# Lösungen der Übungsaufgaben zu **Kapitel 7**

**Ü1**:
Sei $p \in \mathbb{P}$ beliebig gewählt.

IA: $n = 2$ :
Zu zeigen ist $p \mid a_1 \cdot a_2 \Rightarrow p \mid a_1 \vee p \mid a_2$, dies ist aber genau die Aussage von Satz 7.1 und damit bereits bewiesen.

IS: Sei $k \in \mathbb{N}$ mit $k \geq 2$ beliebig aber fest.

IV: Für beliebige k-viele natürliche Zahlen $a_1, a_2, ..., a_k$ gelte:
$p \mid a_1 \cdot a_2 \cdot ... \cdot a_k \Rightarrow p \mid a_1 \vee p \mid a_2 \vee ... \vee p \mid a_k$

IB: Dann gilt auch für (k+1)-viele nat. Zahlen $a_1, a_2, ..., a_k, a_{k+1}$:
$p \mid a_1 \cdot a_2 \cdot ... \cdot a_k \cdot a_{k+1} \Rightarrow p \mid a_1 \vee p \mid a_2 \vee ... \vee p \mid a_k \vee p \mid a_{k+1}$

Gelte also $p \mid a_1 \cdot a_2 \cdot ... \cdot a_k \cdot a_{k+1}$

$\Rightarrow$ $p \mid (a_1 \cdot a_2 \cdot ... \cdot a_k) \cdot a_{k+1}$ (ASS „$\cdot$“)

$\Rightarrow$ $p \mid s \cdot a_{k+1}$ mit $s := a_1 \cdot a_2 \cdot ... \cdot a_k$ und $s \in \mathbb{N}$ (Multiplikation in $\mathbb{N}$ abgeschlossen)

$\Rightarrow$ $p \mid s \vee p \mid a_{k+1}$ (Satz 7.1)

Statt $p \mid s$ läßt sich auch schreiben $p \mid a_1 \cdot a_2 \cdot ... \cdot a_k$ und mit IV gilt dann: $p \mid a_1 \vee p \mid a_2 \vee ... \vee p \mid a_k$.

$\Rightarrow$ $(p \mid a_1 \vee p \mid a_2 \vee ... \vee p \mid a_k) \vee p \mid a_{k+1}$ (**IV**)

$\Rightarrow$ $p \mid a_1 \vee p \mid a_2 \vee ... \vee p \mid a_k \vee p \mid a_{k+1}$ (ASS „$\vee$“)

Insgesamt ist nach dem Induktionsaxiom damit die Behauptung bewiesen.

t

**Ü2**:
heuristische Beispiele:
$k_1 = 2+1 = 3,\ 3 \in \mathbb{P}$
$k_2 = 2 \cdot 3+1 = 7,\ 7 \in \mathbb{P}$
$k_3 = 2 \cdot 3 \cdot 5+1 = 31,\ 31 \in \mathbb{P}$
$k_4 = 2 \cdot 3 \cdot 5 \cdot 7+1 = 211,\ 211 \in \mathbb{P}$
$k_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11+1 = 2311,\ 2311 \in \mathbb{P}$
$k_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13+1 = 30031$, aber $30031 \notin \mathbb{P}$!,
da $30031 = 59 \cdot 509$

D.h. k ist nicht stets eine Primzahl, da z.B. $k_6$ keine Primzahl ist (was schwer zu sehen ist, da die echten Teiler von 30031 ziemlich groß sind).

Wichtig festzuhalten ist also, daß auch eine ganze Reihe von Beispielen, für die die Aussage gilt, noch keinerlei Gewähr dafür gibt, daß die Behauptung immer gilt. In diese Falle tappt man hier sehr schnell.

**Ü3**:

Zu zeigen: Jede natürliche Zahl besitzt eine Primfaktorzerlegung.

Da Primzahlen - wie im großen GEPAD in der Vorbemerkung auf Seite 209 herausgestellt - eine PFZ besitzen, bleibt im folgenden Beweis noch zu zeigen, daß selbiges auch für alle zusammengesetzten Zahlen gilt. Deshalb wird im **IA** mit der ersten zusammengesetzten Zahl begonnen.

**IA**: Die erste zusammengesetzte Zahl $z_1 = 4$ hat eine Primfaktorzerlegung, nämlich die Zerlegung $2 \cdot 2$.

**IS**: Sei $k \in \mathbb{N}$ mit $k \geq 1$ beliebig aber fest.

**IV**: Die ersten k zusammengesetzten Zahlen $z_1, z_2, ..., z_k$ haben eine Primfaktorzerlegung.

**IB**: Dann hat auch die (k+1)-te zusammengesetzte Zahl $z_{k+1}$ eine PFZ.

$z_{k+1}$ sei die (k+1)-te zusammengesetzte Zahl. Für eine zusammengesetzte Zahl n gilt nach Definition „Zusammengesetzte Zahl“:
Es gibt natürliche Zahlen $a, b \neq 1$ mit $z_{k+1} = a \cdot b$.

Für a und b gilt zudem: $a < z_{k+1}$ und $b < z_{k+1}$ (vgl. Beweis der Charakterisierung im großen GEPAD, S. 203).

Entweder sind a oder b nun prim oder sie sind wiederum zusammengesetzt, in jedem Fall besitzen sie jedoch eine PFZ:

1. Fall: a und b prim: vgl. Vorbemerkung

2. Fall: entweder a oder b prim: O.B.d.A.: a prim, dann ist b zusammengesetzt.
a hat dann laut Vorbemerkung eine PFZ, b hat eine PFZ nach IV, da b ($< z_{k+1}$) eine der ersten k zusammengesetzten Zahlen ist.

3. Fall: a und b zusammengesetzt: Da $a,b < z_{k+1}$ gilt, haben a und b nach IV eine PFZ.

In allen drei Fällen ist eine PFZ von $z_{k+1} = a \cdot b$ das Produkt der PFZ'en von a und b, d.h. die (k+1)-te zusammengesetzte Zahl $z_{k+1}$ hat eine PFZ.

Insgesamt ist nach P3 damit die Behauptung bewiesen.

t

**Ü4**:

1.Fall: p und q sind beides ungerade Zahlen,
(d.h. sowohl p als auch q sind ungleich 2).
Sowohl die Summe als auch die Differenz zweier ungerader Zahlen ist jedoch stets gerade.
Da nun p und q beide größer als 2 sind, ist die Summe p+q auf jeden Fall größer als 2.
Insgesamt gilt dann: $2 \mid p+q$ und $p+q>2$

$$\Rightarrow \quad p+q \notin \mathbb{P}$$

Die Betrachtung des ersten Falls zeigt also, daß eine der beiden Primzahlen gerade, d.h. gleich 2 sein muß.

2.Fall: p oder q ist eine gerade Zahl,
d.h. p oder q ist 2.
Es muß gelten p>q, da sonst p–q negativ ist (und damit keine Primzahl).
Dann gilt: $q = 2$.
D.h. für mögliche Lösungen für p und q gilt:
$q = 2$ und $p+2 \in \mathbb{P}$ und $p-2 \in \mathbb{P}$ .
Eine mögliche Lösung ergibt sich für $p = 5$,
da $5+2 \in \mathbb{P}$ und $5-2 \in \mathbb{P}$ .

Drei Primzahlen der Form p–2, p und p+2 bilden einen sogenannten Primzahldrilling. Ob es weitere Primzahldrillinge neben (3/5/7) gibt, soll in der nächsten Aufgabe untersucht werden.

**Ü5**:
Ein Primzahldrilling ist (3/5/7). Bei jedem anderen Primzahldrilling muß $p_1>3$ gelten, da 2 für $p_1$ offensichtlich nicht in Betracht kommt.

Suche nach weiteren Primzahldrillingen:
Untersucht werden jeweils drei aufeinanderfolgende ungerade Zahlen (da gerade Zahlen größer 2 nicht prim sein können):

5, 7, 9: kein Primzahldrilling
9, 11, 13: kein Primzahldrilling
11, 13, 15: kein Primzahldrilling
13, 15, 17: kein Primzahldrilling
15, 17, 19: kein Primzahldrilling
17, 19, 21: kein Primzahldrilling
usf.

Es fällt auf, daß bei allen Versuchen, einen weiteren Primzahldrilling zu konstruieren, dieses daran scheitert, daß jeweils eine der drei Zahlen (die hier jeweils durch Unterstreichen gekennzeichnet sind) durch 3 teilbar ist.

Nun zum Beweis:

Gilt nun $p_1>3$ für $p_1 \in \mathbb{P}$, so folgt: $3 \nmid p_1$ .
[3 ist die einzige Primzahl, die von 3 geteilt wird, bei jeder größeren käme zu den beiden Teilern 1 und p als weiterer Teiler 3 hinzu.]

Wenn gilt $3 \nmid p_1$, so läßt $p_1$ bei Division durch 3 entweder den Rest 1 oder den Rest 2 (vgl. 🕮 Division mit Rest):

1.Fall: $p_1$ läßt den Dreierrest 1, d.h. es gibt ein $q \in \mathbb{N}_0$ mit $p_1 = q \cdot 3+1$ (Satz über Division mit Rest).
Für $p_2$ läßt sich dann folgern:

$$\begin{aligned} p_2 &= p_1+2 \\ &= (q \cdot 3+1)+2 \\ &= q \cdot 3+3 \\ &= 3(q+1) \end{aligned}$$

d.h. $3 \mid p_2$ (nach def. Teilbarkeit, $q+1 \in \mathbb{N}_0$ , da $q \in \mathbb{N}_0$ ),
dann ist $p_2$ ($>p_1>3$) aber keine Primzahl.

2.Fall: $p_1$ läßt den Dreierrest 2,
d.h. es gibt ein $q \in \mathbb{N}_0$ mit $p_1 = q \cdot 3+2$ .

[Setzt man diese Summe analog zum ersten Fall für $p_1$ in den Ausdruck für $p_2$ ein, so wird man feststellen, daß dieses nicht zu dem erwünschten Widerspruch führt. Daher untersucht man, was sich ergibt, wenn man in den Ausdruck für $p_3$ einsetzt.]

$p_3 = p_2+2 = (p_1+2)+2 = p_1+4$
Aus $p_1 = q \cdot 3+2$ ergibt sich dann:

$$\begin{aligned} p_3 &= p_1+4 \\ &= (q \cdot 3+2)+4 \\ &= q \cdot 3+6 \\ &= 3(q+2) \end{aligned}$$

d.h. $3 \mid p_3$
dann ist $p_3$ aber keine Primzahl.

Insgesamt ergibt sich damit, daß für $p_1 \neq 3$ $p_2$ und $p_3$ nicht gleichzeitig auch Primzahlen sein können, d.h. 3 ist die einzige Zahl, die für $p_1$ in Frage kommt, also ist (3/5/7) der einzige Primzahldrilling.

t

**Ü6**:
Bem.: Zur Definition 🕮 Fakultät ($n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot n$) vgl. Unterkap. 10.3 .

Laut Tip überlegt man sich, durch welche Zahlen n!+k teilbar ist, falls k eine Zahl zwischen 2 und n ist.

Beispiel (für $n \geq 6$):
Sei $k = 6$, dann gilt $6 \mid n!$, da n! den Faktor 6 explizit enthält
($n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \underline{6} \cdot ... \cdot n$).
Mit $6 \mid 6$ folgt dann (Satz 6.3 (ii)), daß 6 auch die Summe teilt: $6 \mid n!+6$ .

Allgemein gilt $k \mid k$ (Satz 6.1 (ii)) und (da $k \leq n$) auch $k \mid n!$ .
Damit folgt (Satz 6.3 (ii)): $k \mid n!+k$ .

Also hat <u>jede</u> Zahl n!+k mit $2 \leq k \leq n$ (dies ist eine Zahl zwischen n!+2 und n!+n) neben den Teilern 1 und sich selbst noch (mindestens) den Teiler k und ist somit keine Primzahl.

Wählt man eine beliebige Zahl n, so lassen sich (n–1) viele aufeinanderfolgende Zahlen (von n!+2 bis n!+n) finden, die zusammengesetzt sind.
Sei beispielsweise $n = 4$, dann sind die drei Zahlen 4!+2, 4!+3 und 4!+4 zusammengesetzt.
Durch Wahl eines <u>großen</u> n, kann man demnach auch (beliebig) große Lücken finden.

t

**Ü7**:
Nein, es gibt keine Primzahlen, die diese Aussage erfüllen:
Aus $p \mid n+1$ und $p \mid n$ folgt $p \mid 1$ (Satz 6.3 (iv)). Aus $p \mid 1$ folgt aber (nach Satz 6.4 (i)) $p \leq 1$ und damit erhält man einen Widerspruch zu def. Primzahl.

**Ü8**:

a)

In der PFZ der gesuchten Zahl ($n \in \mathbb{N}$) kommen höchstens die Primfaktoren 2, 3 und 5 vor, d.h. $n = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3}$ mit $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{N}_0$.

Für die Anzahl der Teiler t(n) soll gelten: $t(n) = 8$.

Nach Satz 7.5 wird die Anzahl der Teiler berechnet, indem die um 1 erhöhten Exponenten der Primfaktoren multipliziert werden, also:

$t(n) = (\alpha_1+1) \cdot (\alpha_2+1) \cdot (\alpha_3+1)$

Da die Anzahl der Teiler also ein Produkt (mit maximal 3 Faktoren) ist, wird 8 in Faktoren zerlegt - und zwar auf alle Arten, auf die dieses möglich ist:

1. $8 = 2 \cdot 2 \cdot 2 \Rightarrow t(n) = (1+1) \cdot (1+1) \cdot (1+1)$

   $\Rightarrow (\alpha_1+1) \cdot (\alpha_2+1) \cdot (\alpha_3+1) = (1+1) \cdot (1+1) \cdot (1+1)$ (Satz 7.5)

   $\Rightarrow \alpha_1 = 1 \ \wedge \ \alpha_2 = 1 \ \wedge \ \alpha_3 = 1$

   d.h. n hat drei Primfaktoren, die jeweils den Exponenten 1 haben:

   Einzige Möglichkeit für n: $2^1 \cdot 3^1 \cdot 5^1 = \mathbf{30}$

2. $8 = 2 \cdot 4$, dann hat die gesuchte Zahl n zwei Primfaktoren, von denen der eine den Exponenten 1 (1+1 ergibt dann den ersten Faktor, nämlich 2) und der andere den Exponenten 3 hat:

   $t(n) = (1+1) \cdot (3+1) \Rightarrow n = p_k^1 \cdot p_m^3$ mit $k \neq m$ und $p_k, p_m \in \{2,3,5\}$

   $2^1 \cdot 3^3 = \mathbf{54}$, $2^1 \cdot 5^3 = \mathbf{250}$, $2^3 \cdot 3^1 = \mathbf{24}$, $2^3 \cdot 5^1 = \mathbf{40}$, $3^1 \cdot 5^3 = \mathbf{375}$,

   $3^3 \cdot 5^1 = \mathbf{135}$

3. $8 = 1 \cdot 8$, dann hat n nur einen Primfaktor, da 1 von einem Exponenten 0 herrührt (d.h. von einer Primzahl, die in der PFZ von n nicht enthalten ist!): $n = p_k^7$ mit $p_k \in \{2,3,5\}$

   $2^7 = \mathbf{128}$, $3^7 = \mathbf{2187}$, $5^7 = \mathbf{78125}$

Es gibt also insgesamt 10 Möglichkeiten für die gesuchte Zahl n.

b)

Um die Zahlen zu bestimmen, die 20 Teiler und vier verschiedene Primfaktoren haben, bestimmt man zuerst (analog zu Teil a)) die multiplikativen Zerlegungen der 20:

$20 = 2 \cdot 2 \cdot 5$ $\qquad$ $20 = (2 \cdot 2) \cdot 5 = 4 \cdot 5$

$20 = 2 \cdot (2 \cdot 5) = 2 \cdot 10$ $\qquad$ $20 = 2 \cdot 2 \cdot 5 = 1 \cdot 20$

Dies sind alle unterschiedlichen Zerlegungen der 20 in Faktoren (dies wird besonders deutlich, wenn man von der PFZ $2 \cdot 2 \cdot 5$ ausgeht).

Gäbe es nun eine Zahl mit den gewünschten Eigenschaften, so müßte sich 20 in ein Produkt von 4 Faktoren ungleich 1 zerlegen lassen. [Der Faktor 1 liefert keine Erkenntnisse über die gesuchte Zahl, da er von einem Exponenten 0 herrührt, d.h. vom Auftreten des Faktors 1 läßt sich nicht auf einen weiteren Primfaktor in der Zahl schließen].

In den Zerlegungen tauchen jedoch nie vier Faktoren auf, die größer als 1 sind. Damit kann es die gesuchte Zahl nicht geben.

**Ü9**:
Da a eine Quadratzahl ist, gibt es eine natürliche Zahl k, die mit sich selbst multipliziert a ergibt: $a = k^2$
Sei k in seiner kanonischen PFZ gegeben:

$$k = \prod_{i=1}^{\infty} p_i^{\alpha_i} \quad \text{mit } p_i \in \mathbb{P},\ \alpha_i \in \mathbb{N}_0,\ i \in \mathbb{N}$$

$$\Rightarrow \quad a = \left( \prod_{i=1}^{\infty} p_i^{\alpha_i} \right)^2$$

$$\Rightarrow \quad a = \prod_{i=1}^{\infty} (p_i^{\alpha_i})^2 \qquad \text{(Potenzgesetz)}$$

$$\Rightarrow \quad a = \prod_{i=1}^{\infty} p_i^{2\alpha_i} \qquad \text{(Potenzgesetz)}$$

$$\Rightarrow \ t(a) = \prod_{i=1}^{\infty} (2\alpha_i + 1) \qquad \text{(Satz 7.5)}$$

Da $2\alpha_i+1$ (mit $\alpha_i \in \mathbb{N}_0$) stets eine ungerade Zahl ist, ist keiner der Faktoren durch 2 teilbar, daher ist auch das gesamte Produkt nicht durch 2 teilbar. Andernfalls ergäbe sich ein Widerspruch mit Satz 7.2, da $2 \in \mathbb{P}$:

Ann.: $2 \mid \prod_{i=1}^{\infty} (2\alpha_i + 1)$

$$\Rightarrow \quad 2 \mid 2\alpha_1 + 1 \ \vee \ 2 \mid 2\alpha_2 + 1 \ \vee \ \ldots \ \vee \ 2 \mid 2\alpha_k + 1 \ \vee \ \ldots \qquad \text{(SATZ 7.2)}$$

Dies ist ein Widerspruch zu „$2\alpha_i + 1$ ist stets eine ungerade Zahl".

Somit ist die Anzahl der Teiler t(a) ungerade.

Gilt auch die Umkehrung? **JA**

Sei $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ und damit $t(a) = \prod_{i=1}^{\infty} (\alpha_i + 1)$.
Da t(a) ungerade ist, kann keiner der Faktoren $(\alpha_i+1)$ gerade sein, da andernfalls auch t(a) gerade wäre (TRANS„$\mid$"). Also ist für alle $i \in \mathbb{N}$ $\alpha_i$ gerade, d.h. es gibt natürliche Zahlen $k_i$ mit $\alpha_i = 2k_i$.
Somit ergibt sich für die PFZ von a: $a = \prod_{i=1}^{\infty} p_i^{2k_i} = \prod_{i=1}^{\infty} (p_i^{k_i})^2 = \left( \prod_{i=1}^{\infty} p_i^{k_i} \right)^2$
Damit ist a eine Quadratzahl.

t

Bemerkung:
Was hier gezeigt worden ist, ist eine sehr naheliegende Erkenntnis:
Die 🕮 Teilermenge einer beliebigen Zahl n setzt sich zusammen aus Paaren von Teilern, die miteinander multipliziert n ergeben. Den Partner, den jeder Teiler hat, nennt man Komplementärteiler (vgl. Kap. 6, Ü9). Da nun Teiler und Komplementärteiler immer paarweise auftreten, gibt es insgesamt immer geradzahlig viele Teiler - außer bei Quadratzahlen.
Genau bei den Quadratzahlen stimmt einer Teiler mit seinem Komplementärteiler überein: Bei der Quadratzahl $a^2$ ist a der Komplementtärteiler zu a, so daß sich hier eine ungerade Anzahl von Teilern ergibt.

**Ü10**:

a)

$12 = 2^2 \cdot 3\ ,\ 216 = 2^3 \cdot 3^3$

$\Rightarrow\ a = 2^{\alpha_1} \cdot 3^{\alpha_2}$

$\wedge\ \ b = 2^{\beta_1} \cdot 3^{\beta_2}$

Wegen $a \mid 2^3 \cdot 3^3$ (= kgV(a,b)) und $b \mid 2^3 \cdot 3^3$ kommen in der PFZ von a und b keine anderen Primfaktoren als im kgV vor (nach Satz 7.4 enthält der Teiler einer Zahl dieselben Primfaktoren dieser Zahl mit kleineren oder gleichen Exponenten).

Nach Satz 7.6 gilt:

$ggT(a,b) = 2^{\min(\alpha_1,\beta_1)} \cdot 3^{\min(\alpha_2,\beta_2)} = 2^2 \cdot 3 \ \Rightarrow\ \min(\alpha_1,\beta_1) = 2 \ \wedge\ \min(\alpha_2,\beta_2) = 1$

$kgV(a,b) = 2^{\max(\alpha_1,\beta_1)} \cdot 3^{\max(\alpha_2,\beta_2)} = 2^3 \cdot 3^3 \ \Rightarrow\ \max(\alpha_1,\beta_1) = 3 \ \wedge\ \max(\alpha_2,\beta_2) = 3$

Für $\alpha_1$ und $\beta_1$ gilt demnach: $\alpha_1 = 2 \ \wedge\ \beta_1 = 3$
oder $\alpha_1 = 3 \ \wedge\ \beta_1 = 2$

und für $\alpha_2$ und $\beta_2$ gilt: $\alpha_2 = 1 \ \wedge\ \beta_2 = 3$
$\alpha_2 = 3 \ \wedge\ \beta_2 = 1$

Damit ergeben sich folgende oder Möglichkeiten für a und b:

❶ $a = 2^2 \cdot 3^1 = 12\ ,\ b = 2^3 \cdot 3^3 = 216$

❷ $a = 2^2 \cdot 3^3 = 108\ ,\ b = 2^3 \cdot 3^1 = 24$

❸ $a = 2^3 \cdot 3^1 = 24\ ,\ b = 2^2 \cdot 3^3 = 108$

❹ $a = 2^3 \cdot 3^3 = 216\ ,\ b = 2^2 \cdot 3^1 = 12$

b)

Sei $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ mit $p_i \in \mathbb{P},\ \alpha_i \in \mathbb{N}_0, i \in \mathbb{N}$ $\qquad 315 = 3^2 \cdot 5 \cdot 7$

Dann gilt nach Satz 7.6 :

$$ggT(a,315) = 3^{\min(2,\alpha_2)} \cdot 5^{\min(1,\alpha_3)} \cdot 7^{\min(1,\alpha_4)}$$

(wegen $ggT(a,315) \mid 315$ kommen keine anderen Primfaktoren in Frage)

$$\Rightarrow\ (ggT(a,315))^2 = 3^{2 \cdot \min(2,\alpha_2)} \cdot 5^{2 \cdot \min(1,\alpha_3)} \cdot 7^{2 \cdot \min(1,\alpha_4)} \qquad \text{(Potenzgesetz)}$$

Aus Satz 7.6 folgt ferner: $kgV(a,315) = 3^{\max(2,\alpha_2)} \cdot 5^{\max(1,\alpha_3)} \cdot 7^{\max(1,\alpha_4)}$

Damit läßt sich die zu untersuchende Gleichung wie folgt umformen:

$$(ggT(a,315))^2 = kgV(a,315)$$

$$\Leftrightarrow\ \ 3^{2 \cdot \min(2,\alpha_2)} \cdot 5^{2 \cdot \min(1,\alpha_3)} \cdot 7^{2 \cdot \min(1,\alpha_4)} = 3^{\max(2,\alpha_2)} \cdot 5^{\max(1,\alpha_3)} \cdot 7^{\max(1,\alpha_4)}$$

$$\Leftrightarrow\ \ 2 \cdot \min(2,\alpha_2) = \max(2,\alpha_2) \ \wedge\ 2 \cdot \min(1,\alpha_3) = \max(1,\alpha_3)$$

$$\wedge\ 2 \cdot \min(1,\alpha_4) = \max(1,\alpha_4) \qquad \text{(wegen FusZa)}$$

Da sich nach FusZa jede natürliche Zahl (ungleich 1) eindeutig in ein Produkt von Primzahlen zerlegen läßt, können zwei gleiche Zahlen ( $(ggT(a,315))^2 = kgV(a,315)$ ) nicht unterschiedliche Zerlegungen haben, insbesondere bedeutet dies hier, daß die Exponenten der Primzahlpotenzen an jeder Stelle übereinstimmen müssen.

Damit gilt:

❶ $2 \cdot \min(2,\alpha_2) = \max(2,\alpha_2) \Rightarrow \alpha_2 = 1 \vee \alpha_2 = 4$,

denn: $\min(2,\alpha_2) \in \{0,1,2\} \Rightarrow 2 \cdot \min(2,\alpha_2) \in \{0,2,4\} \Rightarrow \max(2,\alpha_2) \in \{0,2,4\}$

$\Rightarrow \max(2,\alpha_2) \in \{2,4\}$ ($\max(2,\alpha_2)$ ist nach def. mindestens 2)

$\Rightarrow \max(2,\alpha_2) = 2 \vee \max(2,\alpha_2) = 4$

$\Rightarrow \alpha_2 = 1 \vee \alpha_2 = 2 \vee \alpha_2 = 4$

Prüft man diese Fälle hinsichtlich der Bedingung $2 \cdot \min(2,\alpha_2) = \max(2,\alpha_2)$, so stellt man fest, daß nur die beiden obigen Fälle in Frage kommen.

❷ $2 \cdot \min(1,\alpha_3) = \max(1,\alpha_3) \Rightarrow \alpha_3 = 2$ ,

denn: $\min(1,\alpha_3) \in \{0,1\} \Rightarrow 2 \cdot \min(1,\alpha_3) \in \{0,2\} \Rightarrow \max(1,\alpha_3) \in \{0,2\}$

$\Rightarrow \alpha_3 = 2$

❸ $2 \cdot \min(1,\alpha_4) = \max(1,\alpha_4) \Rightarrow \alpha_4 = 2$ (mit analoger Argumentation)

Für den Primfaktoren der PFZ der gesuchten Zahl a gibt es somit folgende Möglichkeiten:

$p_2 = 3$ kann mit den Exponenten 1 oder 4 vorkommen
$p_3 = 5$ kann nur mit dem Exponenten 2 vorkommen
$p_4 = 7$ kann ebenfalls nur mit dem Exponenten 2 vorkommen

Für a existieren also die beiden folgenden Möglichkeiten:

$a = 3^1 \cdot 5^2 \cdot 7^2 = \mathbf{3675}$ oder $a = 3^4 \cdot 5^2 \cdot 7^2 = \mathbf{99225}$

**Ü11**:

Nach FusZa gilt: a,b,c besitzen eindeutige (kanonische) PFZ:

Sei $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \ldots$ ,

$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} \cdot \ldots$ ,

$c = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k} \cdot \ldots$

mit $\alpha_i$, $\beta_i$, und $\gamma_i \in \mathbb{N}_0$ .

Dann ergibt sich: $b \cdot c = p_1^{\beta_1+\gamma_1} \cdot p_2^{\beta_2+\gamma_2} \cdot \ldots \cdot p_k^{\beta_k+\gamma_k} \cdot \ldots$ (Potenzrechnung)

Die erste Voraussetzung läßt sich dann nach Satz 7.4 wie folgt umformen:

$a \mid b \cdot c \Leftrightarrow \alpha_i \le \beta_i + \gamma_i$ für alle $i \in \mathbb{N}$ ⊠

Nach Voraussetzung gilt außerdem: $\mathrm{ggT}(a,b) = 1$

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

$$\Leftrightarrow \quad \prod_{i=1}^{\infty} p_i^{\min(\alpha_i,\beta_i)} = 1 \qquad \text{(Satz 7.6)}$$

Ein Produkt natürlicher Zahlen ($p_i^{\min(\alpha_i,\beta_i)} \in \mathbb{N}$ ) ergibt genau dann 1, wenn jeder einzelne Faktor 1 ist, d.h. es muß gelten: $p_i^{\min(\alpha_i,\beta_i)} = 1$ für alle $i \in \mathbb{N}$ . Da $p_i \ge 2$ und $p_i^0 = 1$, müssen alle Exponenten 0 sein:

$\Rightarrow \quad \min(\alpha_i,\beta_i) = 0 \quad$ für alle $i \in \mathbb{N}$

$\Rightarrow \quad \alpha_i = 0 \ \vee \ \beta_i = 0 \quad$ für alle $i \in \mathbb{N}$ ✪

Sei $i \in \mathbb{N}$ beliebig, wegen ✪ gilt einer der beiden Fälle:

1. Fall: $\alpha_i = 0$

$\Rightarrow \quad \alpha_i \le \gamma_i \qquad$ (da $\gamma_i \in \mathbb{N}_0$)

2. Fall: $\beta_i = 0$

$\Rightarrow \quad \alpha_i \le 0+\gamma_i \qquad$ (✉)

$\Rightarrow \quad \alpha_i \le \gamma_i$

Also gilt für alle $i \in \mathbb{N}$: $\alpha_i \le \gamma_i$

$\Rightarrow \ a \mid c \qquad$ (Satz 7.4)

t

**Ü12**:

Nach FusZa gilt: a,b,n besitzen eindeutige (kanonische) PFZ:

Sei $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \ldots$ ,

$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} \cdot \ldots$ ,

$n = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k} \cdot \ldots$

mit $p_i \in \mathbb{P}$, $\alpha_i,\beta_i,\gamma_i \in \mathbb{N}_0$ und $i \in \mathbb{N}$.

Dann ergibt sich: $n \cdot a = p_1^{\gamma_1+\alpha_1} \cdot p_2^{\gamma_2+\alpha_2} \cdot \ldots \cdot p_k^{\gamma_k+\alpha_k} \cdot \ldots$

und $n \cdot b = p_1^{\gamma_1+\beta_1} \cdot p_2^{\gamma_2+\beta_2} \cdot \ldots \cdot p_k^{\gamma_k+\beta_k} \cdot \ldots$

Nach Satz 7.6 gilt : $ggT(a,b) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i,\beta_i)}$

$\Leftrightarrow \quad n \cdot ggT(a,b) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i,\beta_i)+\gamma_i}$ (Potenzrechnung)

Nach Satz 7.6 gilt ferner: $ggT(na,nb) = \prod_{i=1}^{\infty} p_i^{\min(\gamma_i+\alpha_i,\ \gamma_i+\beta_i)}$

Damit läßt sich die zu zeigende Aussage wie folgt umformen:

$n \cdot ggT(a,b) = ggT(na,nb)$

$\Leftrightarrow \quad \prod_{i=1}^{\infty} p_i^{\min(\alpha_i,\beta_i)+\gamma_i} = \prod_{i=1}^{\infty} p_i^{\min(g_i+a_i,g_i+b_i)}$

$\Leftrightarrow \quad \min(\alpha_i,\beta_i) + \gamma_i = \min(\gamma_i+\alpha_i\ ,\ \gamma_i+\beta_i)$ für alle $i \in \mathbb{N}$ ❀

Es gilt: $\min(\alpha_i,\beta_i) = \alpha_i \ \vee \ \min(\alpha_i,\beta_i) = \beta_i$

1. Fall: $\min(\alpha_i,\beta_i) = \alpha_i$

$\Rightarrow$ $\min(\alpha_i,\beta_i) + \gamma_i = \alpha_i + \gamma_i$

UND $\min(\gamma_i+\alpha_i , \gamma_i+\beta_i) = \alpha_i + \gamma_i$ (da aus $\alpha_i \le \beta_i$ folgt $\alpha_i+\gamma_i \le \beta_i+\gamma_i$)

$\Rightarrow$ $\min(\alpha_i,\beta_i) + \gamma_i = \min(\gamma_i+\alpha_i , \gamma_i+\beta_i)$

2. Fall: $\min(\alpha_i,\beta_i) = \beta_i$

Dieser Fall verläuft analog zum 1. Fall - für beide Minima ergibt sich $\beta_i + \gamma_i$ und damit die Gleichheit.

In beiden Fällen erhält man, daß die Minima an allen Stellen ($i\in\mathbb{N}$) gleich sind und wegen ❀ gilt damit die zu zeigende Aussage.

t

**Ü13**:
Seien a,b in ihrer kanonischen PFZ wie folgt gegeben:

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \ldots$

$\wedge$ $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} \cdot \ldots$ mit $p_i\in\mathbb{P}$, $\alpha_i,\beta_i \in \mathbb{N}_0$ und $i\in\mathbb{N}$

$\Rightarrow$ $kgV(a,b) = \prod_{i=1}^{\infty} p_i^{\max(\alpha_i,\beta_i)}$ (Satz 7.6)

Es gilt also:

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \ldots$ und $kgV(a,b) = \prod_{i=1}^{\infty} p_i^{\max(\alpha_i,\beta_i)}$

$\Rightarrow ggT(a,kgV(a,b)) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i,\ \max(\alpha_i,\beta_i))}$ 💣 (Satz 7.6)

Nach def. Maximum gilt: $\alpha_i \le \max(\alpha_i,\beta_i)$ für alle $i\in\mathbb{N}$,

so ergibt sich: $\min(\alpha_i, \max(\alpha_i,\beta_i)) = \alpha_i$ für alle $i\in\mathbb{N}$ (def. Minimum)

$\Rightarrow ggT(a,kgV(a,b)) = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ ($i\in\mathbb{N}$) (💣)

$= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \ldots$

$= a$

t