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:

$$a = 1 \Rightarrow a = 2 : \triangle 100100$$
$$b = 0 \Rightarrow b = 1 : \triangle 10010$$
$$c = 0 \Rightarrow c = 1 : \triangle 1001$$

Es ist zu sehen $13 \mid 1001$, denn es gilt: $1001 = 13 \cdot 77$. Hieraus folgt: $13 \mid 10010, 13 \mid 100100$ und damit auch $13 \mid abcabc$. □

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

TODO: Der restliche Beweis mit dem Satz von Wilson □

[1] Für $n > 4$ gilt außerdem: $n|(n-1)!$. Die gesamte Primzerlegung von n ist in $(n-1)!$ enthalten.

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. TODO $\square$

1.4 Aufgabe 4

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

Beweis. Obwohl die Zahlen $\binom{n}{v}$ als Brüche definiert sind, gilt stets:

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

Dies ist auf die Identität

$$\binom{n-1}{v-1} + \binom{n-1}{v} = \binom{n}{v}$$

zurückzuführen, mit der sich jeder Binomialkoeffizient rekursiv als die Summe natürlicher Zahlen berechnen lässt. Per Definition gilt:

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

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

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. $\square$

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 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 gibt $v_i \in \mathbb{N}$ mit $b^2 = av_1, a^3 = b^2 v_2, b^4 = a^3 v_3, a^5 = b^4 v_4, \ldots$. Es sind

$$\begin{aligned} a &= p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r} \\ b &= p_1^{\mu_1} \cdot p_2^{\mu_2} \cdot \ldots \cdot p_r^{\mu_r} \end{aligned}$$

die kanonischen Primzerlegungen von a und b. Für $a = b$ ist die Behauptung offensichtlich richtig. Angenommen $a \neq b$ und es werden zwei Fälle unterschieden:

$0 < a < b$: Die Zahl a besitzt als Teiler von b^2 einen Primfaktor $p^{\mu-n} := p_i^{\mu_i - n}$ mit $0 < n \leq \mu$ und $i = 1, \ldots, r$. Es gilt $p^{\mu-n} \mid b^2$ d.h. $b^2 = p^{\mu-n} v_1$, was äquivalent zu $p^{2\mu} = p^{\mu-n} \cdot p^{\mu+n}$ ist. Wird dieses Schema fortgeführt, entstehen die Gleichungen

$$\begin{aligned} p^{3\mu-3n} &= p^{2\mu} \cdot p^{\mu-3n} \\ p^{4\mu} &= p^{3\mu-3n} \cdot p^{\mu+3n} \\ p^{5\mu-5n} &= p^{4\mu} \cdot p^{\mu-5n} \\ p^{6\mu} &= p^{5\mu-5n} \cdot p^{\mu+5n} \\ &\vdots \\ p^{2k\mu} &= p^{(2k-1)\mu-(2k-1)n} \cdot p^{\mu+(2k-1)n} \\ p^{(2k+1)\mu-(2k+1)n} &= p^{2k\mu} \cdot p^{\mu-(2k+1)n} \qquad (*) \end{aligned}$$

mit $k \in \mathbb{N}^{\times}$. Im allgemeinen lässt sich aus $(*)$ die Ungleichung

$$\mu - 2kn - n \geq 0$$

ableiten. k ist frei wählbar, man setze $k = \mu$ und führt die ursprüngliche Behauptung mit

$(1-2n)\mu - n \geq 0$ zum Widerspruch.

$a > b$: Die Zahl a besitzt als Teiler von b^2 einen Primfaktor $p^{\mu+n} := p_i^{\mu_i+n}$ mit $0 < n \leq \mu$ und $i = 1, \dots, r$. Wäre $n > \mu$ gilt $a \nmid b^2$ und es bleibt nichts mehr zu zeigen. Wie zuvor gilt $p^{\mu+n} \mid b^2$, woraus nach demselben Prinzip die Gleichung $p^{2\mu} = p^{\mu+n} \cdot p^{\mu-n}$ und letztendlich

$$\begin{aligned} p^{2k\mu} &= p^{(2k-1)\mu+(2k-1)n} \cdot p^{\mu-(2k-1)n} \qquad (**) \\ p^{(2k+1)\mu+(2k+1)n} &= p^{2k\mu} \cdot p^{\mu+(2k+1)n} \end{aligned}$$

folgt. Aus $(**)$ kann die Ungleichung

$$\mu - 2kn + n \geq 0$$

abgeleitet werden. Man setze $k = 2\mu$ und erzeugt mit $(1-4n)\mu + n \geq 0$ auch in diesem Fall einen Widerspruch. $\square$

Literaturverzeichnis

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