

Inhaltsverzeichnis

I	Elementare Zahlentheorie	1
1	Seite 28	1
1.1	Aufgabe 1	1
1.2	Aufgabe 2	2
1.3	Aufgabe 3	3
1.4	Aufgabe 4	4
1.5	Aufgabe 5	6
1.6	Aufgabe 6	7
2	Seite 33	8
2.1	Aufgabe 3	8
2.2	Aufgabe 4	9
3	Seite 53	11
3.1	Aufgabe 1	11
3.2	Aufgabe 2	12
	Literaturverzeichnis	13

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 $\{0, 1, 2, \dots, 9\}$ 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:

$$a = 1 \text{ nach } a = 2 : \triangle 100100$$

$$b = 0 \text{ nach } b = 1 : \triangle 10010$$

$$c = 0 \text{ nach } c = 1 : \triangle 1001$$

Es ist zu sehen $13 \mid 1001$ mit $1001 = 13 \cdot 77$. Hieraus folgt $13 \mid 10010, 13 \mid 100100$ und damit auch $13 \mid 1001 \cdot v_1 + 10010 \cdot v_2 + 100100 \cdot v_3 = abcabc$ mit $v_{1,2,3} \in \{0, 1, 2, \dots, 9\}$. \square

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. Ist n eine zusammengesetzte Zahl $n = ab$ mit $a, b > 1$, dann gilt $a \mid (n-1)!$ und dadurch $a \nmid (n-1)! + 1$ weshalb ebenfalls $n \nmid (n-1)! + 1$.

Der restliche Beweis mit dem Satz von Wilson

□

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:

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

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 $p \mid \binom{p}{v}$. \square

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

Lemma 1. *Sei p eine Primzahl. Dann gilt*

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

Beweis. Die folgende Identität ist korrekt:

$$\begin{aligned} \binom{p^n}{v} &= \frac{p^n}{v} \binom{p^n-1}{v-1} \\ v \binom{p^n}{v} &= p^n \binom{p^n-1}{v-1} \end{aligned}$$

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

$$\begin{aligned}p^{n-a}q\binom{p^n}{v} &= p^n\binom{p^n-1}{v-1} \\ q\binom{p^n}{v} &= p^a\binom{p^n-1}{v-1}\end{aligned}$$

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):

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

Jeder Summand ist als Produkt von $\binom{p}{1}, \dots, \binom{p}{p-1}$ durch p teilbar. Sei $n \in B$. Um $n+1 \in B$ zu verifizieren, rechnen wir wie folgt:

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

Wieder ist zu sehen, dass jeder Term als ein Vielfaches von $\binom{p^{n+1}}{1}, \dots, \binom{p^{n+1}}{p^{n+1}-1}$ durch p teilbar ist. \square

1.6 Aufgabe 6

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

Beweis.

□

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 $c^2 = p_1^{2m_1} p_2^{2m_2} \cdot \dots \cdot p_r^{2m_r}$ 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 $i = 1, \dots, r$ vollständig zwischen a und b verteilt sein. Somit sind es immer Quadratzahlen. \square

Zum Beispiel:

$$20^2 = 2^4 5^2 \quad 1) \quad ab = (2^4)(5^2) = 4^2 \cdot 5^2$$

$$210^2 = 2^2 3^2 5^2 7^2 \quad 1) \quad ab = (2^2 3^2 5^2)(7^2) = 30^2 \cdot 7^2$$

$$2) \quad ab = (2^2 3^2)(5^2 7^2) = 6^2 \cdot 35^2$$

$$3) \quad ab = (2^2)(3^2 5^2 7^2) = 2^2 \cdot 105^2$$

2.2 Aufgabe 4

Es seien a, b natürliche Zahlen, für die gilt: $a \mid b^2, b^2 \mid a^3, a^3 \mid b^4, b^4 \mid a^5, \dots$

Zeigen sie: $a = b$.

Beweis. Es sind

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

die Primzerlegungen von a und b . Es ist direkt festzuhalten, dass $X_i = Y_i$ für alle $i = 1, \dots, r$. 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:

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

Es lassen sich die folgenden Ungleichungen ableiten oder direkt ablesen:

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

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

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

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

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.