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 Natürliche, ganze und rationale Zahlen. Teilbarkeit. Primzahlen (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:

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

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 $n \in \mathbb{P}$.

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

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

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

Beweis. Lemma 1 zeigt, dass $n \mid (n-1)!$ für alle n zusammengesetzt. Man kann also schließen, wegen $n \neq 1$, 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 $n \geq 1$.

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 $p \mid \binom{p}{v}$. □

Die eben beschriebene Teilbarkeit lässt sich ganz wesentlich verallgemeinern. Der Beweis des folgenden Lemmas wir in der nächsten Aufgabe hilfreich sein.

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

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

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 (Remmert und Ullrich 2008, S. 64).
2. Anderenfalls ist $v = p^{n-a}q$ mit $a \in \mathbb{N}$ und $0 < a \leq n$. Die Zahlen p und q sind teilerfremd und es gilt $a > 0$ wegen $v < p^n$.

Wir haben 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 $p^a \mid \binom{p^n}{v}$ aufgrund der Teilerfremdheit von p und q. Außerdem gilt $p \mid p^a$ und durch die Transitivität der Teilbarkeit $p \mid \binom{p^n}{v}$. □

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:

$$(a+b)^p - (a^p + b^p) = \underbrace{\left[a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p\right]}_{\text{Binomischer Lehrsatz (Remmert und Ullrich 2008, S. 19)}} - (a^p + b^p)$$

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

Primzahl p teilt die Summe, da jeder Summand 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 $2 \mid n^4 + 4^n \geq 32$. □

2 Der Hauptsatz der elementaren Zahlentheorie (33)

2.1 Aufgabe 1

Folgern Sie aus der Eindeutigkeit der Primzerlegung das Fundamentallemma 1.4 (Remmert und Ullrich 2008, S. 26).

Beweis. Die Primzahl p teilt das Produkt zweier Zahlen a und b

$$p \mid (X_1^{m_1} X_2^{m_2} \cdots X_r^{m_r})(Y_1^{m_1} Y_2^{m_2} \cdots Y_s^{m_s})$$

□

2.2 Aufgabe 2

Führen Sie für die Menge $E := \{4k+1 : k \in \mathbb{N}\}$ entsprechende Betrachtungen durch wie für die Menge D aus der Bemerkung in Abschnitt 2. Zeigen Sie insbesondere, dass in E die Zerlegung in in E unzerlegbare Elemente nicht eindeutig bis auf Reihenfolge ist.

2.3 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 $c^2 = p_1^{2m_1} p_2^{2m_2} \cdots p_r^{2m_r}$ mit $p_1, \ldots, p_r \in \mathbb{P}$ und $m_1, \ldots, m_r \in \mathbb{N}^\times$ 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 $2m_1, \ldots, 2m_r$ vollständig zwischen a und b verteilt sein. Somit sind es immer Quadratzahlen. □

Beispiel 1:	$20^2 = 2^4 5^2$	1)	$ab = (2^4)(5^2) = 4^2 \cdot 5^2$
Beispiel 2:	$210^2 = 2^2 3^2 5^2 7^2$	1)	$ab = (2^2 3^2 5^2)(7^2) = 30^2 \cdot 7^2$
		2)	$ab = (2^2 3^2)(5^2 7^2) = 6^2 \cdot 35^2$
		3)	$ab = (2^2)(3^2 5^2 7^2) = 2^2 \cdot 105^2$

2.4 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 $a = X_1^{m_1} X_2^{m_2} \cdots X_r^{m_r}$, $b = Y_1^{n_1} Y_2^{n_2} \cdots Y_s^{n_s}$ mit $X_1, \ldots, X_r, Y_1, \ldots, Y_r, \in \mathbb{P}$ und $m_1, \ldots, m_r, n_1, \ldots, n_r, \in \mathbb{N}^\times$ die Primzerlegungen von a und b. Es ist direkt festzuhalten, dass $r = s$ und $X_i = Y_i$ 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:

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

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

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

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

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 $a = b$. $\square$

3 Anwendung des Hauptsatzes. Zahlentheorie im Körper $\mathbb{Q}$ (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 $a + b = p^m v$ mit $v \in \mathbb{Z}$ und zeigen durch umformen:

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

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

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:

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

3.3 Aufgabe 3

Seien $n \in \mathbb{N}^\times$, $a_1, \ldots, a_n \in \mathbb{Z}$. Die reelle Zahl x erfülle $x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$. Zeigen Sie: x ist entweder irrational oder ganz.

3.4 Aufgabe 4

Seien $q_1, \ldots, q_s$ Primzahlen, $b := q_1 \cdot q_2 \cdots q_s \in \mathbb{N}$ sowie $m_1, \ldots, m_k \in \mathbb{N}^\times$ derart, dass gilt: $\frac{1}{b} = \frac{1}{m_1} + \frac{1}{m_2} + \cdots + \frac{1}{m_k}$. Zeigen Sie: Jede Zahl $q_i, 1 \leq i \leq s$, teilt wenigstens eine der

Zahlen $m_1, \ldots, m_k$.

Beweis. Durch Hauptnennerdarstellung entsteht mit $v := \frac{m_1 \cdots m_r}{m_1} + \frac{m_1 \cdots m_r}{m_2} + \cdots + \frac{m_1 \cdots m_r}{m_r}$ die folgende Gleichung:

$$\frac{1}{b} = \frac{v}{m_1 m_2 \cdots m_k}$$
$$bv = m_1 m_2 \cdots m_k$$

Es ist zu sehen $b \mid m_1 m_2 \cdots m_k$ und damit die zu zeigende Aussage. □

3.5 Aufgabe 5

Berechnen Sie die Fibonaccidarstellung des Bruches $\frac{21}{23}$.

Beweis. $n_1 = \min\{w \in \mathbb{N} : w \geq \frac{23}{21}\} = 2$. Der größte in $\frac{21}{23}$ enthaltene Stammbruch ist $\frac{1}{2}$.

$$\text{Es ist} \quad \frac{21}{23} = \frac{1}{2} + \frac{a_1}{b_1} \quad \text{mit} \quad \frac{a_1}{b_1} = \frac{21}{23} - \frac{1}{2} = \frac{2 \cdot 21 - 23}{2 \cdot 23} = \frac{19}{46}.$$

$n_2 = \min\{w \in \mathbb{N} : w \geq \frac{46}{19}\} = 3$. Der größte in $\frac{19}{46}$ enthaltene Stammbruch ist $\frac{1}{3}$.

$$\text{Es ist} \quad \frac{19}{46} = \frac{1}{3} + \frac{a_2}{b_2} \quad \text{mit} \quad \frac{a_2}{b_2} = \frac{3 \cdot 19 - 46}{3 \cdot 46} = \frac{11}{138}.$$

$n_3 = \min\{w \in \mathbb{N} : w \geq \frac{138}{11}\} = 13$. Der größte in $\frac{11}{138}$ enthaltene Stammbruch ist $\frac{1}{13}$.

$$\text{Es ist} \quad \frac{11}{148} = \frac{1}{13} + \frac{a_3}{b_3} \quad \text{mit} \quad \frac{a_3}{b_3} = \frac{13 \cdot 11 - 138}{13 \cdot 138} = \frac{5}{1794}.$$

$n_4 = \min\{w \in \mathbb{N} : w \geq \frac{1794}{5}\} = 359$. Der größte in $\frac{5}{1794}$ enthaltene Stammbruch ist $\frac{1}{359}$.

$$\text{Es ist} \quad \frac{5}{1794} = \frac{1}{359} + \frac{a_4}{b_4} \quad \text{mit} \quad \frac{a_4}{b_4} = \frac{359 \cdot 5 - 1794}{359 \cdot 1794} = \frac{1}{644046}.$$

Die Fibonaccidarstellung des Bruches $\frac{21}{23}$ lautet:

$$\frac{21}{23} = \frac{1}{2} + \frac{1}{3} + \frac{1}{13} + \frac{1}{359} + \frac{1}{644046}$$

□

3.6 Aufgabe 6

Zeigen Sie: Es gibt keine ägyptische Bruchdarstellung $\frac{21}{23} = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}$, $1 < n_1 < n_2 < \cdots < n_k$, mit höchstens 3 Stammbrüchen (d. h. notwendig $k \geq 4$).

3.7 Aufgabe 7

Beweisen Sie die angegebene Eindeutigkeitsaussage für die Fibonaccidarstellung (Remmert und Ullrich 2008, S. 53).

4 Größter gemeinsamer Teiler (70)

4.1 Aufgabe 1

Seinen $a, m, n \in \mathbb{N}^\times$. Bestimmen Sie den größten gemeinsamen Teiler von $a^m - 1$ und $a^n - 1$.

4.2 Aufgabe 2

Seien $a, b \in \mathbb{N}^\times$ teilerfremd und $c \in \mathbb{N}$ so, dass gilt: $a \mid c$ und $b \mid c$. Zeigen Sie: $ab \mid c$.

Das Kriterium für paarweise Teilerfremdheit (Remmert und Ullrich 2008, S. 65) enthält als einfache

Folgerung 1. *Seien $a, b \in \mathbb{Z}$ zwei teilerfremde Zahlen, dann ist $\min(w_p(a), w_p(b)) = 0$ für alle $p \in \mathbb{P}$.*

Beweis. Wäre p eine Primzahl für die gilt $w_p(a) > 0$ und $w_p(b) > 0$. Dann wäre gerade dieses p ein gemeinsamer Teiler von a und b. $\square$

Beweis. Es gilt $w_p(a) \leq w_p(c)$, $w_p(b) \leq w_p(c)$ für alle $p \in \mathbb{P}$ nach dem Teilbarkeitskriterium (ebd., S. 50). Es ist $ab = \sum\limits_p p^{w_p(a)+w_p(b)}$ die Primzerlegung von ab. Da a und b teilerfremd sind, gilt nach Folgerung 1 mindestens $w_p(a) = 0$ oder $w_p(b) = 0$ und dadurch $w_p(a) + w_p(b) \leq w_p(c)$. Es folgt $ab \mid c$. $\square$

4.3 Aufgabe 3

Seien $a, b \in \mathbb{N}^\times$. Zeigen Sie: $\mathrm{ggT}(a + b, a - b) \geq \mathrm{ggT}(a, b)$.

4.4 Aufgabe 4

Seien $a, b, m \in \mathbb{Z}$. Zeigen Sie die Äquivalenz folgender Aussagen:

i) Es gibt eine ganze Zahl x mit $m \mid (ax - b)$

ii) $\mathrm{ggT}(a, m) \mid b$

Beweis. i) $\Rightarrow$ ii): Sei $t = \mathrm{ggT}(a, m)$. Es gilt $t \mid a$, $t \mid m$ und aus letzterem $t \mid ax - b$. Weiter gilt nach den Rechenregeln zur Teilbarkeit $t \mid b$ und dies erledigt die Beweisrichtung.

ii) $\Rightarrow$ i): $\mathrm{ggT}(a,m)$ liefert die Gleichung $t = ra + sm$ mit $r, s \in \mathbb{Z}$. Aus $\mathrm{ggT}(a,m) \mid b$ folgt mit $v \in \mathbb{Z}$:

$$\begin{aligned} b &= tv = rva + svm \\ svm &= b - rva \qquad x := rv \\ (-sv)m &= ax - b \end{aligned}$$

Daher $m \mid (ax - b)$. $\square$

4.5 Aufgabe 5

Seien $m, n \in \mathbb{Z}$ teilerfremd, $k := mn$ sowie $a, b \in \mathbb{Z}$ beliebig. Zeigen Sie (unter Verwendung von Unterabschnitt 4.4):

a) Es gibt eine ganze Zahl u mit $m \mid (u - a)$ und $n \mid (u - b)$

b) Für eine ganze Zahl x sind äquivalent:

  i) $m \mid (x - a)$ und $n \mid (x - b)$

  ii) $k \mid (x - u)$

Beweis. a) Es ist $pm = u - a$ und $qn = u - b$ mit $p, q \in \mathbb{Z}$. D. h. u ist die Lösung der Gleichung $pm - qn = b - a$. Nach Voraussetzung existiert $rm + sn = 1$ mit $r, s \in \mathbb{Z}$. Bemerke die Terme rm und sn haben zwangsweise unterschiedliche Vorzeichen. Nach Multiplikation mit $b - a$ entsteht daher

$$(br - ar)m + (bs - as)n = b - a. \tag{1}$$

Also, es existiert ein u mit

$$u = (br - ar)m + a = (bs - as)n + b.$$

b) Gleichung 1 gibt eine Lösung für u. Es ist leicht hierdurch alle anderen Lösungen anzugeben. Mit dem Wissen des Vorzeichenverhaltens von (1), rechne man mit $v \in \mathbb{Z}$ wie folgt:

$$(br - ar + vn)m + (bs - as + vm)n = b - a + (vmn - vmn)$$

Sind also $x = (br - ar + v_1 n)m + a$ und $u = (br - ar + v_2 n)m + a$ mit $v_1 \neq v_2 \in \mathbb{Z}$

zwei Lösungen der Teilbarkeit, dann ist $x - u = v_1 mn - v_2 mn = (v_1 - v_2)mn$. Mit $k := mn$ gilt also $k \mid x - u$.

$\square$

4.6 Aufgabe 6

a) Seien $\mathfrak{a}, \mathfrak{b}$ zwei Ideale in $\mathbb{Z}$. Zeigen Sie: $\mathfrak{a} \cap \mathfrak{b}$ ist wieder ein Ideal in $\mathbb{Z}$.

b) Zeigen Sie: Für ganze Zahlen a, b, v sind folgende Aussagen äquivalent:

   i) $v \geq 0$ und $\mathbb{Z}v = \mathbb{Z}a \cap \mathbb{Z}b$

   ii) $v = \mathrm{kgV}(a, b)$

Lemma 3. *Es seien $a, b \in \mathbb{Z}$ zwei Zahlen derart, dass für das von ihnen erzeugte Hauptideal $\mathbb{Z}a, \mathbb{Z}b$ gilt: $\mathbb{Z}a \subseteq \mathbb{Z}b$. Dann ist notwendigerweise $b \mid a$.*

Beweis. Es wird o. B. d. A. angenommen $a, b \geq 0$. Der Fall für $b = a$ und $a = 0$ ist klar. Ist $b = 0$, so muss a als einzige Teilmenge ebenfalls 0 sein. Es kann niemals gelten $b > a$, denn dann wäre $a \notin \mathbb{Z}b$. Es muss also sein $b < a$. Es ist $a \in \mathbb{Z}b$ und es gilt somit die Gleichung $bx = a$ mit $x \in \mathbb{Z}$. Es folgt $b \mid a$. $\square$

Beweis. a) Wir zeigen, dass $\mathfrak{a} \cap \mathfrak{b}$ die Bedingungen der Definition eines Ideals in $\mathbb{Z}$ erfüllt (Remmert und Ullrich 2008, S. 60).

ad 1): Angenommen $a, b \in \mathfrak{a} \cap \mathfrak{b}$. Es wird gezeigt, dass auch $a - b \in \mathfrak{a} \cap \mathfrak{b}$. Per Annahme wissen wir $a, b \in \mathfrak{a}$ und $a, b \in \mathfrak{b}$. Nach Idealdefinition ist somit ebenfalls $a - b \in \mathfrak{a}$ und $a - b \in \mathfrak{b}$. Es folgt $a - b \in \mathfrak{a} \cap \mathfrak{b}$.

ad 2): Angenommen $a \in \mathfrak{a} \cap \mathfrak{b}$. Es wird gezeigt, dass auch $xa \in \mathfrak{a} \cap \mathfrak{b}$ mit $x \in \mathbb{Z}$. Per Annahme wissen wir $a \in \mathfrak{a}$ und $a \in \mathfrak{b}$. Nach Idealdefinition ist somit ebenfalls $xa \in \mathfrak{a}$ und $xa \in \mathfrak{b}$. Es folgt $xa \in \mathfrak{a} \cap \mathfrak{b}$.

b) Aus $\mathbb{Z}v = \mathbb{Z}a \cap \mathbb{Z}b$ folgt $\mathbb{Z}v \subseteq \mathbb{Z}a$, $\mathbb{Z}v \subseteq \mathbb{Z}b$ und nach Lemma 3 also $a|v$ und $b|v$. Die Zahl v ist somit ein gemeinsames Vielfaches von a und b. Angenommen c ist ein weiteres gemeinsames Vielfaches von a und b, dann gilt $a|c$ und $b|c$. Wieder nach Lemma 3 ist also $\mathbb{Z}c \subseteq \mathbb{Z}a$ und $\mathbb{Z}c \subseteq \mathbb{Z}b$. Es folgt die logische Schlussfolgerung

$$(\mathbb{Z}c \subseteq \mathbb{Z}a) \wedge (\mathbb{Z}c \subseteq \mathbb{Z}a) \wedge (\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}v) \Rightarrow \mathbb{Z}c \subseteq \mathbb{Z}v.$$

Es gilt also $v \mid c$, sowie $a \mid v$ und $b \mid v$. Die Zahl v erfüllt somit alle Eingenschaften des kleinsten gemeinsamen Vielfaches von a und b.

$\square$

4.7 Aufgabe 7

Seien $a, b, c \in \mathbb{N}^\times$. Zeigen Sie: Es gilt $a^2 + b^2 = c^2$ genau dann, wenn es $s, u, v \in \mathbb{N}^\times$ mit $u > v$ gibt, sodass entweder $a = 2suv$, $b = s(u^2 - v^2)$, $c = s(u^2 + v^2)$ oder $a = s(u^2 + r^2)$, $b = 2suv$, $c = s(u^2 + v^2)$.

5 Über die Verteilung und Darstellung von Primzahlen (81)

5.1 Aufgabe 1

Zeigen Sie mit Hilfe des Kriterium von `Lucas-Lehmer` (Remmert und Ullrich 2008, S. 78), dass die Zahlen $M_p = 2^p - 1$ für $p = 3$, $p = 5$ und $p = 7$ Primzahlen sind.

5.2 Aufgabe 2

Zeigen Sie direkt: Es gibt unendliche Primzahlen der Form:
a) $6k + 5$, $k \in \mathbb{N}$
b) $4k + 3$, $k \in \mathbb{N}$

Lemma 4. *Sind $a_1, \ldots, a_k$ Zahlen der Form $a_v = qb_v + 1$, $q, b_v \in \mathbb{Z}$, $1 \leq v \leq k$. Dann ist auch ihr Produkt $a_1 a_2 \cdots a_k$ von der Form $qb + 1$, $b \in \mathbb{Z}$.*

Beweis. Der Beweis ergibt sich unmittelbar durch Induktion, da $(qm + 1)(qn + 1) = q(qmn + m + n) + 1$ für alle $m, n \in \mathbb{Z}$. □

Beweis. a) Angenommen es gäbe nur endlich viele Primzahlen der Form $6k + 5$, etwa $p_1, p_2, \ldots, p_s$ mit $p_1 := 2$. Man betrachte die Zahl $a := (2 \cdot 3)(p_1 p_2 \cdots p_s) - 1 \in \mathbb{N}^{\times}$. Diese Zahl ist von der Form $6k + 5$. Sei $a = q_1^{m1} q_2^{m2} \cdots q_t^{m_t}$ die Primzerlegung von a. Jede Primzahl q_i ist von allen Primzahlen $2, 3, p_1, \ldots, p_s$ verschieden, da 1 nicht durch q_i teilbar ist, $i = 1, 2, \ldots, t$. Nun muss aber mindestens eine Primzahl q_i von der Form $6k + 5$ sein; denn alle anderen Möglichkeiten können wie folgt ausgeschlossen werden:

(a) Die Primzahlen q_i können nicht gerade oder sonstig teilbar sein, denn dann wären es keine Primzahlen. D. h. die folgenden Formen fallen weg:

$$6k + 0,\ 6k + 2 = 2(3k + 1),\ 6k + 3 = 3(2k + 1),\ 6k + 4 = 2(3k + 2)$$

(b) Zusätzlich können sie nicht alle in der Form $6k + 1$ sein; denn so wäre nach dem eingangs bewiesenen auch die Zahl $a = q_1^{m1} q_2^{m2} \cdots q_t^{m_t}$ von der Form $6k + 1$, was nicht möglich ist.

b) Angenommen es gäbe nur endlich viele Primzahlen der Form $4k+3$, etwa $p_1, p_2, \ldots, p_s$ mit $p_1 := 2$. Man betrachte die Zahl $a := (2 \cdot 2)(p_1 p_2 \cdots p_s) - 1 \in \mathbb{N}^\times$. Diese Zahl ist von der Form $4k+3$. Sei $a = q_1^{m1} q_2^{m2} \cdots q_t^{m_t}$ die Primzerlegung von a. Jede Primzahl q_i ist von allen Primzahlen $2, p_1, \ldots, p_s$ verschieden, da 1 nicht durch q_i teilbar ist, $i = 1, 2, \ldots, t$. Nun muss aber mindestens eine Primzahl q_i von der Form $4k+3$ sein; denn alle anderen Möglichkeiten können wie folgt ausgeschlossen werden:

(a) Die Primzahlen q_i können nicht gerade oder sonstig teilbar sein, denn dann wären es keine Primzahlen. D. h. die folgenden Formen fallen weg:

$$4k+0,\ 4k+2 = 2(2k+1)$$

(b) Zusätzlich können sie nicht alle in der Form $4k+1$ sein; denn so wäre nach dem eingangs bewiesenen auch die Zahl $a = q_1^{m1} q_2^{m2} \cdots q_t^{m_t}$ von der Form $4k+1$, was nicht möglich ist.

□

5.3 Aufgabe 3

Zeigen Sie: Für alle natürlichen Zahlen $n \geq 2$ gilt: $n < 2^{\Pi(n)} \cdot \sqrt{n}$.

6 Zahlentheoretische Funktionen (92)

6.1 Aufgabe 1

Zeigen Sie: Für jedes $n \in \mathbb{N}^\times$ gibt es unendlich viele $a \in \mathbb{N}^\times$ mit $n \mid \varphi(a)$.

6.2 Aufgabe 2

Bestimmen Sie alle $n \in \mathbb{N}^\times$, für die $\varphi(n)$ eine Potenz von 2 ist.

6.3 Aufgabe 3

Beweisen Sie für $n \geq 2$:

a) $\varphi_1(n) = \frac{1}{2} n\varphi(n)$

b) $\varphi_2(n) = \frac{1}{3} n^2 \varphi(n) + \frac{n}{6} \prod_{p \mid n} (1 - p)$

7 Integritätsringe. Teilbarkeitstheorie in Integritätsringen (110)

7.1 Aufgabe 1

Sei R ein Integritätsring, seien $a, b, c, d \in R$. Zeigen Sie:

a) Aus $a \sim b$ und $c \sim d$ folgt: $ac \sim bd$.

b) Aus $a \sim b$ und $ac \sim bd$ und $a \neq 0$ folgt: $c \sim d$.

Beweis. a) Es folgt direkt aus Rechenregel 3) der Teilbarkeit (Remmert und Ullrich 2008, S. 23): Aus $a \mid b$ und $c \mid d$ folgt $ac \mid bd$; aus $b \mid a$ und $d \mid c$ folgt $bd \mid ac$.

b) Wir zeigen $c \mid d$ aus dem Gegebenen:

$$\text{Es gilt}\quad b \mid a \underset{\text{mit } c \in R}{\Rightarrow} bc \mid {\color{green}ac}$$
$$\text{Es gilt}\quad {\color{green}ac} \mid bd \underset{\text{transitiv}}{\Rightarrow} bc \mid bd \underset{\text{kürzen}}{\Rightarrow} c \mid d$$

Wir zeigen $d \mid c$ aus dem Gegebenen:

$$\text{Es gilt}\quad a \mid b \underset{\text{mit } d \in R}{\Rightarrow} ad \mid {\color{green}bd}$$
$$\text{Es gilt}\quad {\color{green}bd} \mid ac \underset{\text{transitiv}}{\Rightarrow} ad \mid ac \underset{\text{kürzen}}{\Rightarrow} d \mid c$$

□

Literaturverzeichnis

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