Der große Satz von Fermat und der Ring $\mathbb{Z}[\rho]$

Vortrag im Rahmen der Vorlesung „Algebra I“ im Wintersemester 2002/03

Tobias Hartnick[†]

1 Der Rand eines Buches

In der Mathematik des antiken Griechenlands, spielte die Ästhetik eine noch größere Rolle, als das in der heutigen Mathematik der Fall ist. Es gehörte zu den Grundüberzeugungen der antiken Mathematik, dass alle Dinge sich durch Verhältnisse ganzer Zahlen zueinander ausdrücken lassen und ihr ästhetischer Wert sich an diesen Zahlenverhältnissen bemisst. Dieses Ästhethik-Verständnis leitete sich aus der musikalischen Harmonielehre ab, in der sich die Saitenteilungsverhältnisse, die den Intervallen entsprechen, ebenfalls durch kleine ganze Zahlen ausdrücken lassen.

Seit Pythagoras (vermutlich auch schon länger) war den Griechen bekannt, dass die Seitenlängen a, b, c eines rechtwinkligen Dreiecks dem Verhältnis

$$a^2 + b^2 = c^2$$

genügen. Ein im Sinne der griechischen Ästhetik „schönes“ rechtwinkliges Dreieck entspricht also einer Lösung dieser Gleichung in den natürlichen Zahlen.

Die Griechen haben über die Jahrhunderte eine bemerkenswerte Vielfalt an Methoden entwickelt, um solche ganzzahligen Lösungen einer Gleichung zu finden. Der griechische Mathematiker Diophant von Alexandria[1] hat die Lösungen vieler dieser Probleme in seiner „Arithmetica“ niedergeschrieben. Noch heute bezeichnet man derartige Probleme deshalb als diophantische Gleichungen. Unter anderem beschäftigt er sich auch mit dem Problem des rechtwinkligen Dreiecks. Die folgende Lösung des Problems ist die Antwort auf Frage 20 im fünften Buch der „Arithmetica“:

1.1 Definition

Ein Tripel $(x, y, z) \in \mathbb{N}^3$ heißt ein primitives pythagoräisches Tripel, wenn es die folgenden beiden Bedingungen erfüllt:

(i) Es gilt: $x^2 + y^2 = z^2$

(ii) Die Zahlen x, y, z sind paarweise teilerfremd.

Jede beliebige ganzzahlige Lösung von Gleichung (i) ist dann von der Form $(x', y', z') = (lx, ly, lz)$ mit einem pythaoräischen Tripel (x, y, z) und einer ganzen Zahl l.

1.2 Satz

Die primitiven pythagoräischen Tripel sind (bis auf mögliche Vertauschung von x und y) genau die Tripel (x, y, z) von der Form $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$ mit natürlichen Zahlen $a > b > 0$, die $\mathrm{ggT}(a, b) = 1$ und $a + b \equiv 1 \mod 2$ erfüllen.

Beweis: Dass jedes solche Paar (a, b) ein pythagoräisches Tripel definiert, ist wegen

[†]Kommentare, Kritik und Anregungen an: tobias.hartnick@tu-clausthal.de

[1]Diophants Lebensdaten lassen sich nur grob eingrenzen. Es wird vermutet, dass seine Hauptwerke um 250 n. Chr. entstanden sind, aber sicher weiß man nur, dass er zwischen 100 v. Chr. und 350 n.Chr. gelebt haben muss.

$$(2ab)^2 + (a^2 - b^2)^2 = 4a^2b^2 + a^4 - 2a^2b^2 + b^4 = a^4 2a^2b^2 + b^4 = (a^2 + b^2)^2$$

klar. Die Primitivität zeigt man leicht und verschiedene Paare ergeben offensichtlich verschiedeme Tripel. Sei andererseits (x, y, z) ein beliebiges primitives pythagoräisches Tripel. x, y können wegen der Teilerfremdheit nicht beide gerade sein. Wären beide ungerade, so wäre $x^2 + y^2 \equiv 2 \mod 4$, aber 2 ist kein Quadrat in $\mathbb{Z}/(4\mathbb{Z})$. O.B.d.A. seien also x gerade und y ungerade. Dann muss z wegen $z^2 = x^2 + y^2$ ungerade sein.

Nach Voraussetzung ist $\text{ggT}(x, z) = 1$. Sei nun $d := \text{ggt}(z - x, z + x)$. Dann gilt:

$$d|(z-x), d|(z+x) \Rightarrow d|(z-x)+(z+x), d|(z-x)+(z+x) \Rightarrow d|2x, d|2z \Rightarrow d|\text{ggt}(2x, 2z) = 2$$

Aber $d \neq 2$, da $z + x$ ungerade ist. Also $d = 1$ und $(z - x), (z + x)$ sind teilerfremd. Andererseits:

$$y^2 = (z - x)(z + x)$$

Also müssen $(z - x)$ und $(z + x)$ Quadrate ganzer Zahlen sein:

$$z - x = u^2, z + x = t^2$$

Da x ungerade und z gerade ist, sind t und u ungerade und es gilt $t > u > 0$. Dann sind $t + u$ und $t - u$ gerade, etwa

$$t + u = 2a, t - u = 2b$$

Dann gilt $t = a + b$, $u = a - b$ und damit schließlich

$$x = \frac{(z+x)-(z-x)}{2} = \frac{t^2-u^2}{2} = \frac{(a+b)^2-(a-b)^2)}{2} = 2ab$$

$$z = \frac{(z+x)+(z-x)}{2} = \frac{t^2+u^2}{2} = \frac{(a+b)^2+(a-b)^2)}{2} = a^2 + b^2$$

$$y = \sqrt{z^2 - x^2} = \sqrt{(a^2+b^2)^2 - (2ab)^2} = \sqrt{a^4 + 2a^2b^2 + b^4 - 4a^2b^2} = \sqrt{a^4 - 2a^2b^2 + b^4} = \sqrt{(a^2-b^2)^2} = a^2 - b^2.$$

Man kann zeigen, dass a, b auch die anderen genannten Voraussetzungen erfüllen.

Als gebildeter Mensch besaß auch der Jurist Pierre de Fermat(1601-1665) eine neuzeitliche Ausgabe der „Arithmetica“, und an eben jener Stelle fügte er seinen berühmt gewordenen Kommentar an:

„Es ist aber nicht möglich, einen Kubus in zwei Kuben, oder ein Biquadrat in zwei Biquadrate und allgemein eine Potenz, höher als die zweite, in zwei Potenzen mit demselben Exponenten zu zerlegen. Ich habe hierfür einen wahrhaft wunderbaren Beweis, doch ist dieser Rand zu schmal, um ihn zu fassen.“

In moderner mathematischer Terminologie heißt das:

$$\forall x, y, z \in \mathbb{Z} \setminus \{0\} : x^n + y^n \neq z^n$$

Der Hobbymathematiker Fermat war berühmt dafür, dass er seinen Mitmenschen ständig mathematischen Rätsel aufgab, die außer ihm selbst niemand beantworten konnte. Es sind unzählige solcher Aufgaben überliefert. Bemerkenswerterweise hat Fermat jedoch diese Randnotiz nie veröffentlicht. Er hat sich aber sehr wohl intensiv mit dieser Behauptung beschäftigt und für den Exponenten $n = 4$ ist von ihm auch eine (ebenfalls unveröffentlichte) Lösung erhalten. Darin entwickelt er eine völlig neuartige und sehr mächtige Methode, die noch heute in der Zahlentheorie von großer Bedeutung ist:

1.3 Satz

Die Gleichung $a^4 + b^4 = c^4$ besitzt keine nichttriviale Lösung in den ganzen Zahlen.

Beweis[2]**:** Wir betrachten die allgemeinere Gleichung $a^4 + b^4 = c^2$ und nehmen an, es gäbe ein Tripel $(x, y, z) \in \mathbb{Z}^3$, das die Gleichung löst. Dann können wir o.B.d.A. die folgenden Annahmen machen:

- $x, y, z \in \mathbb{N}$
- x, y seien teilerfremd. (Andernfalls wäre $ax'^4 + ay'^4 = z^2 \Rightarrow x'^4 + y'^4 = (\frac{z}{a^2})^2$, also gäbe es eine kleinere Lösung)
- x sei gerade und y ungerade. (Wären x, y beide ungerade, so wäre $z^2 = x^4 + y^4 \equiv 2 \mod 4$, aber 2 ist kein Quadrat in $\mathbb{Z}/(4\mathbb{Z})$. Also ist o.B.d.A. x gerade und wegen der Teilerfremdheit y dann ungerade.)

Idee (Fermats Prinzip des Abstiegs[3]**):** Da die Gleichung eine Lösung besitzt, gibt es ein *kleinstes* $z \in \mathbb{N}$, so dass Lösungen (x, y, z) existieren.

Sei also $(x^2)^2 + (y^2)^2 = z^2$ eine in diesem Sinne minimale Lösung. Nach 1.2 existieren dann natürliche Zahlen a, b mit $a > b > 0, \mathrm{ggT}(a, b) = 1$, die

$$x^2 = 2ab, \quad y^2 = a^2 - b^2, \quad z = a^2 + b^2$$

erfüllen. Betrachte nun die Gleichung $b^2 + y^2 = a^2$. Es gilt:

- a ist ungerade und b ist gerade. (a und b können nicht beide gerade oder beide ungerade sein, da sonst $y^2 = b^2 - a^2$ gerade wäre. Wäre b ungerade und a gerade, so wäre $y^2 = a^2 - b^2 \equiv -1 \mod 4$, aber -1 ist kein Quadrat in $\mathbb{Z}/(4\mathbb{Z})$.)
- a, b, y sind paarweise teilerfremd. (a, b sind nach Voraussetzung teilerfremd, wäre t ein gemeinsamer Teiler von y und a, so würde t auch $b^2 = (y \cdot y) - (a \cdot a)$ und damit b teilen, im Widerspruch zur Teilfremdheit von a und b. Durch Vertauschen der Rollen von a und b folgt die Behauptung.)

Wir finden also wiederum nach 1.2 ganze Zahlen c, d mit $c > d > 0$, $\mathrm{ggT}(c, d) = 1$, die

$$b = 2cd, \quad y = c^2 - d^2, \quad a = c^2 + d^2$$

erfüllen.

- $c, d, c^2 + d^2$ sind paarweise teilerfremd. (c, d sind nach Voraussetzung teilerfremd, wäre t ein gemeinsamer Teiler von c und $c^2 + d^2$, so würde t auch $d^2 = (c^2 + d^2) - c \cdot c$ und damit d teilen, im Widerspruch zur Teilfremdheit von c und d. Durch Vertauschen der Rollen von c und d folgt die Behauptung.)

Rückeinsetzen liefert:

$$(\frac{x}{2})^2 = \frac{1}{4}2ab = \frac{1}{2}(c^2 + d^2)(2cd) = cd(c^2 + d^2)$$

Da die Faktoren teilerfremd sind, müssen sie selbst Quadrate sein, d.h. es gibt $p, q, r \in \mathbb{N}$ mit

$$c = p^2, \quad d = q^2, \quad c^2 + d^2 = r^2$$

Dann gilt aber

$$p^4 + q^4 = c^2 + d^2 = r^2,$$

[2]Die hier wiedergegebene Form des Beweises geht auf Euler (1770) zurück.
[3]Auch: „Reductio ad absurdum“ bzw. „ad infinitum“.

d.h. das Tripel (p, q, r) ist ebenfalls eine Lösung der Ausgangsgleichung. Wegen $z = a^2 + b^2 = (c^2 + d^2)^2 + 4c^2d^2 > (c^2 + d^2)^2 = r^4 > r$ ist diese Lösung im obigen Sinne kleiner als (x, y, z), im Widerspruch dazu, dass die Ausgangslösung bereits minimal sein sollte. Also gilt die Behauptung.

Fermats Methode kann in der Tat auf viele andere Exponenten angewendet werden. Die Existenz eines allgemeinen Beweis für alle Zahlen, der auf dieser Methode beruht, wird heute bezweifelt.

Der von $n = 4$ abgesehen einfachste Fall $n = 3$ lässt sich in der Tat mit einem geschickten Fermatabstieg lösen, jedoch benötigt man ein zusätzliches algebraisches Hilfsmittel. Die Idee besteht darin, das Problem zunächst zu verallgemeinern und nach Lösungen der Fermatgleichung im Erweiterungsring $\mathbb{Z}[\rho]$ von $\mathbb{Z}$ zu fragen. In diesem Ring kann man dann gewisse Teilbarkeitsbeziehungen ausnutzen (die es in $\mathbb{Z}$ nicht gibt) und auf diese Weise zu jeder Lösung eine weitere Lösung konstruieren, die in einem gewissen Sinne kleiner ist.[4] Wir stellen im Folgenden die benötigten Eigenschaften dieses Rings kurz zusammen.

[4]Ein alternativer Zugang, der auf Gauß zurückgeht, verwendet stattdessen den sogenannten Eisenstein-Körper $\mathbb{Q}(\sqrt{-3})$

2 Der Ring $\mathbb{Z}[\rho]$

Es sei im Folgenden stets $\rho := \frac{1}{2}(-1 + i\sqrt{3})$.

2.1 Proposition

Beim Rechnen mit ρ sind die folgenden Identitäten nützlich:

(i) ρ ist eine dritte Einheitswurzel, die $\rho + 1 = -\rho^2 = -\overline{\rho}$ erfüllt.

(ii) Für $\alpha, \beta \in \mathbb{C}$ gilt:

$$\alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \rho\beta)(\alpha + \rho^2\beta)$$

Beweis: (i) Nachrechnen.

(ii) Mit (i) rechnet man:

$$(\alpha + \beta)(\alpha + \rho\beta)(\alpha + \rho^2\beta) = (\alpha + \beta)(\alpha^2 + \rho\alpha\beta - (-\rho^2)\alpha\beta + \rho^3\beta^2)$$
$$= (\alpha + \beta)(\alpha^2 + \rho\alpha\beta - (\rho + 1)\alpha\beta + \beta^2) = (\alpha + \beta)(\alpha^2 - \alpha\beta + \beta^2) = \alpha^3 + \beta^3$$

2.2 Erinnerung

In Abschnitt 2.6 der Vorlesung[5] haben wir gesehen:

- $\mathbb{Z}[\rho]$ ist mit der Norm $N(a + b\rho) := (a + b\rho)(a - b\rho) = (a - \frac{1}{2}b)^2 + \frac{3}{4}b^2$ ein euklidischer Ring.
- Die Norm ist multiplikativ, d.h. $N(\chi\xi) = N(\chi)N(\xi)$ für alle $\chi, \xi \in \mathbb{Z}[\rho]$.
- Die Einheitengruppe von $\mathbb{Z}[\rho]$ ist gegeben durch $\mathbb{Z}[\rho]^\times = \{\xi \in \mathbb{Z}[\rho] | N(\xi) = 1\} = \{\pm 1, \pm\rho, \pm\rho^2\}$.

2.3 Proposition

Sei $\lambda := 1 - \rho$

(i) $N(\lambda) = 3$ und λ ist irreduzibel in $\mathbb{Z}[\rho]$.

(ii) Für alle $\omega \in \mathbb{Z}[\rho]$ gilt:

$$\omega \equiv 0 \mod \lambda \vee \omega \equiv 1 \mod \lambda \vee \omega \equiv -1 \mod \lambda$$

(iii) Für alle $\omega \in \mathbb{Z}[\rho]$ gilt:

$$\lambda \nmid \omega \Rightarrow \omega^3 \equiv \pm 1 \mod \lambda^4$$

Beweis: (i) Nach Definition ist $N(\lambda) = (1 - \frac{1}{2}(-1))^2 + \frac{3}{4}(-1)^2 = 3$. Insbesondere ist $N(\lambda)$ irreduzibel in $\mathbb{Z}$ und mit der Multiplikativität der Norm und der Tatsache $N(\xi) = 1 \Rightarrow \xi \in \mathbb{Z}[\rho]^\times$ folgt die Behautptung.

(ii) $\omega \in \mathbb{Z}[\rho]$ besitzt die Form $\omega = a + b\rho$ mit $a, b \in \mathbb{Z}$. Damit:

$$\omega = a + b\rho = a + b - b(1 - \rho) = a + b - b\lambda \equiv a + b \mod \lambda$$

Andererseits besitzt die Zahl 3 in $\mathbb{Z}[\rho]$ die Faktorisierung

$$3 = 1 - \rho - (1 - \rho) + 1 = 1 - \rho - \rho^2 + \rho^3 = (1 - \rho)(1 - \rho^2) = \lambda(1 - \rho^2),$$

[5] Siehe `http://www.math.tu-clausthal.de/Arbeitsgruppen/Zahlentheorie/elsholtz/algebra1/vorlesung.html`.

d.h. $\lambda|3$ Wegen $a+b \in \mathbb{Z}$ existiert ein $r \in \{0, \pm 1\}$ mit $a+b \equiv r \mod 3$ und mit der Teilbarkeit $\lambda|3$ folgt[6]

$$\omega \equiv a+b \equiv r \mod \lambda$$

(iii) Nach (ii) folgt aus $\lambda \nmid \omega$ bereits $\omega \equiv \pm 1 \mod \lambda$. Zur Vereinfachung der Schreibweise sei $\alpha = \pm\omega$ so gewählt, dass $\alpha \equiv 1 \mod \lambda$, d.h. $\alpha = 1 + \beta\lambda$, $\beta \in \mathbb{Z}[\rho]$. Setzen wir in 2.1.(ii) $\beta := -1$, so erhalten wir $\alpha^3 - 1 = (\alpha-1)(\alpha-\rho)(\alpha-\rho^2)$. Damit folgt:

$$\alpha^3 - 1 = (\alpha-1)(\alpha-\rho)(\alpha-\rho^2) = (1+\beta\lambda-1)(1+\beta\lambda-\rho)(1+\beta\lambda-\rho^2) = \beta\lambda(\beta\lambda+1-\rho)(\beta\lambda+(1-\rho^2))$$

$$= \beta\lambda(\beta\lambda+(1-\rho))(\beta\lambda+(1-\rho)(1+\rho)) = \beta\lambda(\beta\lambda+\lambda)(\beta\lambda+\lambda(1+\rho)) = \beta\lambda^3(\beta+1)(\beta+(1+\rho)) \overset{2.1.(i)}{=} \lambda^3\beta(\beta+1)(\beta-\rho^2)$$

Außerdem gilt: $\rho^2 - 1 = (\rho+1)(\rho-1) = (\rho+1)\lambda \equiv 0 \mod \lambda$, d.h. $\rho^2 \equiv 1 \mod \lambda$. Damit ergibt sich auch

$$\beta(\beta+1)(\beta-\rho^2) \equiv \beta(\beta+1)(\beta-1) \mod \lambda.$$

Nach (ii) muss aber eine der drei aufeinanderfolgenden Zahlen $(\beta-1), \beta, (\beta+1)$ durch λ teilbar sein. Also $\beta(\beta+1)(\beta-\rho^2) \equiv 0 \mod \lambda$ und damit

$$\beta(\beta+1)(\beta-\rho^2) \equiv 0 \mod \lambda \Rightarrow \lambda^3\beta(\beta+1)(\beta-\rho^2) \equiv 0 \mod \lambda^4 \Rightarrow \alpha^3 - 1 \equiv 0 \mod \lambda^4$$

Nach Definition von α war nun gerade $\pm(\omega^3 \mp 1) = \alpha^3 - 1 \equiv 0 \mod \lambda^4$, d.h. $\omega^3 \equiv \pm 1 \mod \lambda$.

[6] Bekanntlich gilt: $a+b \equiv r \mod c$, $d|c \Rightarrow a+b \equiv r \mod d$.

3 Ein algebraischer Beweis für $n = 3$

Wir betrachten jetzt wie angekündigt das verallgemeinerte Fermat-Problem für den Exponenten $n = 3$, indem wir Lösungen der Gleichung $\xi^3+\eta^3+\zeta^3 = 0$ nicht nur in $\mathbb{Z}$, sondern auch in $\mathbb{Z}[\rho]$ suchen. Ein erster Schritt in diese Richtung ist das folgende Lemma:

3.1 Lemma

Sein $\xi, \eta, \zeta \in \mathbb{Z}[\rho]$ und λ wie in 2.3 definiert. Dann gilt:

$$\xi^3 + \eta^3 + \zeta^3 = 0 \Rightarrow \lambda | \xi\eta\zeta$$

Beweis: Angenommen $\lambda \nmid \xi\eta\zeta$. Dann gilt nach 2.3.(iv):

$$0 = \xi^3 + \eta^3 + \zeta^3 \equiv \pm 1 \pm 1 \pm 1 \in \{\pm 1, \pm 3\} \mod \lambda^4$$

Dies würde aber bedeuten $\lambda^4 | \pm 1$ oder $\lambda^4 | \pm 3$. Es ist aber $N(\lambda) = 3$ und wegen der Multiplikativität der Norm damit $N(\lambda^4) = (N(\lambda))^4 = 3^4$, aber $N(\pm 1) = 1$, $N(\pm 3) = 9$ und somit $N(\lambda^4) \nmid N(\pm 1)$ bzw. $N(\lambda^4) \nmid N(\pm 3)$. Also kann erst recht keine Teilbarkeit vorliegen und die Annahme war falsch. Es gilt also die Behauptung.

3.2 Bemerkung

Wenn also die für uns interessante Fermatgleichung in $\mathbb{Z}$ eine Lösung besäße, dann gäbe es ein Tripel (ξ, η, ζ) in $\mathbb{Z}[\rho]$ mit $\xi^3 + \eta^3 + \zeta^3 = 0$, wobei eine der drei Zahlen dann durch λ teilbar wäre. Wegen der Symmetrie können wir o.B.d.A. annehmen, dass $\lambda | \zeta$, d.h. $\lambda^n \| \zeta$ für ein $n \geq 1$ gilt. Da es weiterhin keine Einschränkung bedeutet die Zahlen ξ, η und ζ als teilerfremd anzunehmen, genügt es also die Unlösbarkeit der Gleichung

$$\xi^3 + \eta^3 + \lambda^{3n}\gamma^3 = 0$$

in $\mathbb{Z}[\rho]$ unter den Bedingungen $n \geq 1$, $\mathrm{ggT}(\xi, \eta) = 1$ und $\lambda \nmid \xi\eta\gamma$ mittels Abstieg zu zeigen. Es erweist sich als beweistechnisch vorteilhaft, eine leicht verschärfte Variante dieser Aussage zu zeigen:

3.3 Lemma

Seien $\xi, \eta, \gamma \in \mathbb{Z}[\rho]$ und λ wie in 2.3 definiert. Gilt für eine Einheit ε unter den genannten Bedingungen die Gleichung

$$(*) \quad \xi^3 + \eta^3 + \varepsilon\lambda^{3n}\gamma^3 = 0,$$

so ist bereits $n \geq 2$.

Beweis: Die Gleichung $(*)$ impliziert zusammen mit 2.3.(iii) die Kongruenz

$$-\varepsilon\lambda^{3n}\gamma^3 = \xi^3 + \eta^3 \equiv \pm 1 \pm 1 \mod \lambda^4.$$

Erster Fall: $-\varepsilon\lambda^{3n}\gamma^3 \equiv \pm 2 \mod \lambda^4$

Im Falle $n = 1$ bedeutet dies gerade $-\varepsilon\lambda^3\gamma^3 \equiv \pm 2 \mod \lambda^4$ und Multiplikation mit λ liefert $0 \equiv -\varepsilon\lambda^4\gamma^3 \equiv 2\lambda \mod \lambda^4$. Dies würde notwendig $\lambda | 2$ (sogar $\lambda^3 | 2$) zu Folge haben, aber $N(\lambda) = 3$ und $N(2) = 4$. Also muss notwendig $n \geq 2$ gelten.

Zweiter Fall: $-\varepsilon\lambda^{3n}\gamma^3 \equiv 0 \mod \lambda^4$

Wegen $-\varepsilon\gamma^3 \not\equiv 0 \mod \lambda$ bzw. $-\varepsilon\lambda^3\gamma^3 \not\equiv 0 \mod \lambda^4$ bedeutet dies ebenfalls $n \geq 2$.

Unser Fermatabstieg beruht nun auf dem folgenden Argument: Wenn die Gleichung $(*)$ unter den gemachten Voraussetzungen eine Lösung beäße, gäbe es ein kleinstes $n \geq 2$, für dass eine Lösung existierte. Wir zeigen nun, dass wir zu jedem $n \geq 2$ ein kleineres n finden können, so dass ebenfalls eine Lösung existiert. So erhalten wir mit dem Fermatprinzip den gewünschten Widerspruch.

3.4 Satz (Fermat-Abstieg)

Existiert unter den Voraussetzungen von 3.3 eine Lösung der Gleichung $(*)$ für ein $n \geq 2$, so existiert auch eine Lösung für $n-1$ anstatt n.

Beweis: Aus $(*)$ und 2.1.(ii) folgt die Gleichheit $-\varepsilon\lambda^{3n}\gamma^3 = \xi^3 + \eta^3 = (\xi+\eta)(\xi+\rho\eta)(\xi+\rho^2\eta)$.

Behauptung 1: Einer der drei Faktoren ist durch λ^2 teilbar, die beiden anderen durch λ, aber nicht λ^2.

Zunächst ist $(\xi+\eta)(\xi+\rho\eta)(\xi+\rho^2\eta) \equiv 0 \mod \lambda^{3n}$ mit $3n > 3$, also muss mindestens einer der drei Faktor durch λ^2 teilbar sein. Um daraus die Behauptung zu folgern, betrachten wir die Differenzen der drei Faktoren. Es gilt:

$$(\xi+\eta) - (\xi+\rho\eta) = \eta(1-\rho) = \eta\lambda$$

$$(\xi+\rho\eta) - (\xi+\rho^2\eta) = \eta(\rho-\rho^2) = \eta\rho(1-\rho) = \rho\eta\lambda$$

$$(\xi+\eta) - (\xi+\rho^2\eta) = \eta(1-\rho^2) = \eta\rho^3 - \rho^2 = \rho^2\eta(1-\rho) = \rho^2\eta\lambda$$

Die Differenzen sind also zueinander konjugierte Vielfache von λ, aber keien Vielfachen von λ^2. Damit haben wir:

- λ teilt einen der Faktoren und alle Differenzen. $\longrightarrow$ λ teilt alle Faktoren.
- λ^2 teilt einen der Faktoren und keine der Differenzen. $\longrightarrow$ λ^2 teilt genau einen Faktor.

Damit haben wir Behauptung 1 gezeigt.

Da die Differenzen konjugiert sind, können wir durch geeignete Wahl der Einheit ε o.B.d.A. voraussetzen, dass λ^2 den ersten Faktor teilt. Wir erhalten damit

$$(**) \quad \xi+\eta = \lambda^{3n-2}\kappa_1, \quad \xi+\rho\eta = \lambda\kappa_2, \quad \xi+\rho^2\eta = \lambda\kappa_3$$

für irgendwelche $\kappa_1, \kappa_2, \kappa_3 \in \mathbb{Z}[\rho]$, die keinen Teiler λ mehr enthalten.

Behauptung 2: Die Zahlen $\kappa_1, \kappa_2, \kappa_3$ sind paarweise teilerfremd.

Wir zeigen dies nur für κ_2 und κ_3, die anderen Fälle gehen analog. Es gilt:

$$(\kappa_2 - \kappa_3)\lambda = (\xi+\rho\eta) - (\xi+\rho^2\eta) = \rho(1-\rho)\eta = \rho\lambda\eta$$

Also $\kappa_2 - \kappa_3 = \rho\eta$. Andererseits gilt:

$$\rho(\lambda\kappa_3) - \rho^2(\lambda\kappa_2) = \rho(\xi+\rho^2\eta) - \rho^2(\xi+\rho\eta) = \rho\xi + \eta - \rho^2\xi - \eta = \rho(\rho-1)\xi = \rho\lambda\xi$$

Also $\rho\kappa_3 - \rho^2\kappa_2 = \rho\xi$. Ist nun τ eine gemeinsamer Teiler von κ_2 und κ_3, so folgt $\tau|\eta$ und $\tau|\xi$. Nach Voraussetzung ist dann τ eine Einheit. Dies liefert (den betrachteten Teil von) Behauptung 2.

Andererseits waren die κ_i ja gerade so gewählt, dass

$$-\varepsilon\lambda^{3n}\gamma^3 = \lambda^{3n-2}\kappa_1\lambda\kappa_2\lambda\kappa_3$$

gilt, d.h.

$$-\varepsilon\gamma^3 = \kappa_1\kappa_2\kappa_3$$

und aus der paarweisen Teilerfremdheit folgt dann, dass die κ_i bis auf Einheiten selbst dritte Potenzen sein müssen:

$$(***) \quad \kappa_1 = \varepsilon_1\theta^3, \quad \kappa_2 = \varepsilon_2\varphi^3, \quad \kappa_3 = \varepsilon_3\psi^3 \quad (\varepsilon_i \in \mathbb{Z}[\rho]^\times, \theta, \phi, \psi \in \mathbb{Z}[\rho] \text{ paarweise teilerfremd})$$

Behauptung 3 Eines der beiden Tripel $(\theta, \phi, \pm\psi)$ löst die Gleichung $(*)$ für $(n-1)$ anstatt n.

Setzen wir $(***)$ in $(**)$ ein, so erhalten wir

$$\xi + \eta = \varepsilon_1\lambda^{3n-2}\theta^3, \quad \xi + \rho\eta = \varepsilon_2\lambda\varphi^3, \quad \xi + \rho^2\eta = \varepsilon_3\lambda\psi^3$$

Dies bedeutet aber:

$$0 = (1+\rho-(\rho+1))(\xi+\eta) = (1+\rho-(-\rho^2))(\xi+\eta) = (\xi+\eta)+\rho(\xi+\eta)+\rho^2(\xi+\eta) \overset{\rho^4=\rho}{=} \xi+\eta+\rho\xi+\rho^4\eta+\rho^2\xi+\rho^2\eta$$

$$= \xi + \eta + \rho\xi + \rho^2\eta + \rho^2\xi + \rho^4\eta = (\xi+\eta) + \rho(\xi+\rho\eta) + \rho^2(\xi+\rho^2\eta) = \varepsilon_1\lambda^{3n-2}\theta^3 + \rho\varepsilon_2\lambda\varphi^3 + \rho^2\varepsilon_3\lambda\psi^3$$

Kürzen von λ und Division durch $\rho\varepsilon_2$ liefert die Gleichung

$$\varphi^3 + \varepsilon_4\psi^3 + \varepsilon_5\lambda^{3n-3}\theta^3 = 0,$$

für gewisse Einheitem $\varepsilon_4, \varepsilon_5$. Es bleibt zu zeigen, dass $\varepsilon_4 = \pm 1$ gilt. (Das Vorzeichen können wir mit dem Vorzeichen von ψ korrigieren.) Dazu betrachten wir zunächst die Kongruenz

$$\varphi^3 + \varepsilon_4\psi^3 = -\lambda^{3n-3}\theta^3 \overset{n\geq 3}{\Rightarrow} \varphi^3 + \varepsilon_3\psi^3 \equiv 0 \mod \lambda^2$$

Wegen $\lambda \nmid \varphi$ und $\lambda \nmid \psi$ gilt dann nach 2.3.(iii) schon $\varphi^3 \equiv \pm 1 \mod \lambda^4$ und $\psi^3 \equiv \pm 1 \mod \lambda^4$, also gelten diese Kongruenzen erst recht modulo λ^2. Dies liefert:

$$0 \equiv \varphi^3 + \varepsilon_4\psi^3 \equiv \pm 1 \pm \varepsilon_4 \mod \lambda^2$$

Nach 2.2 kann $\pm 1 \pm \varepsilon_4$ nur Werte aus $\{\pm 1 \pm 1, \pm 1 \pm \rho, \pm 1 \pm \rho^2\}$ annehmen. Wir müssen zeigen, dass $\pm 1 \pm \varepsilon_4 = \pm 1 \pm 1$. Nun gilt aber mit $\rho^2 = -\rho - 1$:

$$\pm 1 \pm \varepsilon_4 = \left\{ \begin{array}{l} \pm(1+\rho) \\ \pm(1-\rho) \\ \pm(1+\rho^2) \\ \pm(1-\rho^2) \end{array} \right\} \Rightarrow \pm 1 \pm \varepsilon_4 = \left\{ \begin{array}{l} \pm(1+\rho) \\ \pm(1-\rho) \\ \pm\rho \\ \pm(2+\rho) \end{array} \right\} \Rightarrow N(\pm 1 \pm \varepsilon_4) = \left\{ \begin{array}{l} 3 \\ 1 \\ 1 \\ 3 \end{array} \right\}$$

Diese Zahlen können aber nicht von λ^2 mit $N(\lambda^2) = N(\lambda)^2 = 9$ geteilt werden. Also gilt Behauptung 3 und damit die gesamte Behauptung.

Beachten wir das Prinzip des Fermatabstiegs und das in 3.2 Gesagte, so erhalten wir schließlich:

3.5 Korollar

Die Gleichung $\xi^3 + \eta^3 + \varepsilon\lambda^{3n}\gamma^3 = 0$ besitzt unter den Voraussetzungen von 3.3 keine Lösung. Es gilt der große Satz von Fermat für den Exponenten $n = 3$.

Man beachte, dass der Fall $n = 3$ aus zwei Gründen relativ einfach zu behandeln ist:

- Die Gleichung $\alpha^3 + \beta^3 = \gamma^3$ kann mittels der Beziehung $\alpha^3 + \beta^3 = (\alpha+\beta)(\alpha+\rho\beta)(\alpha+\rho^2\beta)$ in einem *Erweiterungsring* von $\mathbb{Z}$ vereinfacht werden.
- Der spezielle Erweiterungsring $\mathbb{Z}[\rho]$ ist *euklidisch* mit multiplikativer Norm. Wir können deshalb einerseits Teilbarkeitsbedingungen und andererseits Teilbarkeitsbedingungen der Normen ausnutzen.

4 Der Fall $n = 5$ und Sophie-Germain-Primzahlen

Der nächste zu untersuchende Fall wäre $n = 5$. Dieser Fall ist auch deshalb interessant, weil man ein allgemeineres Prinizip erkennt:

4.1 Definition

Eine Primzahl p heisst **Sophie-Germain-Primzahl**, wenn sie ungerade ist und auch $q := 2p + 1$ eine Primzahl ist.

5 ist wegen $2 \cdot 5 + 1 = 11$ Sophie-Germai-Primzahl. Bei solchen Primzahlen erweist es sich als zweckmäßig, den Beweis in zwei Schritte zu unterteilen:

- **Fall 1:** Es gibt keine Lösung der Gleichung $x^p + y^p + z^p = 0$ für ganze Zahlen x, y, z mit $p \nmid xyz$.
- **Fall 2:** Es gibt keine Lösung der Gleichung $x^p + y^p + z^p = 0$ für ganze Zahlen x, y, z mit $p|xyz$.

Fall 1 ist stets der einfachere Fall. Im Fall $p = 5$ ist er besonders einfach:

Fall 1 für n=5: Wir zeigen zunächst:

$$\textit{Für beliebige } a, b \in \mathbb{Z} \textit{ folgt aus } a \equiv b \mod 5 \textit{ schon } a^5 \equiv b^5 \mod 5^2.$$

Seien also $a, b \in \mathbb{Z}$ mit $a - b = 5c$ für ein $c \in \mathbb{Z}$. Dann gilt:

$$(a-b)^5 = a^5 - 5a^4b + 10a^3b^2 - 10a^2b^3 + 5ab^4 - b^5 = a^5 - b^5 - 5(a^4b - ab^4) + 10(a^3b^2 - a^2b^3)$$

Beachtet man $a^4b - ab^4 = ab(a^3 - b^3) = ab(a^2 + b^2)(a - b) = 5ab(a^2 + b^2)c$ und $a^3b^2 - a^2b^3 = a^2b^2(a - b) = 5a^2b^2c$ einerseits und $(a - b)^5 = 25c^2$ andererseits, so erhält man:

$$25c^2 = a^5 - b^5 - 25ab(a^2 + b^2)c + 50a^2b^2c$$

Also $a^5 - b^5 \equiv 0 \mod 5^2$.

Damit können wir jetzt unsere Behauptung beweisen: Angenommen es wäre $x^5 + y^5 + z^5 = 0$ und $5 \nmid xyz$. Dann wären x, y, z modulo 5 kongruent zu ± 1 oder ± 2. Wegen $(\pm 1)^5 = \pm 1$ und $(\pm 2)^5 = 32 \equiv 2 \mod 5$ folgt daraus $x^5 \equiv x \mod 5$ und analog für y und z. Dies liefert:

$$x + y + z \equiv 0 \mod 5$$

Da keiner der drei Summanden 0 ist kann dies nur dann der Fall sein, wenn zwei der Zahlen kongruent zu ± 1 und die andere kongruent zu ∓ 2 ist. Insbesondere müssen zwei der Zahlen kongruent modulo 5 sein, o.B.d.A. etwa x und y. Wir haben also $x \equiv y \mod 5$ und nach dem eben gezeigten damit

$$x^5 \equiv y^5 \mod 5^2.$$

Dies liefert:

$$x^5 + y^5 + z^5 \equiv 0 \mod 5 \Rightarrow -z^5 \equiv x^5 + y^5 \equiv 2x^5 \mod 5^2$$

Aber es gilt auch:

$$x + y + z \equiv 0 \mod 5 \Rightarrow -z \equiv x + y \equiv 2x \mod 5 \Rightarrow -z^5 \equiv 2^5 x^5 \mod 5^2$$

Dies zusammen bedeutet aber $2^5 \equiv 2 \mod 5^2$ und das ist offensichtlich falsch.

Will man den ersten Fall für eine beliebige Sophie-Germain-Primzahl behandeln, so kann man das folgende Lemma benutzen:

4.2 Lemma (Sophie Germain)

Seien p, q verschiedene Primzahlen, die den folgenden Bedingungen genügen:

(i) Gilt $x^p + y^p + z^p \equiv 0 \mod q$, so gilt auch $q|xyz$.

(ii) $a^p \not\equiv p \mod q$ für alle $a \in \mathbb{Z}$.

Dann gilt „Fall 1“ für den Exponenten p.

Ist p eine Sophie-Germain-Primzahl und $q := 2p + 1$, so kann man nachweisen, dass p und q den Voraussetzungen des Sophie-Germain-Lemmas genügen.[7] Damit hat man:

4.3 Satz

Sei p eine Sophie-Germain-Primzahl und $x^p + y^p + z^p = 0$ für ganze Zahlen x, y, z mit $p \nmid xyz$. Dann ist $x = y = z = 0$.

4.4 Bemerkung

Mithilfe des Sophie-Germain-Lemmas konnte Legendre den ersten Fall auch für Primzahlen p mit $ap+1 \in \mathbb{P}$ und $a \in \{4, 8, 10, 14, 16\}$ beweisen. Der zweite Fall ($p|xyz$) ist aber schon im Fall $n = 5$ aufwendig (mehrstufiger Abstieg, sehr unübersichtlich, irgendwann gehen die Buchstaben aus, s.[Rib99]. S.52 ff.). Man findet aber kein allgemeines Beweisprinizip für den zweiten Fall aller Sophie-Germain-Primzahlen.

4.5 Ausblick

Selbst wenn man einen Beweis für den vielzitierten „Second Case“ hätte, der für alle Sophie-Germain-Primzahlen funktionieren würde, wäre man immer noch weit von einem Beweis von Fermats letztem Satz entfernt. Man ist sich heute weitgehend einig, dass die Bearbeitung der großen Fermatschen Satzes allein mit Mitteln der elementaren Algebra nicht gelingen kann. Die entsprechenden Versuche waren aber aus heutiger Sicht trotzdem äußerst fruchtbar: Auf der Suche nach dem großen Beweis wurden Methoden entwickelt, ohne die die moderne Algebra undenkbar wäre. Beispielsweis wurde die gesamte Theorie der Erweiterungsringe eigens für den Fall $n = 3$ entwickelt! Ohne diese moderne Algebra wüssten wir heute auch nichts über algebraische Geometrie, elliptische Kurven oder Modulformen - kurz: wir wüssten nichts über die Hilfsmittel, mit denen Andrew Wiles 1995 den großen Fermatschen Satz - bzw. in der heute üblichen Bezeichnung: den Satz von Fermat-Wiles - schlussendlich beweisen konnte.

[7] Eine detaillierte Diskussion des Sophie-Germain-Lemmas und seiner Anwendungen findet sich in [Rib99]. Der hier zitierte Nachweis ist auf S.112 näher ausgeführt.

A Literatur

Ich habe mich bei meiner Ausarbeitung an die folgenden Bücher gehalten:

- [Har79] Hardy, G.H./Wright, E.M.: An Introduction to the Theory of Numbers, Oxford University Press, Oxford 1979
- [Rib99] Ribenboim, R.: Fermat's Last Theorem for Amateurs, Springer, New York 1999
- [Sin00] Singh, S.: Fermats letzter Satz, dtv, München 2000
- [Sti89] Stillwell, J.: Mathematics and Its History, Springer, New York 1989

[Har79] ist *der* Klassiker auf dem Gebiet der Zahlentheorie, der inzwischen aber in einigen Punkten veraltet ist. [Rib99] ist eine sehr ausführliche, historisch orientierte Darstellung der algebraischen Methoden, die im Zusammenhang mit Fermats Satz entwickelt wurden. [Sti89] ist eine sehr schöne Zusammenstellung klassischer mathematischer Probleme mit vielen historischen Anmerkungen.

Alle genannten Bücher mit Ausnahme von [Sin00] sind in der Institutsbibliothek vorhanden ([Har79] auch in deutscher Übersetzung). Dort findet man auch eine ganze Reihe weiterführender Literatur zum Problemkreis dieses Vortrags, etwa:

- [Har77] Edwards, H.M.: Fermat's Last Theorem - A Generic Introduction to Algebraic Number Theory, Springer, New York 1977
- [Ste79] Stewart, I.N./Tall, D.O.: Algebraic Number Theory, Chapman and Hall, London 1979