Gelöste und ungelöste Probleme in der Zahlentheorie

Teilnehmer:

Kristin Emmrich	Heinrich-Hertz-Oberschule
Loryn Fechner	Herder-Oberschule
Felix Neumann	Georg-Forster-Oberschule
Alexandra Stepanova	Herder-Oberschule
Roman Stolzenburg	Herder-Oberschule
Walter Unger	Georg-Forster-Oberschule

Gruppenleiter:

Jürg Kramer	Humboldt-Universität zu Berlin, Mitglied im DFG-Forschungszentrum MATHEON
Anna v. Pippich	Humboldt-Universität zu Berlin

Als *pythagoreisches Zahlentripel* (x, y, z) bezeichnet man drei positive natürliche Zahlen x, y, z, die der Gleichung $x^2 + y^2 = z^2$ genügen. Geometrisch können x, y, z als Seiten eines rechtwinkligen Dreiecks aufgefasst werden. In unserem Sommerschul-Kurs werden wir zunächst der Frage nachgehen, ob es endlich oder unendlich viele pythagoreische Zahlentripel gibt; dazu werden wir für pythagoreische Zahlentripel eine allgemeine Formel herleiten.

Das berühmte *Fermat-Problem* stellt in Verallgemeinerung der Suche nach pythagoreischen Zahlentripeln die Frage, ob es positive natürliche Zahlen x, y, z gibt, die der Gleichung

$$x^n + y^n = z^n$$

für einen natürlichen Exponenten $n > 2$ genügen. Die *Vermutung von Fermat* aus dem Jahr 1637, dass es keine solchen natürlichen Zahlen gibt, wurde erst 1995 von Andrew Wiles vollständig bewiesen. In unserem Kurs werden wir die Vermutung von Fermat für den Exponenten $n = 4$ beweisen.

Es zeigt sich, dass sich hinter dem Satz von Wiles eine noch viel tiefer liegende Vermutung der Zahlentheorie verbirgt: die sogenannte *abc-Vermutung*. Diese Vermutung ist bis heute unbewiesen und stellt ein sehr aktives Forschungsfeld dar. Zunächst werden wir die *abc*-Vermutung für Polynome in einer Variablen (*Satz von Mason*) formulieren und beweisen. Als Folgerung werden wir das Analogon der Fermat-Vermutung für Polynome beweisen. Motiviert durch die Analogie zwischen den ganzen Zahlen und Polynomen in einer Variablen können wir nun die *abc*-Vermutung für ganze Zahlen präzise formulieren und die Grenzen ihrer Gültigkeit ausloten. Schließlich zeigen wir, dass die *abc*-Vermutung den Satz von Wiles für große Exponenten n impliziert.

1 Geschichte

Der Satz von Pythagoras: Dieser Satz wurde bereits im Altertum bei der Landvermessung und beim Bau angewendet. Pythagoras hat den Satz wahrscheinlich auf einer Reise nach Ägypten gefunden. Man nimmt an, dass der Satz schon lange vor Pythagoras bekannt war. Die Gleichung $4961^2 + 6480^2 = 8161^2$ wurde bereits ca. 1500 v. Chr. in babylonischen Keilschrifttexten erwähnt.
Weitere Rechenvorschriften zur Erzeugung pythagoreischer Tripel finden sich im Buch des griechischen Mathematikers Diophant (ca. 250 v.Chr., in Alexandria). Deswegen werden Probleme, bei denen es um ganzzahlige Lösungen von Gleichungen geht, auch „diophantische Probleme“ genannt.
Pierre de Fermat (17. Jh.), Hobby-Mathematiker, schrieb seine mathematischen Entdeckungen auf Buchrändern und in Briefen an bedeutende Gelehrten seiner Zeit, unter anderem die Vermutung, dass es keine positiven natürliche Zahlen x, y, z gibt, die der Gleichung $x^n + y^n = z^n$ für einen natürlichen Exponenten $n > 2$ genügen.Über dieses Problem schrieb er auf einem Buchrand: „Für diese Behauptung habe ich einen wahrhaft wunderbaren Beweis gefunden, aber dieser Rand ist zu schmal, um ihn zu fassen.“
Kummer (19. Jh.) bewies die Fermat-Vermutung für alle Primzahlexponenten kleiner als 100 (mit Ausnahme zweier Fälle). Bis etwa 1990 gelang es, die Gültigkeit der Fermat-Vermutung für alle Exponenten n kleiner als 4 Millionen zu beweisen.
Am 23. Juni 1993 wurde ein Beweis für die Fermat-Vermutung von Wiles veröffentlicht, jedoch wurde bereits 1994 die Unvollständigkeit dieses Beweises gezeigt. Es dauerte über ein Jahr, bis schließlich Andrew Wiles mit einem korrigierten Beweis an die Öffentlichkeit trat. Am 27. Juni 1997 wurde der Beweis als richtig anerkannt und so bekam Andrew Wiles den Wolfskehl-Preis (der von Wolfskehl für die Erbringung des Beweises ausgesetzt worden war).

2 Pythagoreische Tripel

Unser Ziel ist es, alle primitiven pythagoreischen Tripel (x, y, z), die die Gleichung $x^2 + y^2 = z^2$ ganzzahlig erfï£¡llen, zu berechnen. Dazu benötigen wir Grundlagen über die Rationalität von grafischen Objekten.

Definition 2.1. *Ein rationaler Punkt ist ein Punkt, der aus rationalen Koordinaten besteht.*

Definition 2.2. *Eine rationale Gerade ist eine Gerade der Form $aX + bY + c = 0$, bei der die Koeffizienten rational sind.*

Lemma 2.3. *Eine Gerade, die zwei rationale Punkte verbindet, ist eine rationale Gerade.*

Beweis. Seien $P_1(x_1, y_1)$ und $P_2(x_2, y_2)$ rationale Punkte. Die Steigung m der Geraden $Y = mX + t$ durch diese Punkte berechnet sich zu

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Da diese Operationen den Ring der rationalen Zahlen nicht verlassen, ist auch m rational. Die Verschiebung t in Y-Richtung ist

$$t = Y - mX = Y - \frac{y_2 - y_1}{x_2 - x_1} \cdot X.$$

Einsetzen von P_1 ergibt

$$t = y_1 - \frac{y_2 - y_1}{x_2 - x_1} \cdot x_1.$$

Somit ist auch t rational und es handelt sich also um eine rationale Gleichung. □

Lemma 2.4. *Der Schnittpunkt zweier rationaler Geraden ist ein rationaler Punkt.*

Beweis. Ohne der Beschränkung der Allgemeinheit seien die beiden rationalen Geraden von der Form

$$f(X) = Y = -\frac{a_1}{b_1}X - \frac{c_1}{b_1},$$
$$g(X) = Y = -\frac{a_2}{b_2}X - \frac{c_2}{b_2}.$$

Durch Gleichsetzen erhält man

$$\frac{a_1}{b_1}X + \frac{c_1}{b_1} = \frac{a_2}{b_2}X + \frac{c_2}{b_2} \quad \Longleftrightarrow$$
$$X = \left(\frac{c_2}{b_2} - \frac{c_1}{b_1}\right) \cdot \left(\frac{a_1}{b_1} - \frac{a_2}{b_2}\right)^{-1}.$$

Daraus folgt, dass die X-Koordinate des Schnittpunkts rational ist. Durch Einsetzen in f erhält man

$$Y = -\frac{a_1}{b_1} \cdot \left(\frac{c_2}{b_2} - \frac{c_1}{b_1}\right) \cdot \left(\frac{a_1}{b_1} - \frac{a_2}{b_2}\right)^{-1} - \frac{c_1}{b_1}.$$

Also ist auch die Y-Koordinate rational. Der Schnittpunkt ist folglich rational, denn seine beiden Koordinaten sind rational. □

Definition 2.5. *Ein rationaler Kegelschnitt ist gegeben durch eine Gleichung der Form*

$$aX^2 + bXY + cY^2 + dX + eY + f = 0,$$

wobei die Koeffizienten rational sind.

Lemma 2.6. *Die Schnittpunkte eines rationalen Kegelschnitts mit einer rationalen Geraden sind nicht immer rational. Aber, wenn einer von beiden rational ist, dann ist es auch der andere.*

Beweis. Gegeben seien die Gleichungen

$$aX^2 + bXY + cY^2 + dX + eY + f = 0 \tag{2.1}$$

und

$$Y = mX + t \tag{2.2}$$

mit rationalen Koeffizienten. Durch Einsetzen von (2.2) in (2.1) erhält man

$$aX^2 + bX(mX + t) + c(mX + t)^2 + dX + e(mX + t) + f = 0.$$

Durch Umformen erhält man eine Gleichung der Form

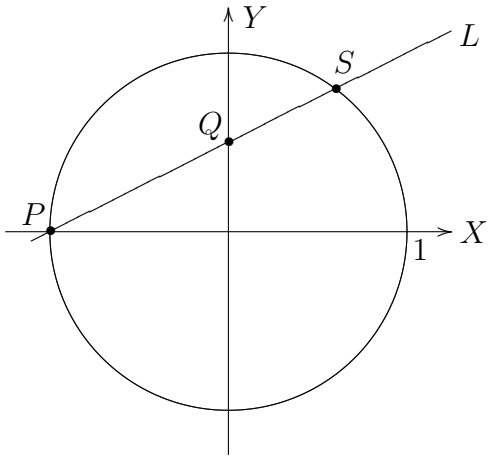
$$AX^2 + BX + C = 0$$

mit $A, B, C \in \mathbb{Q}$. Die Lösungen dieser Gleichung sind gegeben durch

$$x_{1/2} = -\frac{B}{2A} \pm \sqrt{\frac{B^2}{4A^2} - \frac{C}{A}}.$$

Da die auftretende Quadratwurzel nicht zwangsläufig eine rationale Zahl ist, sind auch $x_{1/2}$ nicht immer rational. Angenommen x_1 sei rational. Dann ist folglich die zweite Lösung x_2 auch rational. Und wenn die X-Koordinate rational ist, dann ist es nach Einsetzen in (2.2) auch die Y-Koordinate. Das heißt, wenn der eine Schnittpunkt rational ist, dann ist es auch der zweite. □

Gegeben sei der Einheitskreis $X^2 + Y^2 = 1$. Wir nehmen einen rationalen Punkt auf dem Kreis, zum Beispiel $P(-1, 0)$, und einen rationalen Punkt $Q(0, t)$ auf der Y-Achse. Nach 2.3 ist die Gerade L, die diese beiden Punkte verbindet, eine rationale Gerade. Diese Gerade schneidet unseren Kreis in zwei Punkten, nämlich in P und in $S(x, y)$. Da der Kreis ein spezieller rationaler Kegelschnitt ist, folgt nach 2.6, dass S ebenfalls rational ist, weil Q ja rational ist.



Die Gleichung der rationalen Geraden L ist $L(X) = t(1+X)$. Durch Umformen und Gleichsetzen von der Kreisgleichung und $L(X)$ erhält man

$$1 - X^2 = Y^2 = t^2(1+X)^2.$$

Wie man sieht, ist die erste Lösung der Gleichung $X = -1$, weil der Punkt P auf dem Kreis und auf L liegt. Um nun auf die zweite Lösung zu kommen, teilen wir durch $(X+1)$ und erhalten nach Umformen

$$1 - X = t^2(1+X) \Longleftrightarrow X(1+t^2) = 1 - t^2 \Longleftrightarrow X = \frac{1-t^2}{1+t^2}.$$

Durch Einsetzen in $L(X)$ erhält man schließlich

$$Y = \frac{2t}{1+t^2}.$$

Diese Formeln für X und Y bieten uns letztendlich die Möglichkeit, die primitiven pythagoreischen Tripel zu charakterisieren.

Definition 2.7. *Ein primitives pythagoreisches Tripel (x, y, z) besteht aus positiven natürlichen Zahlen x, y, z, die teilerfremd sind und der Gleichung*

$$x^2 + y^2 = z^2$$

genügen.

Bemerkung. Wenn (x, y, z) ein primitives pythagoreisches Tripel ist, so sind x, y, z sogar paarweise teilerfremd. Dies sieht man wie folgt ein: Angenommen, y und z hätten einen gemeinsamen Teiler. Dann hätte auch x wegen $x^2 = z^2 - z^2$ diesen Teiler. Dies widerspricht aber der Teilerfremdheit von x, y, z.

Theorem 2.8. *Es sei (x, y, z) ein primitives pythagoreisches Tripel. Dann existieren positive natürliche Zahlen m, n verschiedener Parität mit $n > m$ und $\mathrm{ggT}(m, n) = 1$ derart, dass*

$$x = n^2 - m^2,\ y = 2mn,\ z = m^2 + n^2$$

gilt.

Beweis. Es sei (x, y, z) ein beliebiges primitives pythagoreisches Tripel. Damit setzen wir

$$x' = \frac{x}{z},\ y' = \frac{y}{z}.$$

Der Punkt $S(x', y')$ definiert dann einen Punkt mit rationalen Koordinaten auf dem Einheitskreis $X^2 + Y^2 = 1$, denn es besteht die Äquivalenz

$$x'^2 + y'^2 = 1 \Longleftrightarrow x^2 + y^2 = z^2.$$

Da x und y teilerfremd sind, können x und y nicht beide gerade sein. Die Zahlen x und y können aus folgendem Grund auch nicht beide ungerade sein: Angenommen x und y seien beide ungerade, d.h. $x \equiv y \equiv 1 \bmod 2$. Dann muss z gerade sein, d.h. $z \equiv 0 \bmod 2$, und wir erhalten den Widerspruch

$$2 \equiv x^2 + y^2 = z^2 \equiv 0 \bmod 4.$$

Die Zahlen x und y müssen also unterschiedliche Parität haben. Wir können im folgenden ohne Beschränkung der Allgemeinheit annehmen, dass x ungerade und y gerade ist. Da nun $S(x', y')$ ein rationaler Punkt auf dem Einheitskreis ist, gibt es eine rationale Zahl t, so dass

$$x' = \frac{1 - t^2}{1 + t^2}, \quad y' = \frac{2t}{1 + t^2} \tag{2.3}$$

gilt. Da t eine rationale Zahl ist, kann diese als Quotient zweier teilerfremder natürlicher Zahlen m und n dargestellt werden, d.h.

$$t = \frac{m}{n}. \tag{2.4}$$

Wenn wir jetzt (2.4) in (2.3) einsetzen, erhalten wir

$$\frac{x}{z} = x' = \frac{1 - m^2/n^2}{1 + m^2/n^2} = \frac{n^2 - m^2}{n^2 + m^2}, \tag{2.5}$$

$$\frac{y}{z} = y = \frac{2 \cdot m/n}{1 + m^2/n^2} = \frac{2mn}{n^2 + m^2}. \tag{2.6}$$

Da $(n^2 - m^2)$ und $(n^2 + m^2)$ aus (2.5) sowie $2mn$ und $(n^2 + m^2)$ aus (2.6) nicht zwangsläufig teilerfremd sein müssen, gibt es ein $\lambda \in \mathbb{N}$, so dass

$$\lambda x = n^2 - m^2, \quad \lambda y = 2mn, \quad \lambda z = n^2 + m^2$$

gilt. Da λ die Zahlen $(n^2 + m^2)$ und $(n^2 - m^2)$ teilt, muss es auch die Summe $2n^2$ und die Differenz $2m^2$ teilen. Da m und n aber teilerfremd sind, folgt daraus, dass λ die Zahl 2 teilen muss. Die natürliche Zahl λ kann somit nur die Werte 1 oder 2 annehmen. Im folgenden zeigen wir indirekt, dass $\lambda = 1$ sein muss. Dazu nehmen wir an, dass $\lambda = 2$ gilt. Da x nach obiger Annahme ungerade ist, folgt somit mit $\lambda x = n^2 - m^2$ die Kongruenz $n^2 - m^2 = \lambda x \equiv 2 \bmod 4$. Da jedoch n^2 und m^2 entweder kongruent zu 0 oder 1 mod 4 sind, ist das nicht möglich. Also gilt $\lambda = 1$.

Somit kommen wir auf die Bildungsvorschrift

$$x = n^2 - m^2, \quad y = 2mn, \quad z = n^2 + m^2, \tag{2.7}$$

womit der Satz vollständig bewiesen ist. □

3 Die Vermutung von Fermat

Fermat hat das Problem der Suche nach pythagoreischen Tripeln dahingehend verallgemeinert, dass er die Vermutung aufgestellt hat, dass keine von Null verschiedenen ganzzahligen Lösungen x, y, z für die Gleichung $x^n + y^n = z^n$ für ein $n \in \mathbb{N}$, $n \geq 3$, existieren.
Einen Beweis seiner Vermutung hat Fermat uns allerdings nicht hinterlassen, sondern nur in einer Randnotiz geschrieben, er habe einen wahrhaft wunderbaren Beweis gefunden, leider reiche der Platz hier aber nicht aus, um ihn aufzuschreiben.

Theorem 3.1. *Die Vermutung von Fermat ist für $n = 4$ korrekt.*

Beweis. Im Gegensatz zur Behauptung nehmen wir an, dass teilerfremde $x, y, z \in \mathbb{N}_{>0}$ mit der Eigenschaft $x^4 + y^4 = z^4$ existieren. Wir haben diese Annahme zu einem Widerspruch zu führen.
Indem wir $w = z^2$ schreiben, erhalten wir die Gleichung

$$(x^2)^2 + (y^2)^2 = w^2$$

und stellen fest, dass (x^2, y^2, w) ist ein primitives pythagoreisches Tripel ist. Gemäß Satz 2.8 existieren positive natürliche Zahlen p, q verschiedener Parität mit $p > q$ und $\mathrm{ggT}(p, q) = 1$ derart, dass

$$x^2 = 2pq, \quad y^2 = p^2 - q^2, \quad w = p^2 + q^2$$

gilt. Umstellen der zweiten Gleichung ergibt

$$q^2 + y^2 = p^2.$$

Da p und q teilerfremd sind, ist (q, y, p) ein primitives pythagoreisches Tripel, wobei p ungerade ist. Eine erneute Anwendung von Satz 2.8 liefert positive natürliche Zahlen a, b verschiedener Parität mit $a > b$ und $\mathrm{ggT}(a, b) = 1$ derart, dass

$$q = 2ab, \quad y = a^2 - b^2, \quad p = a^2 + b^2$$

gilt. Einsetzen von $q = 2ab$ und $p = a^2 + b^2$ in die Gleichung $x^2 = 2pq$ liefert

$$x^2 = 2pq = 2(a^2 + b^2) \cdot 2ab = 4ab(a^2 + b^2) \Longleftrightarrow \left(\frac{x}{2}\right)^2 = ab(a^2 + b^2).$$

Damit ist das Produkt $ab(a^2 + b^2)$ also ein Quadrat. Da die Zahlen a, b, $(a^2 + b^2)$ paarweise teilerfremd sind, müssen a, b und $(a^2 + b^2)$ selbst Quadratzahlen sein, d.h.

$$a = x_1^2, \quad b = y_1^2, \quad a^2 + b^2 = w_1^2$$

mit positiven natürlichen Zahlen x_1, y_1, w_1. Ausgehend von unserer Annahme haben wir damit positive natürliche Zahlen x_1, y_1, w_1 gefunden, die der Gleichung

$$x_1^4 + y_1^4 = w_1^2$$

genügen. Überdies stellen wir fest:

$$\begin{aligned} x_1 < x, &\quad \text{denn} \quad x_1^2 = a < 2ab = q < 2pq = x^2, \\ y_1 < y, &\quad \text{denn} \quad y_1^2 = b < a + b < ((a + b)(a - b))^2 = y^2, \\ w_1 < w, &\quad \text{denn} \quad w_1^2 = a^2 + b^2 = p < p^2 + q^2 = w < w^2. \end{aligned}$$

Damit greift nun die *Methode des unendlichen Abstiegs:* Ausgehend von den positiven natürlichen Zahlen x, y, w mit $x^4 + y^4 = w^2$ haben wir kleinere positive natürliche Zahlen x_1, y_1, w_1 mit $x_1^4 + y_1^4 = w_1^2$ konstruiert. Diesen Prozess kann man offensichtlich fortsetzen und eine unendliche Folge von Tripeln (x_j, y_j, w_j) von immer kleiner werdenden positiven natürlichen Zahlen konstruieren, die der Gleichung $x_j^4 + y_j^4 = w_j^2$ genügen. Dies ist ersichtlich ein Widerspruch, da es nur endlich viele positive natürliche Zahlen gibt, die kleiner als x sind. □

4 Der Satz von Mason

In diesem Kapitel beweisen wir den Satz von Mason, der auch als *abc*-Vermutung für komplexe Polynome in einer Variablen bezeichnet wird. Dazu stellen wir zunächst einige Begriffe bereit und beweisen zwei Lemmas.

Es sei $f \in \mathbb{C}[X]$ ein Polynom mit komplexen Koeffizienten, d.h.

$$f(X) = c_n X^n + c_{n-1} X^{n-1} + \ldots + c_1 X + c_0,$$

wobei $c_1, \ldots, c_n \in \mathbb{C}$ und $c_n \neq 0$ gilt. Der Grad von f ist hierbei durch $\deg(f) = n$ gegeben. Der *Fundamentalsatz der Algebra* besagt, dass wir $f \in \mathbb{C}[X]$ schreiben können als

$$f(X) = c \cdot (X - \alpha_1)^{a_1} \cdot \ldots \cdot (X - \alpha_m)^{a_m}, \tag{4.1}$$

wobei $c \in \mathbb{C}$ mit $c \neq 0$ ist, $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ die verschiedenen Nullstellen von f sind und $a_1, \ldots, a_m \in \mathbb{N}_{>0}$ die jeweiligen Vielfachheiten der Nullstellen bezeichnen. Damit erhalten wir für den Grad von f die Gleichheit

$$\deg(f) = n = a_1 + \ldots + a_m = \sum_{j=1}^{m} a_j.$$

Definition 4.1. *Für $f \in \mathbb{C}[X]$ mit der Zerlegung* (4.1) *definieren wir*

$$n_0(f) := \textit{Anzahl der verschiedenen Nullstellen von } f = m.$$

Bemerkung. Es gilt $n_0(f) \leq \deg(f)$. Die Differenz der beiden Zahlen $n_0(f)$ und $\deg(f)$ kann allerdings sehr groß sein. Zum Beispiel ist für $f(X) := (X-1)^{10101}$ der Grad $\deg(f) = 10101$ und $n_0(f) = 1$.

Lemma 4.2. *Sei $f \in \mathbb{C}[X]$ und $f \neq 0$. Dann gilt*

$$n_0(f) = \deg(f) - \deg\big(\mathrm{ggT}(f, f')\big). \tag{4.2}$$

Beweis. Sei $f \in \mathbb{C}[X]$ und $f \neq 0$. Wir schreiben f wie in (4.1) als

$$f(X) = c \cdot (X - \alpha_1)^{a_1} \cdot \ldots \cdot (X - \alpha_m)^{a_m}, \tag{4.3}$$

wobei $c \in \mathbb{C}$ mit $c \neq 0$ ist und $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ die verschiedenen Nullstellen mit den Vielfachheiten $a_1, \ldots, a_m \in \mathbb{N}_{>0}$ bezeichnen. Ableiten von f unter Verwendung der Produktregel liefert

$$\begin{aligned} f'(X) = {} & c \cdot a_1 \cdot (X - \alpha_1)^{a_1 - 1} \cdot (X - \alpha_2)^{a_2} \cdot \ldots \cdot (X - \alpha_m)^{a_m} \\ & + c \cdot (X - \alpha_1)^{a_1} \cdot \Big[(X - \alpha_2)^{a_2} \cdot \ldots \cdot (X - \alpha_m)^{a_m}\Big]'. \end{aligned} \tag{4.4}$$

Schreiben wir $(X-\alpha_1)^{a_1} = (X-\alpha_1)^{a_1-1} \cdot (X-\alpha_1)$, so zeigt die Gleichheit (4.1), dass das Polynom $(X-\alpha_1)^{a_1-1}$ das Polynom f teilt. Aus der Gleichheit (4.4) folgt, dass das Polynom $(X-\alpha_1)^{a_1-1}$ auch das Polynom f' teilt. Daraus folgt

$$(X-\alpha_1)^{a_1-1} | \operatorname{ggT}(f, f').$$

Analog erhalten wir für jeden Wert $j \in \{2, \ldots, m\}$, dass

$$(X-\alpha_j)^{a_j-1} | \operatorname{ggT}(f, f')$$

gilt. Insgesamt erhalten wir damit die Aussage

$$(X-\alpha_1)^{a_1-1} \cdot \ldots \cdot (X-\alpha_m)^{a_m-1} | \operatorname{ggT}(f, f').$$

Aus Gradgründen folgt nun

$$\operatorname{ggT}(f, f') = (X-\alpha_1)^{a_1-1} \cdot \ldots \cdot (X-\alpha_m)^{a_m-1}.$$

Daraus ergibt sich

$$\deg\big(\operatorname{ggT}(f, f')\big) = \sum_{j=1}^{m} (a_j - 1) = \sum_{j=1}^{m} a_j - m = \deg(f) - n_0(f), \tag{4.5}$$

woraus die Behauptung unmittelbar folgt. □

Lemma 4.3. *Seien $f, g \in \mathbb{C}[X]$. Dann ist*

$$n_0(f \cdot g) \leq n_0(f) + n_0(g),$$

wobei die Gleichheit genau dann gilt, wenn f und g teilerfremd sind.

Beweis. Diese Behauptung ergibt sich unmittelbar aus dem Fundamentalsatz der Algebra. □

Theorem 4.4 (Satz von Mason). *Für alle nicht-konstanten, teilerfremden Polynome $a, b, c \in \mathbb{C}[X]$ mit $a + b = c$ gilt die Ungleichung*

$$\max\big(\deg(a), \deg(b), \deg(c)\big) \leq n_0(a \cdot b \cdot c) - 1.$$

Beweis. Aus der Gleichheit

$$a + b = c \tag{4.6}$$

folgt durch Ableiten die Gleichheit

$$a' + b' = c'. \tag{4.7}$$

Multiplizieren von (4.6) mit a' und von (4.7) mit a liefert die Gleichheiten

$$a'a = a'c - a'b \quad \text{und} \quad aa' = ac' - ab'.$$

Nach Gleichsetzen und Umformen erhalten wir

$$ab' - a'b = ac' - a'c. \tag{4.8}$$

Nun teilen $\mathrm{ggT}(a, a')$ und $\mathrm{ggT}(b, b')$ offensichtlich die linke Seite von (4.8). Da jetzt $\mathrm{ggT}(c, c')$ entsprechend die rechte Seite der Gleichung (4.8) teilt, muss $\mathrm{ggT}(c, c')$ auch die linke Seite von (4.8), d.h. $ab' - a'b$, teilen. Insgesamt haben wir also die Teilbarkeiten

$$\begin{aligned} &\mathrm{ggT}(a, a')|(ab' - a'b),\\ &\mathrm{ggT}(b, b')|(ab' - a'b),\\ &\mathrm{ggT}(c, c')|(ab' - a'b). \end{aligned}$$

Aufgrund der paarweisen Teilerfremdheit der Polynome a, b, c ergibt sich somit die Teilbarkeitsbeziehung

$$\mathrm{ggT}(a, a') \cdot \mathrm{ggT}(b, b') \cdot \mathrm{ggT}(c, c')|(ab' - a'b). \tag{4.9}$$

Aus folgendem Grund ist die Differenz $ab' - a'b$ ungleich dem Nullpolynom: Wäre nämlich $ab' - a'b = 0$, so könnte man die Gleichung schreiben als $a'b = ab'$. Daraus würde $a|a'b$ folgen. Da aber a und b nach Voraussetzung teilerfremd sind, ergäbe sich daraus $a|a'$. Da dies jedoch nur fi£¡r $a' = 0$ möglich ist, müsste a ein konstantes Polynom sein. Dies widerspricht aber unserer Voraussetzung.
Da nun $ab' - a'b$ nicht das Nullpolynom ist und aufgrund von (4.9) von dem Produktpolynom $\mathrm{ggT}(a, a') \cdot \mathrm{ggT}(b, b') \cdot \mathrm{ggT}(c, c')$ geteilt wird, besteht die Ungleichung

$$\deg\big(\mathrm{ggT}(a, a') \cdot \mathrm{ggT}(b, b') \cdot \mathrm{ggT}(c, c')\big) \leq \deg(ab' - a'b). \tag{4.10}$$

Unter Berücksichtigung der Eigenschaft $\deg(f \cdot g) = \deg(f) + \deg(g)$ $(f, g \in \mathbb{C}[X])$ erhalten wir aus (4.10) die Ungleichung

$$\deg\big(\mathrm{ggT}(a, a')\big) + \deg\big(\mathrm{ggT}(b, b')\big) + \deg\big(\mathrm{ggT}(c, c')\big) \leq \deg(ab' - a'b). \tag{4.11}$$

Aufgrund der weiteren Gradeigenschaft

$$\deg(f + g) \leq \max\big(\deg(f), \deg(g)\big) \quad (f, g \in \mathbb{C}[X])$$

erhalten wir für die rechte Seite von (4.11) die Abschätzung

$$\deg(ab' - a'b) \leq \max\big(\deg(ab'), \deg(a'b)\big).$$

Die Grade $\deg(ab')$ und $\deg(a'b)$ berechnen wir unter Berücksichtigung der bekannten Formel $\deg(f') = \deg(f) - 1$ ($f \in \mathbb{C}[X]$, $\deg(f) > 0$) zu

$$\begin{aligned}\deg(ab') &= \deg(a) + \deg(b') = \deg(a) + \deg(b) - 1 \\ &= \deg(a) - 1 + \deg(b) = \deg(a') + \deg(b) = \deg(a'b),\end{aligned}$$

d.h.

$$\deg(ab' - a'b) \leq \max\big(\deg(ab'), \deg(a'b)\big) = \deg(a) + \deg(b) - 1. \tag{4.12}$$

Die Ungleichungen (4.11) und (4.12) zusammengenommen ergeben

$$\deg\big(\mathrm{ggT}(a, a')\big) + \deg\big(\mathrm{ggT}(b, b')\big) + \deg\big(\mathrm{ggT}(c, c')\big) \leq \deg(a) + \deg(b) - 1.$$

Addition von $\deg(c)$ zur vorhergehenden Ungleichung liefert nach Umstellen

$$\begin{aligned}\deg(c) \leq -1 &+ \deg(a) - \deg\big(\mathrm{ggT}(a, a')\big) \\ &+ \deg(b) - \deg\big(\mathrm{ggT}(b, b')\big) \\ &+ \deg(c) - \deg\big(\mathrm{ggT}(c, c')\big).\end{aligned}$$

Nach dreimaliger Anwendung von Lemma 4.2 ergibt sich damit die Ungleichung

$$\deg(c) \leq n_0(a) + n_0(b) + n_0(c) - 1.$$

Da nun a, b, c paarweise teilerfremd sind, ergibt sich mit Hilfe von Lemma 4.3

$$n_0(a) + n_0(b) + n_0(c) = n_0(a \cdot b \cdot c),$$

und damit die Ungleichung

$$\deg(c) \leq n_0(a \cdot b \cdot c) - 1.$$

Aus Symmetriegründen beweist man in analoger Weise

$$\deg(a) \leq n_0(a \cdot b \cdot c) - 1 \quad \text{und} \quad \deg(b) \leq n_0(a \cdot b \cdot c) - 1,$$

woraus insgesamt die Behauptung des Satzes von Mason folgt. □

5 Der Satz von Fermat für Polynome

Mit Hilfe des Satzes von Mason (Theorem 4.4) können wir das Analogon der Fermat-Vermutung für Polynome beweisen.

Theorem 5.1 (Fermat für Polynome). *Für $n \geq 3$ gibt es keine nicht-konstanten, teilerfremden Polynome $f, g, h \in \mathbb{C}[X]$ mit*

$$f^n + g^n = h^n.$$

Beweis. Wir nehmen an, dass $f, g, h \in \mathbb{C}[X]$ nicht-konstante, teilerfremde Polynome mit $f^n + g^n = h^n$ sind. Da dann auch die Polynome f^n, g^n, h^n nicht-konstant und teilerfremd sind, gilt nach dem Satz von Mason (Theorem 4.4) die Ungleichung

$$\max\big(\deg(f^n), \deg(g^n), \deg(h^n)\big) \leq n_0(f^n \cdot g^n \cdot h^n) - 1. \tag{5.1}$$

Wegen

$$n_0(f^n \cdot g^n \cdot h^n) = n_0(f \cdot g \cdot h) \leq \deg\big(f \cdot g \cdot h\big) = \deg(f) + \deg(g) + \deg(h)$$

und unter Berücksichtigung der Eigenschaft $\deg(q^n) = n \cdot \deg(q)$ ($q \in \mathbb{C}[X]$) erhalten wir aus (5.1) die Ungleichung

$$n \cdot \max\big(\deg(f), \deg(g), \deg(h)\big) \leq \deg(f) + \deg(g) + \deg(h) - 1. \tag{5.2}$$

Da weiter $\deg(q) \leq \max\big(\deg(f), \deg(g), \deg(h)\big)$ für $q = f, g, h$ gilt, liefert (5.2) die Abschätzungen

$$n \cdot \deg(f) \leq \deg(f) + \deg(g) + \deg(h) - 1 \tag{5.3}$$
$$n \cdot \deg(g) \leq \deg(f) + \deg(g) + \deg(h) - 1 \tag{5.4}$$
$$n \cdot \deg(h) \leq \deg(f) + \deg(g) + \deg(h) - 1. \tag{5.5}$$

Addition von (5.3), (5.4) und (5.5) ergibt nun die Ungleichung

$$\begin{aligned} & n \cdot \big(\deg(f) + \deg(g) + \deg(h)\big) \leq 3 \cdot \big(\deg(f) + \deg(g) + \deg(h)\big) - 3 \\ \iff & (n-3) \cdot \big(\deg(f) + \deg(g) + \deg(h)\big) \leq -3. \end{aligned}$$

Dies ist für $n \geq 3$ offensichtlich ein Widerspruch ist, da dann die linke Seite der letzten Ungleichung nicht negativ ist. Damit ist der Satz von Fermat für Polynome bewiesen. □

6 Die Analogie zwischen den ganzen Zahlen und Polynomen

In diesem Abschnitt vergleichen wir Eigenschaften der ganzen Zahlen mit Eigenschaften von Polynomen mit komplexen Koeffizienten. Insbesondere werden wir das Analogon des Grades eines Polynoms für ganze Zahlen entdecken und schließlich die Funktion $n_0(f)$ (siehe Definition 4.1) auch für ganze Zahlen definieren.

Eigenschaft	$\mathbb{Z}$	$\mathbb{C}[X]$
Elemente	ganze Zahlen a	Polynome $f = f(X)$ mit komplexen Koeffizienten
Teilbarkeit	$a \in \mathbb{Z}$ $b \in \mathbb{Z}$ $a\|b \iff \exists c \in \mathbb{Z} : b = a \cdot c$	$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$ $g = b_m X^m + b_{m-1} X^{m-1} + \ldots + b_0$ $f\|g \iff \exists h \in \mathbb{C}[X] : g = f \cdot h$
Division mit Rest	$a, b \in \mathbb{Z}, b \neq 0$ $\Longrightarrow \exists q, r \in \mathbb{Z},$ $0 \leq r < \|b\|$: $a = q \cdot b + r$	$f, g \in \mathbb{C}[X], g \neq 0$ $\Longrightarrow \exists q, r \in \mathbb{C}[X],$ $r = 0$ oder $\deg(r) < \deg(g)$: $f = q \cdot g + r$
Analogie z.B.:	$a \in \mathbb{Z}, a \neq 0$ $\ln(\|a\|)$ $\ln(\|a \cdot b\|) = \ln(\|a\|) + \ln(\|b\|)$	$f \in \mathbb{C}[X], f \neq 0$ $\deg(f)$ $\deg(f \cdot g) = \deg(f) + \deg(g)$
Division mit Rest (revisited)	$a, b \in \mathbb{Z}, b \neq 0$ $\Longrightarrow \exists q, r \in \mathbb{Z},$ $r = 0$ oder $0 \leq \ln(\|r\|) < \ln(\|b\|)$: $a = q \cdot b + r$	$f, g \in \mathbb{C}[X], g \neq 0$ $\Longrightarrow \exists q, r \in \mathbb{C}[X],$ $r = 0$ oder $\deg(r) < \deg(g)$: $f = q \cdot g + r$

ggT(.,.)	$a, b \in \mathbb{Z}$, nicht beide Null: ggT(a, b) definiert; Berechnung mit Hilfe des Euklidischen Algorithmus	$f, g \in \mathbb{C}[X]$, nicht beide Null: ggT(f, g) definiert; Berechnung mit Hilfe des Euklidischen Algorithmus
Einheiten	$\{-1, +1\}$	konst. Polynome $\neq 0$ kurz: $\mathbb{C}^\times := \mathbb{C}\backslash\{0\} \subseteq \mathbb{C}[X]$
Primzahlen, bzw. Primpolynome	$2, 3, 5, 7, 11, 13, ..., 229, ...$	$X - \alpha$, $\alpha \in \mathbb{C}$
Fundamentalsatz	der Arithmetik $a \in \mathbb{Z}, \ln(\lvert a\rvert) > 0 \, (\Leftrightarrow \lvert a\rvert > 1)$: $a = \pm p_1^{a_1} \cdot ... \cdot p_m^{a_m}$, wobei $p_1, ..., p_m$ paarweise verschiedene Primzahlen, $a_1, ..., a_m \in \mathbb{N}_{>0}$	der Algebra $f \in \mathbb{C}[X], \deg(f) > 0$: $f(X) = c \cdot (X - \alpha_1)^{a_1} \cdot ... \cdot (X - \alpha_m)^{a_m}$, wobei $c \in \mathbb{C}^\times$, $\alpha_1, ..., \alpha_m \in \mathbb{C}$ paarweise verschieden, $a_1, ..., a_m \in \mathbb{N}_{>0}$
$n_0(.)$	$a \in \mathbb{Z}, \ln(\lvert a\rvert) > 0 \, (\Leftrightarrow \lvert a\rvert > 1)$: $n_0(a) = \sum_{p\lvert a} \ln(p)$	$f \in \mathbb{C}[X], \deg(f) > 0$: $n_0(f) = \sharp$ versch. Nst. von f $= \sharp$ versch. Primpolynome p von f $= \sum_{p\lvert f} 1 = \sum_{p\lvert f} \deg(p)$

1. *Bemerkung (Division mit Rest/Division mit Rest (revisited))*:
Es ist leicht zu erkennen, dass eine Analogie zwischen dem Betrag $|.|$ einer ganzen Zahl und dem Grad deg(.) eines komplexen Polynoms besteht. Diese ist jedoch noch nicht quantifiziert. Deshalb ersetzen wir den Betrag $|a|$ der ganzen Zahl a durch den natürlichen Logarithmus ihres Betrages $\ln(|a|)$. Eine Begründung hierfür liegt darin, dass sich der Logarithmus auf einem Produkt analog zum Grad additiv verhält: es gilt $\ln(|a \cdot b|) = \ln(|a|) + \ln(|b|)$ und $\deg(f \cdot g) = \deg(f) + \deg(g)$. Weiter gilt zum Beispiel $\ln(|a|) = -\infty$ für $a = 0$ und $\deg(f) := -\infty$ für $f = 0$. Damit können wir die Division mit Rest für ganze Zahlen und komplexe Polynome symmetrisch formulieren (siehe Division mit Rest (revisited)).

2. *Bemerkung (Größter gemeinsamen Teiler* ggT*)*:
Zur Veranschaulichung geben wir ein Beispiel, wie man mit Hilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ zweier ganzer Zahlen a und b berechnen kann: Sei $a = 29$ und $b = 17$. Dann gilt:

$$\begin{aligned} 29 &= 1 \cdot 17 + 12; \\ 17 &= 1 \cdot 12 + 5; \\ 12 &= 2 \cdot 5 + 2; \\ 5 &= 2 \cdot 2 + 1; \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Der $\mathrm{ggT}(a, b)$ ist der letzte Rest ungleich Null. Es gilt also $\mathrm{ggT}(29, 17) = 1$. In analoger Weise berechnet man unter Verwendung der Polynomdivison mit Hilfe des Euklidischen Algorithmus den $\mathrm{ggT}(f, g)$ zweier Polynome $f, g \in \mathbb{C}[X]$.

3. *Bemerkung (Einheiten)*:
Einheiten sind alle Elemente einer Menge, die bezüglich der gegebenen Verknüpfung ein inverses Element innerhalb der Menge besitzen. Die Einheiten von $\mathbb{Z}$ bzgl. der Multiplikation sind $+1$ und -1. Die Einheiten von $\mathbb{C}[X]$ bzgl. der Multiplikation sind die konstanten Polynome $c \in \mathbb{C}^\times$.

4. *Bemerkung (Primzahlen/Primpolynome)*:
Primzahlen bzw. Primpolynome sind jene Elemente einer Menge, die nur durch sich selbst, ihre Gegenzahl und die Einheiten teilbar sind. Die Primpolynome sind somit genau die unzerlegbaren bzw. irreduziblen Polynome. Es gibt unendlich viele Primzahlen und Primpolynome.

5. *Bemerkung (Definition von $n_0(.)$)*:
Für ein Polynom f ist $n_0(f)$ definiert als die Anzahl der verschiedenen Nullstellen von f. Im Raum $\mathbb{C}[X]$ der Polynome mit komplexen Koeffizienten bedeutet dies, dass $n_0(f)$ gleich der Anzahl der verschiedenen Primpolynome von f ist. Daher wirkt zunächst eine Übertragung von n_0 für $a \in \mathbb{Z}$ mit $n_0(a) :=$ Anzahl der verschiedenen Primfaktoren von a als logisch. Im Raum $\mathbb{R}[X]$ kann jedoch die Anzahl der verschiedenen Nullstellen von der Anzahl der Primpolynome abweichen. Beispielsweise hat $f(X) = X^2 + 3$ zwei komplexe Nullstellen, lässt sich jedoch in $\mathbb{R}[X]$ nicht weiter faktorisieren. Glücklicherweise können wir $n_0(f)$ auch als $n_0(f) = \sum_{p|f} \deg(p)$ darstellen, wobei p die Primpolynome von f durchläuft. Analog definieren wir nun unter Berücksichtigung der 1. *Bemerkung* die Funktion $n_0(a)$ wie folgt.

Definition 6.1. *Für $a \in \mathbb{Z}, \ln(|a|) > 0$ definieren wir*

$$n_0(a) := \sum_{\substack{p|a \\ p \text{ Primzahl}}} \ln(p).$$

7 Die *abc*-Vermutung

Mithilfe der Analogie aus Kapitel 6 formulieren wir das Analogon des Satzes von Mason (Theorem 4.4) für ganze Zahlen.

Vermutung 7.1. *Für alle teilerfremden, ganzen Zahlen $a, b, c \in \mathbb{Z}\backslash\{0\}$ mit $a+b=c$ gilt die Ungleichung*

$$\max\big(\ln(|a|), \ln(|b|), \ln(|c|)\big) \leq n_0(a \cdot b \cdot c) - 1.$$

Definition 7.2. *Für $a \in \mathbb{Z}, \ln(|a|) > 0$ definieren wir*

$$N_0(a) := \prod_{\substack{p|a \\ p \text{ Primzahl}}} p.$$

Wir formen die Vermutung 7.1 wie folgt äquivalent um.

$$\begin{aligned}
&\max\big(\ln(|a|), \ln(|b|), \ln(|c|)\big) \leq n_0(a \cdot b \cdot c) - 1 \\
&\Leftrightarrow \ln\big(\max\big(|a|, |b|, |c|\big)\big) \leq \sum_{p|abc} \ln(p) - 1 \\
&\Leftrightarrow \ln\big(\max\big(|a|, |b|, |c|\big)\big) \leq \ln\Big(\prod_{p|abc} p\Big) - 1 \\
&\Leftrightarrow \max\big(|a|, |b|, |c|\big) \leq K \cdot \prod_{p|abc} p = K \cdot N_0(a \cdot b \cdot c), \qquad (7.1)
\end{aligned}$$

wobei $K := \exp(1)^{-1}$ ist und wir die Äquivalenzen unter Berücksichtigung der Definition 6.1, des Logarithmusgesetzes $\ln(a)+\ln(b) = \ln(a \cdot b)$ $(a, b \in \mathbb{N}_{>0})$ und anschließendem Exponentieren erhalten haben.

Wir überprüfen die Vermutung 7.1 mit folgendem Beispiel: Für $n \in \mathbb{N}_{>0}$ seien

$$a := 3^{2^n},\ b := -1,\ c := 3^{2^n} - 1.$$

Zunächst versuchen wir, das Produkt der Primteiler $N_0(a \cdot b \cdot c)$ von $a \cdot b \cdot c$ in (7.1) abzuschätzen. Die Zahl a hat als einzigen Primfaktor die 3, die Zahl b hat keinen und die Zahl c hat mindestens den Primfaktor 2, da c eine gerade Zahl ist. Wir zeigen nun mit Hilfe von vollständiger Induktion, dass sogar

$$2^n | (3^{2^n}) - 1$$

für alle $n \in \mathbb{N}$ gilt. Der Induktionsanfang $n = 0$ ist klar: es gilt $2^0 = 1 | 2 = 3 - 1 = 3^{2^0} - 1$. Wir nehmen nun an, dass $2^n | (3^{2^n} - 1)$ für ein festes $n \in \mathbb{N}$ gilt. Wir zeigen $2^{n+1} | (3^{2^{n+1}} - 1)$ wie folgt:

$$3^{2^{n+1}} - 1 = 3^{2^n \cdot 2} - 1 = (3^{2^n})^2 - 1^2 = (3^{2^n} - 1) \cdot (3^{2^n} + 1).$$

Der Faktor $3^{2^n} - 1$ ist nach Induktionsvoraussetzung durch 2^n teilbar. Der Faktor $3^{2^n} + 1$ ist durch 2 teilbar ist, da $3^{2^n} + 1$ eine gerade Zahl ist. Damit ist das Produkt der beiden Faktoren $(3^{2^n} - 1) \cdot (3^{2^n} + 1) = c$ durch 2^{n+1} teilbar, womit die Behauptung bewiesen ist. Der Faktor $c/2^n$ besitzt möglicherweise weitere Primfaktoren, welche in ihrer Vielfachheit eingehen, jedoch nicht den Primfaktor 3. Damit erhalten wir die folgende Abschätzung:

$$\begin{aligned} N_0(a \cdot b \cdot c) &\leq 3 \cdot 1 \cdot 2 \cdot \frac{c}{2^n} = \frac{6}{2^n}(3^{2^n} - 1) \\ &\leq \frac{6}{2^n} \cdot 3^{2^n}. \end{aligned} \tag{7.2}$$

Da $a + b = c$ mit a, b, c teilerfremd und trivialerweise $|a| = 3^{2^n} \leq \max(|a|, |b|, |c|)$ gilt, erhalten wir aus der Vermutung 7.1 die Ungleichung

$$\begin{aligned} 3^{2^n} &\leq K \cdot N_0(a \cdot b \cdot c) \\ &\leq K \cdot \frac{6}{2^n} \cdot 3^{2^n}, \end{aligned}$$

wobei die zweite Ungleichung aufgrund von (7.2) besteht. Division durch 3^{2^n} liefert die Abschätzung

$$1 \leq K \cdot \frac{6}{2^n}.$$

Für $n \to \infty$ gilt jedoch $6/2^n \to 0$. Demnach müsste $1 \leq 0$ gelten. Das ist ein Widerspruch! Die Vermutung 7.1 ist also in dieser Form falsch.

Die richtige Formulierung der bis heute noch unbewiesenen *abc*-Vermutung lautet:

Vermutung 7.3 (Die *abc*-Vermutung). *Zu $\epsilon > 0$ existiert eine Konstante $K(\epsilon)$, so dass für alle teilerfremden, ganzen Zahlen $a, b, c \in \mathbb{Z} \backslash \{0\}$ mit $a + b = c$ die Ungleichung*

$$\max\big(|a|, |b|, |c|\big) \leq K(\epsilon) \cdot N_0(a \cdot b \cdot c)^{1+\epsilon}$$

gilt.

8 Die *abc*-Vermutung impliziert die Fermat-Vermutung

Wäre die *abc*-Vermutung bewiesen, so erhielte man einen sehr kurzen Beweis für die Richtigkeit der Vermutung von Fermat für große Exponenten $n \in \mathbb{N}$.

Proposition 8.1. *Aus der abc-Vermutung 7.3 folgt, dass die Vermutung von Fermat für große Exponenten $n \in \mathbb{N}$ korrekt ist.*

Beweis. Seien $x, y, z \in \mathbb{N}_{>0}$ teilerfremd mit

$$x^n + y^n = z^n.$$

Wir setzen $a := x^n, b := y^n$ und $c := z^n$. Dann gilt

$$N_0(x^n \cdot y^n \cdot z^n) = N_0(x \cdot y \cdot z) \leq x \cdot y \cdot z.$$

Diese Abschätzung liefert zusammen mit *abc*-Vermutung 7.3 die Ungleichungen

$$x^n \leq K(\epsilon) \cdot (x \cdot y \cdot z)^{1+\epsilon}, \tag{8.1}$$
$$y^n \leq K(\epsilon) \cdot (x \cdot y \cdot z)^{1+\epsilon}, \tag{8.2}$$
$$z^n \leq K(\epsilon) \cdot (x \cdot y \cdot z)^{1+\epsilon}. \tag{8.3}$$

Multiplikation von (8.1), (8.2) und (8.3) ergibt die Ungleichung

$$(xyz)^n \leq K(\epsilon)^3 \cdot (x \cdot y \cdot z)^{3+3\epsilon}. \tag{8.4}$$

Wir setzen $\epsilon' := 3\epsilon$ und dividieren (8.4) durch $(x \cdot y \cdot z)^{3+\epsilon'}$. Man erhält

$$(x \cdot y \cdot z)^{n-(3+\epsilon')} \leq K(\epsilon'/3)^3.$$

Logarithmieren dieser Abschätzung liefert

$$\big(n - (3 + \epsilon')\big) \cdot \ln(x \cdot y \cdot z) \leq 3 \cdot \ln\big(K(\epsilon'/3)\big).$$

Da $a, b, c \in \mathbb{N}_{>0}$ und $a + b = c$ ist, gilt $x \cdot y \cdot z \geq 2$ und damit $1/\ln(x \cdot y \cdot z) \leq 1/\ln(2)$. Damit folgt

$$\begin{aligned} n - (3 + \epsilon') &\leq \frac{3}{\ln(2)} \cdot \ln\big(K(\epsilon'/3)\big) \\ \Longrightarrow n &\leq \frac{3}{\ln(2)} \cdot \ln\big(K(\epsilon'/3)\big) + (3 + \epsilon'). \end{aligned}$$

Wir erhalten also eine Schranke für n, so dass sich die Fermatsche Vermutung für alle genügend großen natürlichen Zahlen n als korrekt herausstellt. □

$\ddot{\smile}$ Schön, dass ihr uns bis hierher gefolgt seid. Leider ist es für uns an der Zeit, Schluss zu machen, aber wir hoffen, es hat euch gefallen und es war klar verständlich. Wir hatten jedenfalls eine Menge Spaß hier und finden es schön, dass noch andere Interesse an der Mathematik zeigen. Sämtliche Rechtschreibfehler sind copyrighted. Missbrauch hat gerichtliche Konsequenzen. Sollte noch etwas unklar sein, schließen wir mit Einsteins Worten: „Man sollte nie aufhören, Fragen zu stellen!“ $\ddot{\smile}$