Inhaltsverzeichnis

Kapitel 1

Zahlentheorie

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: $a = b$ (Remmert und Ullrich 2008, S. 33).

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 $i = 1, \ldots, r$. 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

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

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.