.
Beide Zerlegungen haben also mindestens zwei Primfaktoren: $r, s \geq 2$

3) Es kann keine Primzahl in beiden Zerlegungen vorkommen.
Wenn eine Primzahl p in beiden Zerlegungen vorkommt, dann ist $\frac{m}{p}$ eine *kleinere* Zahl als m, die verschiedene PFZ hat. ↯

4) $p_1 \mid m \implies p_1 \mid P_1 \cdot P_2 \cdot \ldots \cdot P_s \implies p_1 \mid P_1$ oder $p_1 \mid P_2$ oder $\cdots$ oder $p_1 \mid P_s$ Lemma von Euklid

5) Wenn eine Primzahl eine Primzahl teilt, dann sind sie gleich. Sonst wäre die größere Zahl keine Primzahl.

6) Die Primzahl p_1 kommt also in beiden PFZ vor. ↯ Widerspruch zu **3)**

Die Annahme war also falsch.
Die PFZ *jeder* natürlichen Zahl $n \geq 2$ muss bis auf die Reihenfolge der Faktoren eindeutig sein.