# Inhaltsverzeichnis

# Teil I

# Elementare Zahlentheorie

Aufgaben aus dem Buch: Reinhold Remmert und Peter Ullrich (2008). *Elementare Zahlentheorie*. Springer. ISBN: 978-3-7643-7730-4.

## 1 Seite 28

### 1.1 Aufgabe 1

Seien $a, b, c$ Ziffern aus der Menge $\{0, 1, 2, \ldots, 9\}$ und $a \neq 0$. Zeigen Sie: 13 teilt die natürliche Zahl *abcabc* (Zifferndarstellung).

*Beweis.* Es werden die Differenzen betrachtet, wenn sich $a, b, c$ um einen Wert verändern:

$$\begin{aligned} a = 1 \text{ nach } a = 2 &: \triangle 100100 \\ b = 0 \text{ nach } b = 1 &: \triangle \ 10010 \\ c = 0 \text{ nach } c = 1 &: \triangle \quad 1001 \end{aligned}$$

Es ist zu sehen $13 \mid 1001$ mit $1001 = 13 \cdot 77$. Hieraus folgt $13 \mid 10010, 13 \mid 100100$ und damit auch $13 \mid 100100 \cdot a + 10010 \cdot b + 1001 \cdot a = abcabc$. □

## 1.2 Aufgabe 2

Sei $n$ eine natürliche Zahl, $n > 1$. Beweisen Sie: Aus $n \mid (n-1)! + 1$ folgt $n \in \mathbb{P}$.

*Beweis.*

**Lemma 1.** *Sei $n \in \mathbb{N}$ eine zusammengesetzte Zahl, $n \neq 4$. Dann gilt:*

$$n \mid (n-1)!$$

*Beweis.* Es ist $n = ab$ mit $a, b \geq 2$. Wir können $(n-1)!$ wie folgt aufschreiben:

$$n = ab \mid 1 \cdot 2 \cdots a(a+1)(a+2) \cdots (a+b) \cdots (ab-1) = (ab-1)!$$

Das Produkt $b$ aufeinanderfolgender Terme enthält zwangsweise ein Vielfaches von $b$. Außerdem enthält $(ab-1)!$ $a$ und somit $ab \mid (ab-1)!$.

Die obige Schreibweise ist korrekt, denn wir haben

$$\begin{aligned} & a + b \leq ab - 1 \\ \iff \quad & 0 \leq ab - a - b - 1 \\ \iff \quad & 2 \leq \underbrace{(a-1)}_{\geq 1} \underbrace{(b-1)}_{\geq 2} \end{aligned}$$

mit $a, b \geq 2$ und niemals $a = b = 2$, da $n \neq 4$. Also mindestens einer der beiden $\geq 3$. □

Lemma 1 zeigt, dass $n \mid (n-1)!$ für alle $n$ zusammengesetzt. Man kann also schließen, dass alle Zahlen mit der Eigenschaft $n \mid (n-1)! + 1$ nicht zusammengesetzt und daher Prim sind. □

## 1.3 Aufgabe 3

Sei $p_n$ die $n$-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$ usw. Zeigen Sie: $p_n \leq 2^{2^{n-1}}$ für alle $n \geq 1$.

*Beweis.* □

## 1.4 Aufgabe 4

Sei $p$ eine Primzahl. Beweisen Sie: $p$ ist ein Teiler von $\binom{p}{v}$ für $1 \leq v < p$.

*Beweis.* Per Definition gilt:

$$\binom{p}{v} = \frac{p(p-1) \cdot \ldots \cdot (p-v+1)}{v!}$$

Es gilt außerdem:

$$\binom{n}{v} \in \mathbb{N} \quad \text{für alle } n, v \in \mathbb{N}$$

Die Primzerlegung des Nenners muss vollständig in der des Zählers vorhanden sein. Wegen $p > v$ ist $p$ jedoch niemals Teil dieser Zerlegung und kann im Zähler nicht gekürzt werden. Es folgt $p \mid \binom{p}{v}$. □

Es kann nun eine verallgemeinerte Eigenschaft der eben beschriebenen Teilbarkeit beschrieben werden. Der Beweis des folgenden Lemmas wir in der nächsten Aufgabe hilfreich sein.

**Lemma 2.** *Sei $p$ eine Primzahl. Dann gilt*

$$p \mid \binom{p^n}{v} \quad \textit{für alle } n \in \mathbb{N} \textit{ und } 1 \leq v < p^n$$

*Beweis.* Die folgende Identität ist korrekt:

$$\binom{p^n}{v} = \frac{p^n}{v}\binom{p^n - 1}{v - 1}$$
$$v\binom{p^n}{v} = p^n\binom{p^n - 1}{v - 1}$$

Es ist somit zu sehen, dass $p^n \mid v\binom{p^n}{v}$.

1. Sind $p$ und $v$ teilerfremd, gilt $p^n \mid \binom{p^n}{v}$ und es bleibt nichts mehr zu zeigen
2. Anderenfalls ist $v = p^{n-a}q$ mit $a \in \mathbb{N}$ und $0 < a \leq n$ (bemerke $p$ und $q$ sind teilerfremd und $a > 0$ wegen $v < p^n$)

Es gilt daher

$$p^{n-a}q\binom{p^n}{v} = p^n\binom{p^n-1}{v-1}$$
$$q\binom{p^n}{v} = p^a\binom{p^n-1}{v-1}$$

und somit $p^a \mid \binom{p^n}{v}$. Außerdem gilt $p \mid p^a$ und letztendlich $p \mid \binom{p^n}{v}$. □

## 1.5 Aufgabe 5

Seien $p \in \mathbb{P}$, $n \in \mathbb{N}^\times$ und $a, b \in \mathbb{Z}$. Zeigen Sie durch Induktion nach $n$: $p$ ist ein Teiler von $((a+b)^{p^n} - (a^{p^n} + b^{p^n}))$.

*Beweis.* Es ist $B$ die Menge aller Zahlen $n \in \mathbb{N}^\times$, sodass für alle $a, b \in \mathbb{Z}$ die behauptete Teilbarkeit richtig ist. Es ist $1 \in B$, denn es gilt nach dem Binomischen Lehrsatz (Remmert und Ullrich 2008, S. 19):

$$\begin{aligned}(a+b)^p - (a^p + b^p) &= \left[a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} ab^{p-1} + b^p\right] - (a^p + b^p) \\ &= \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} ab^{p-1}\end{aligned}$$

$p$ teilt die Summe, da jeder Summand ist als ein Vielfaches von $\binom{p}{1}, \ldots, \binom{p}{p-1}$ durch $p$ teilbar ist. Sei $n \in B$. Um $n+1 \in B$ zu verifizieren, rechnen wir wie folgt:

$$(a+b)^{p^{n+1}} - (a^{p^{n+1}} + b^{p^{n+1}}) = \binom{p^{n+1}}{1} a^{p^{n+1}-1}b + \cdots + \binom{p^{n+1}}{p^{n+1}-1} ab^{p^{n+1}-1}$$

Nach Lemma 2 gilt die obige Eigenschaft auch in diesem Fall. □

## 1.6 Aufgabe 6

Sei $n \geq 2$ eine natürliche Zahl. Zeigen Sie: $n^4 + 4^n$ ist keine Primzahl.

*Beweis.* Wir formen um:

$$\begin{aligned} n^4 + 4^n &= (n^2)^2 + (2^n)^2 \\ &= (n^2 + 2^n)^2 - (22^n n^2) \\ &= (n^2 + 2^n)^2 - (2^{n+1} n^2) \\ &= (n^2 + 2^n)^2 - (2^{\frac{n+1}{2}} n)^2 \qquad \text{bemerke } a^2 - b^2 = (a+b)(a-b) \\ &= (n^2 + 2^n + 2^{\frac{n+1}{2}} n)(n^2 + 2^n - 2^{\frac{n+1}{2}} n) \end{aligned}$$

Es ist zu erkennen, dass für ungerade $n$ immer ein Faktor entsteht. Für $n$ gerade, ist die Zahl offensichtlich keine Primzahl, da $n^4 + 4^n > 2$ und $2 \mid n^4 + 4^n$. □

# 2 Seite 33

## 2.1 Aufgabe 3

Seien $a$ und $b$ positive natürliche Zahlen mit der Eigenschaft, dass es keine Primzahl gibt, die zugleich $a$ und $b$ teilt. Beweisen Sie: Gibt es ein $c \in \mathbb{N}$ mit $ab = c^2$, so existieren $x, y \in \mathbb{N}$ mit $a = x^2$ und $b = y^2$.

*Beweis.* Es ist $c$ eine beliebige zusammengesetzte Zahl und $c^2 = p_1^{2m_1} p_2^{2m_2} \cdot \ldots \cdot p_r^{2m_r}$ ihre Primzerlegung. Man überlege jetzt, wie diese Faktoren zwischen $a$ und $b$ verteilt sein können. Damit keine Primzahl in $a$ oder $b$ gemeinsam vorkommt, müssen die Primpotenzen $p_i^{2m_i}$ mit $i = 1, \ldots, r$ vollständig zwischen $a$ und $b$ verteilt sein. Somit sind es immer Quadratzahlen. □

Zum Beispiel:

$$
\begin{aligned}
20^2 = 2^4 5^2 \qquad & 1) \quad ab = (2^4)(5^2) = 4^2 \cdot 5^2 \\
210^2 = 2^2 3^2 5^2 7^2 \qquad & 1) \quad ab = (2^2 3^2 5^2)(7^2) = 30^2 \cdot 7^2 \\
& 2) \quad ab = (2^2 3^2)(5^2 7^2) = 6^2 \cdot 35^2 \\
& 3) \quad ab = (2^2)(3^2 5^2 7^2) = 2^2 \cdot 105^2
\end{aligned}
$$

## 2.2 Aufgabe 4

Es seien $a, b$ natürliche Zahlen, für die gilt: $a \mid b^2, b^2 \mid a^3, a^3 \mid b^4, b^4 \mid a^5, \ldots$.
Zeigen sie: $a = b$.

*Beweis.* Es sind

$$\begin{aligned} a &= X_1^{m_1} \cdot X_2^{m_2} \cdot \ldots \cdot X_r^{m_r} \\ b &= Y_1^{n_1} \cdot Y_2^{n_2} \cdot \ldots \cdot Y_r^{n_r} \qquad X_i, Y_i \in \mathbb{P} \text{ mit } i = 1, \ldots, r \end{aligned}$$

die Primzerlegungen von $a$ und $b$. Es ist direkt festzuhalten, dass $X_i = Y_i$ für alle $i = 1, \ldots, r$. Hätte $a$ mehr Primfaktoren wie $b$, verletzt dies das Teilbarkeitskriterium (Remmert und Ullrich 2008, S. 33) in $a \mid b^2$; hätte $a$ weniger, verletzt dies $b^2 \mid a^3$. Es bleibt zu zeigen, dass auch die Primpotenzen nicht verschieden sind. Angenommen $a \neq b$ und es werden zwei Fälle unterschieden:

**1)** Es gilt $0 < a < b$ und $a$ hat somit mindestens einen Primfaktoren der Form $X_i^{m_i - s_i}$ mit $0 < s_i < m_i$. Für diesen Beweis reicht es genau einen dieser Faktoren zu untersuchen und wir schreiben $X^{m-s}$ ohne den Index $i$. Es werden die folgenden Fakten aufgeschrieben:

$$\begin{aligned} X^{m-s} &\mid X^{2m} & X^{2m} &= X^{m-s} \cdot X^{m+s} \\ X^{2m} &\mid X^{3m-3s} & X^{3m-3s} &= X^{2m} \cdot X^{m-3s} \\ X^{3m-3s} &\mid X^{4m} & X^{4m} &= X^{3m-3s} \cdot X^{m+3s} \\ X^{4m} &\mid X^{5m-5s} & X^{5m-5s} &= X^{4m} \cdot X^{m-5s} \\ &\vdots & &\vdots \\ X^{(2k-1)m-(2k-1)s} &\mid X^{2km} & X^{2km} &= X^{(2k-1)m-(2k-1)s} \cdot X^{m+(2k-1)s} \\ X^{2km} &\mid X^{(2k+1)m-(2k+1)s} & X^{(2k+1)m-(2k+1)s} &= X^{2km} \cdot X^{m-(2k+1)s} \end{aligned}$$

Es lassen sich die folgenden Ungleichungen ableiten oder direkt ablesen:

$$\begin{aligned} & 2km \geq 2km - m - 2ks + s \\ \iff \quad & 0 \geq -m - 2ks + s \\ \iff \quad & m + (2k-1)s \geq 0 \end{aligned} \tag{1}$$

$$\begin{aligned} & 2km + m - 2ks - s \geq 2km \\ \iff \quad & m - (2k+1)s \geq 0 \end{aligned} \tag{2}$$

Es ist zu sehen, dass Ungleichung 1 für alle $k, m, s$ wahr ist. In 2 wird $k = m$ gewählt und man führt die ursprüngliche Behauptung mit $(1-2s)m - s \geq 0$ zum Widerspruch. Der Term $1 - 2s$ ist wegen $s > 0$ immer negativ.

**2)** Es gilt $a > b$ und $a$ hat somit mindestens einen Primfaktoren der Form $X_i^{m_i+s_i}$ mit $s_i > 0$. Es wird nach demselben Prinzip wie zuvor aufgeschrieben

$$\begin{aligned} X^{(2k-1)m+(2k-1)s} \mid X^{2km} \qquad & X^{2km} = X^{(2k-1)m+(2k-1)s} \cdot X^{m-(2k-1)s} \\ X^{2km} \mid X^{(2k+1)m+(2k+1)s} \qquad & X^{(2k+1)m+(2k+1)s} = X^{2km} \cdot X^{m+(2k+1)s} \end{aligned}$$

und die folgenden Ungleichungen abgelesen:

$$m - (2k-1)s \geq 0 \tag{3}$$

$$m + (2k+1)s \geq 0 \tag{4}$$

Es ist zu sehen, dass Ungleichung 4 für alle $k, m, s$ wahr ist. In 3 wird $k = m + 1$ gewählt und man führt die ursprüngliche Behauptung mit $(1-2s)m - s \geq 0$ zum Widerspruch.

Es folgt $a = b$. □

# 3 Seite 53

## 3.1 Aufgabe 1

Sei $p$ eine Primzahl, $a, b$ seien von Null verschiedene rationale Zahlen, $a + b \neq 0$. Zeigen Sie: $w_p(a + b) \geq \min(w_p(a), w_p(b))$

*Beweis.* Sei $m = \min(w_p(a), w_p(b))$. Es gilt $p^m \mid a$, $p^m \mid b$ und damit auch $p^m \mid a + b$. Wir schreiben $a + b = p^m \cdot v$ und zeigen durch umformen:

$$\begin{aligned} w_p(a+b) &= w_p(p^m \cdot v) \\ &= w_p(p^m) + w_p(v) \\ &= m + w_p(v) \\ &= \min(w_p(a), w_p(b)) + w_p(v) \end{aligned}$$

Es ist zu sehen $w_p(a + b) \geq \min(w_p(a), w_p(b))$. □

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |

## 3.2 Aufgabe 2

Für $x$ reell bezeichne $\lfloor x \rfloor$ die größte ganze Zahl $m$ mit $m \leq x$. Zeigen Sie, dass für $p$ eine Primzahl und $n \in \mathbb{N}$ beliebig gilt:

$$w_p(n!) = \sum_{i=0}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

*Beweis.* □

# Literaturverzeichnis

Remmert, Reinhold und Peter Ullrich (2008). *Elementare Zahlentheorie*. Springer. ISBN: 978-3-7643-7730-4.