Math Semesterber (2009) 56: 105–122
DOI 10.1007/s00591-008-0050-6

Die eindeutige Primfaktorzerlegung

Urs Stammbach

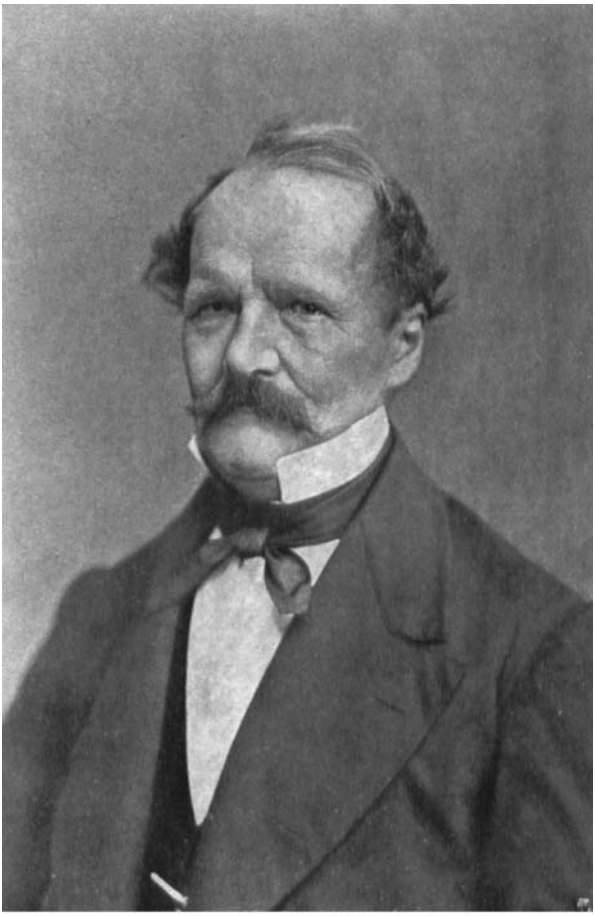
Eingegangen: 18. Juni 2008 / Angenommen: 25. Oktober 2008 / Online: 13. Januar 2009

Zusammenfassung Die Frage der Primfaktorzerlegung in Unterringen der komplexen Zahlen und der unmittelbar damit zusammenhängenden Sätze wird in der heutigen Algebra ohne grossen Aufwand und fast nebenbei behandelt: Studierende haben damit auch kaum Schwierigkeiten. In der Geschichte allerdings verlief die Entwicklung alles andere als gradlinig. Ein genauerer Blick auf die historischen Einzelheiten erlaubt interessante und in vielerlei Hinsicht überraschende Einsichten in die vertrackte Art und Weise, wie sich Mathematik manchmal entwickelt. Hier soll diese Geschichte erzählt werden, wie sie sich aus den neueren mathematikhistorischen Forschungen von H.M. Edwards, R. Bölling, O. Neumann und F. Lemmermeyer ergibt, und zwar auf einem Niveau, das einem Mathematikstudierenden nach einer Algebra-Vorlesung zugänglich ist.

Einleitung

Die hier beschriebenen Vorgänge sind in der mathematischen und der mathematikgeschichtlichen Literatur oft angesprochen worden. Dabei haben sich am Anfang des 20. Jahrhunderts Legenden festgesetzt, die auch von sonst ernstzunehmenden Autoren wie Leonard Eugene Dickson, Felix Klein, Nicolas Bourbaki u. a. in ihren Beiträgen zur Mathematikgeschichte wiederholt wurden. Diese auf David Hilbert und Kurt Hensel (siehe [10, 12]) zurückgehenden Legenden behaupten, dass Eduard Kummer seinerzeit die eindeutige Primfaktorzerlegung in Ringen von Einheitswurzeln für einen – falschen – Beweis der Fermat-Vermutung verwendet habe und dann von Dirichlet auf den Irrtum aufmerksam gemacht worden sei. Erst 1975 hat Harold M. Edwards (siehe [7]) in seinen sorgfältigen Analysen die Unhaltbarkeit dieser

U. Stammbach (✉)
Mathematik, ETH-Zentrum, CH-8092 Zürich, Switzerland
e-mail: stammb@math.ethz.ch



E. E. Kummer

Darstellungen nachgewiesen. Er stützte sich dabei auf Dokumente, die entweder vorher nicht bekannt waren oder vorher nicht in diesem Zusammenhang interpretiert wurden. In der Folge haben Olaf Neumann (siehe [22–25]), Reinhard Bölling (siehe [1, 2]) und Franz Lemmermeyer (siehe [21]) die Auffassungen Edwards im wesentlichen bestätigt; in einigen Teilen haben sie aber auch wichtige Korrekturen anbringen können.

Die Geschichte, wie sie sich gemäss diesen Forschungen abgespielt hat, verlief nicht ganz so – und auch nicht so gradlinig –, wie es die Legenden wahr haben wollten. Vielmehr trat eine Reihe von unerwarteten Verwicklungen und Komplikationen auf, und am Rande der Geschehnisse waren neben Kummer viele weitere Mathematiker beteiligt, oft in einer Art, die überraschende Seitenblicke auf deren Persönlichkeiten eröffnen.

Der vorliegende Text will keine neuen Beiträge zu den Geschehnissen jener Zeit liefern, sondern einfach auf der Grundlage der existierenden mathematikhistorischen Literatur die Geschichte zusammenhängend erzählen. Der Text soll dabei für heutige Studierende der Mathematik leicht zugänglich sein. Nicht zuletzt aus diesem Grund, aber auch um den Fluss und die Dramatik der Entwicklungen deutlicher hervortreten zu lassen, kommen viele mathematische Einzelheiten hier nicht zur Sprache, die sich aus dem damaligen Stand der Mathematik erklären, deren Inhalt und deren Stellenwert aber heute nicht mehr ohne weiteres ersichtlich sind.

Der Autor dankt den Referenten für zahlreiche wichtige Bemerkungen, die zu einer wesentlichen Verbesserung dieses Textes geführt haben.

Zur eindeutigen Primfaktorzerlegung in Mathematik-Geschichte und Mathematik-Studium

Wer Mathematik anfängt zu studieren, weiss gewöhnlich beim Eintritt in die Hochschule schon, was eine *Primzahl* ist, eine ganze Zahl p nämlich, die ausser $\pm p$ und ± 1 keine weiteren Teiler besitzt. „Man" weiss ferner auch, dass sich jede ganze Zahl in „eindeutiger Weise" in ein Produkt von Primzahlen zerlegen lässt. Ist n eine ganze Zahl, $n \neq 0, \pm 1$, so lässt sich n – erstens – schreiben als Produkt von Primzahlen $n = p_1 p_2 \cdots p_r$ und – zweitens – gilt: wenn eine zweite solche Darstellung $n = q_1 q_2 \cdots q_s$ gegeben ist, so folgt $r = s$ und – möglicherweise nach einer Umnummerierung – $p_k = \pm q_k$ für $k = 1, 2, \ldots, r$.

Etwas später, in der ersten Algebravorlesung, hört der Student, die Studentin dann von den komplexen ganzen Zahlen, den Gaussschen Zahlen $\mathbb{Z}[i]$, und lernt, dass in $\mathbb{Z}[i]$ die eindeutige Primfaktorzerlegung ebenfalls gilt. Das entsprechende Resultat lautet folgendermassen: Ist $a + ib \in \mathbb{Z}[i]$, also $a, b \in \mathbb{Z}$, und ist $a + ib \neq \pm 1$, $\pm i$, so gibt es in $\mathbb{Z}[i]$ unzerlegbare Zahlen $p_1, p_2, \ldots, p_n$ mit $a + ib = p_1 p_2 \cdots p_n$. Ferner ist diese Darstellung im folgenden Sinn eindeutig: Ist $a + ib = q_1 q_2 \cdots q_m$ eine zweite solche Darstellung, so folgt $n = m$ und – möglicherweise nach einer Umnummerierung – $p_k = \varepsilon_k q_k$ mit $\varepsilon_k = \pm 1$ oder $\varepsilon_k = \pm i$ für $k = 1, 2, \ldots, n$. Ein Element $u + iv \in \mathbb{Z}[i]$ heisst dabei *unzerlegbar*, wenn es von ± 1 und $\pm i$ verschieden ist und wenn es ausser $\pm(u + iv)$, $\pm i(u + iv)$, ± 1 und $\pm i$ keine Teiler in $\mathbb{Z}[i]$ besitzt. Die hier an mehreren Orten auftretenden Elemente ± 1 und $\pm i$ sind die *Einheiten* von $\mathbb{Z}[i]$; es sind die Elemente $\varepsilon \in \mathbb{Z}[i]$, für die ein $\varepsilon' \in \mathbb{Z}[i]$ existiert mit $\varepsilon\varepsilon' = 1$. In $\mathbb{Z}[i]$ ist also die Darstellung eines Elementes als Produkt von unzerlegbaren Elementen bis auf Reihenfolge und Multiplikation mit einer Einheit eindeutig.

Gewöhnlich wird an dieser Stelle der Algebravorlesung in der Terminologie zwischen Primelementen und unzerlegbaren Elementen unterschieden. Es wird definiert: Ein Element μ heisst ein *Primelement*, wenn es keine Einheit ist und ferner die Eigenschaft hat, dass μ ein Produkt nur dann teilt, wenn es mindestens einen der Faktoren teilt. Auf Grund der Eindeutigkeit der Zerlegung in unzerlegbare Faktoren folgt somit unmittelbar, dass in $\mathbb{Z}[i]$ jedes unzerlegbare Element die Eigenschaft eines Primelementes besitzt.

Wir werden in diesem Beitrag nur Unterringe R von komplexen Zahlen betrachten. In diesem Fall ist eine Zerlegung von Nichteinheiten in ein Produkt von unzerlegbaren Faktoren *immer* gegeben. Dies folgt direkt mit Hilfe der Norm $N(a+ib) = a^2 + b^2$. Es gilt nämlich: Ein Element ε ist genau dann eine Einheit, falls seine Norm Eins ist, $N(\varepsilon) = 1$. Die Norm eines Produktes ist ferner stets das Produkt der Normen der Faktoren. Wenn also in einem Produkt keiner der Faktoren eine Einheit ist, so sind die Normen der Faktoren stets echt kleiner als die Norm des Produktes. Daraus ergibt sich, dass jede Nichteinheit sukzessive in Faktoren zerlegt werden kann, bis die auftretenden Faktoren Einheiten oder nichtzerlegbare Elemente sind. Die Frage stellt sich also nun in einer etwas andern Form, nämlich, ob solche Faktorzerlegungen in unzerlegbare Elemente (bis auf Einheiten) *eindeutig* sind.

Gauss weist die Eindeutigkeit der Zerlegung im Bereich der ganzen Zahlen $\mathbb{Z}$ am Anfang seiner *Disquisitones arithmeticae* (§16) sorgfältig nach. Er folgert sie aus der Tatsache (siehe §14), dass eine Primzahl p ein Produkt ab nur dann teilen kann, wenn p (mindestens) einen der Faktoren teilt. Dieses Resultat, das Gauss Euklid zuschreibt, folgt umgekehrt unmittelbar aus der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$. Die beiden Aussagen sind also in $\mathbb{Z}$ gleichbedeutend. Diese Äquivalenz der beiden Aussagen gilt nun offensichtlich auch für die Faktorzerlegung in unzerlegbare Elemente in den hier betrachteten Unterringen von komplexen Zahlen. Wenn wir den oben eingeführten Begriff eines Primelementes benützen, so gilt also: Die Faktorzerlegung in unzerlegbare Elemente in einem Ring R ist genau dann eindeutig, wenn die unzerlegbaren Elemente in R auch Primelemente sind. Für den Zweck dieses Textes werden die beiden Aussagen als gleichbedeutend behandelt.[1]

In der einführenden Algebravorlesung kommt dann gewiss auch noch ein Beispiel eines Ringes R vor, in dem Zerlegungen in unzelegbare Elemente *nicht eindeutig* zu sein brauchen. Üblicherweise ist dies das Beispiel $\mathbb{Z}[\sqrt{-5}]$, der Ring der komplexen Zahlen der Form $a + ib\sqrt{5}$, $a, b \in \mathbb{Z}$. Hier kann man ohne Schwierigkeiten wesentlich verschiedene Zerlegungen von Zahlen in Produkte von unzerlegbaren Elementen angeben; dies gilt zum Beispiel für die Zahl 6, wo man die zwei folgenden wesentlich verschiedenen Zerlegungen hat

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Die Elemente 2, 3, $1 + i\sqrt{5}$, $1 - i\sqrt{5}$ sind unzerlegbar, wie man unmittelbar sieht, wenn man ihre Normen betrachtet. Es gibt also im Ring $\mathbb{Z}[\sqrt{-5}]$ *keine eindeutige* Zerlegung in unzerlegbare Faktoren.

Aus diesen Bemerkungen wird klar, dass die eindeutige Primfaktorzerlegung heute von Studierenden als spezielle Eigenschaft eines Ringes erkannt wird. Dies war in der Geschichte der Mathematik für lange Zeit nicht der Fall. Natürlich spielt dabei die Tatsache ein grosse Rolle, dass die komplexen Zahlen erst erstaunlich spät

[1] Von einem streng historischen Standpunkt aus müsste man die beiden, für uns offensichtlich äquivalenten Aussagen trotzdem wohl als unterschiedlich ansehen. Dies hängt zusammen mit der Tatsache, dass bis in die Mitte des 19. Jahrhunderts der Begriff eines Ringes in unserem heutigen Sinn, nämlich als eine (wohldefinierte) *Menge* mit Addition und Multiplikation, nicht existierte.

voll als mathematisches Objekte anerkannt worden sind, – dies geschah bekanntlich ausserhalb eines kleinen Kreises von Spezialisten erst im Gefolge der *Commentatio secunda* von Gauss aus dem Jahre 1831 (siehe [9]). Daneben war aber wohl die Gewöhnung an die eindeutige Primfaktorzerlegung im Bereich $\mathbb{Z}$ derart prägend, dass sich viele gar nichts anderes vorstellen konnten.

Man kann dies – wie ich meine – deutlich im Abschnitt der *Commentatio secunda* von Gauss erkennen, wo die Eindeutigkeit der Zerlegung im Bereich der komplexen ganzen Zahlen bewiesen wird. Nachdem Gauss gezeigt hat, dass sich jede komplexe ganze Zahl als Produkt von unzerlegbaren komplexen ganzen Zahlen schreiben lässt, sagt er dort in §37:

Circa hanc resolutionem theorema se offert, unico tantum modo eam fieri posset, quod theorema obiter quidem consideratum per se manifestum videri posset, sed utique demonstratione eget.[2]

Gauss war sich im Gegensatz zu anderen offenbar durchaus im klaren darüber, dass die Eindeutigkeit der Zerlegung nicht selbstverständlich ist. Wie wir oben bereits bemerkt haben, hat er auch für (gewöhnliche) ganze Zahlen am Anfang seiner *Disquisitiones arithmeticae* (siehe §16) die Eindeutigkeit der Primfaktorzerlegung sorgfältig nachgewiesen. Was die Eindeutigkeit der Faktorzerlegung im Bereich der ganzen komplexen Zahlen betrifft, so war Gauss ausserdem der folgende Zusammenhang sicher sehr bewusst. Es war von Fermat vermutet und von Euler bewiesen worden, dass die (gewöhnliche) ungerade Primzahl p genau dann als Summe von zwei Quadraten geschrieben werden kann, wenn p von der Form $4k+1$ ist; ferner hatte Euler auch bewiesen, dass eine solche Darstellung $p = a^2 + b^2$ (bis auf Vorzeichen und Vertauschung) nur auf eine *einzige* Weise möglich ist. Gauss führt in der Tat diesen Satz in §182 seiner *Disquisitiones arithmeticae* an. In der *Commentatio secunda* bildete die Interpretation dieses Resultates im Bereich der komplexen ganzen Zahlen die Basis seiner Überlegungen. Unter den ungeraden Primzahlen p können genau diejenigen der Form $4k+1$ im Bereich der komplexen ganzen Zahlen als Produkt $(a+ib)(a-ib)$ geschrieben werden, denn die Faktorisierung $(a+ib)(a-ib) = p$ ist gleichbedeutend mit $a^2 + b^2 = p$. Mit Hilfe der Tatsache, dass die Zahlen a und b in der Darstellung $p = a^2 + b^2$ im wesentlichen *eindeutig* bestimmt sind, folgert Gauss dann die Eindeutigkeit der Primfaktorzerlegung im Bereich der komplexen ganzen Zahlen. Wäre umgekehrt im Bereich der komplexen ganzen Zahlen die Zerlegung in unzerlegbare Faktoren nicht eindeutig, so ergäbe sich daraus leicht ein Widerspruch zur Eindeutigkeit der Darstellung von Primzahlen als Summen von Quadraten. Der enge Zusammenhang zwischen den beiden Aussagen war Gauss zu Zeiten seiner *Commentatio secunda* zweifellos klar.

Hier wollen wir als nächstes in der Geschichte einen Schritt zurück machen und zeigen, wie das Vertrauen auf die von den (gewöhnlichen) ganzen Zahlen bekannten Rechengesetze, wie insbesondere auf das Gesetz der eindeutigen Faktorzerlegung, selbst so prominente Mathematiker wie Leonhard Euler fehlgeleitet haben.

[2] Eine sinngemässe deutsche Übersetzung lautet etwa so: *Im Zusammenhang damit drängt sich die Vermutung auf, dass eine solche Darstellung nur auf eine einzige Art möglich ist. Diese Tatsache könnte zwar auf den ersten Blick offensichtlich erscheinen, aber sie benötigt durchaus einen Beweis.*

Ein solches Beispiel finden wir in Euler's *Vollständige Anleitung zur Algebra*, die 1770 erschien.[3] Die Stelle, die wir zitieren wollen, ist *Des zweyten Theils zweyter Abschnitt* §182. Dort sagt Euler:

Es sey daher diese Formel vorgelegt $xx + cyy$, *welche zu einem Quadrat gemacht werden soll. Da nun dieselbe aus diesen Faktoren besteht*

$$(x + y\sqrt{-c})(x - y\sqrt{-c}),$$

so müssen dieselben entweder Quadrate, oder mit einerley Zahlen multiplizirte Quadrate seyn. Dann wann das Product von zweyen Zahlen ein Quadrat seyn soll, als z. E. pq, *so wird erfordert, entweder dass* $p = rr$ *und* $q = ss$, *das ist dass ein Factor vor sich ein Quadrat sey, oder dass* $p = mrr$ *und* $q = mss$, *das ist, dass die Factores Quadrate mit einerley Zahl multiplicirt seyen, deswegen setze man* $x + y\sqrt{-c} = m(p + q\sqrt{-c})^2, \ldots$

Diese Behauptung, die Euler in den folgenden Abschnitten in Beweisen einsetzt, ist im allgemeinen falsch, wie das Beispiel für $c = 5$ zeigt. Hier gilt zum Beispiel

$$9 = 4 + 5 \cdot 1 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Links steht ein Quadrat von der Form $x^2 + 5y^2$ und rechts ein Produkt von zwei Zahlen, die unzerlegbar sind und deshalb kein Quadrat sein können.

Zu Zeiten von Gauss' *Commentatio secunda* konnte nun andererseits *eigentlich jedermann* wissen, dass die Eindeutigkeit der Faktorzerlegung in gewissen Fällen verletzt ist. Dazu hätte man nur allgemein bekannte Resultate innerhalb der komplexen Zahlen interpretieren müssen. Offenbar hat aber bis in die 40er Jahre des 19. Jahrhunderts kein Mathematiker diesen Schluss explizit gezogen.

Als konkretes Beispiel erwähnen wir Folgendes: Lagrange hatte in seiner Theorie über die quadratischen Formen (siehe [18], sowie die Darstellungen in [6] und [28]) festgestellt, dass es Zahlen gibt, deren Produkt durch die Form $x^2 + 5y^2$ darstellbar sind, die selbst aber keine solche Darstellung zulassen. Interpretiert mit Hilfe der komplexen Zahlen der Form $x + y\sqrt{-5}$ ergeben seine Resultate einen Widerspruch zur eindeutigen Faktorzerlegung im Bereich dieser Zahlen. Dies lässt sich wie folgt sehen. Nehmen wir an, die eindeutige Faktorzerlegung gelte, und es sei $m + n\sqrt{-5}$ ein unzerlegbares Element. Dann ist auch $m - n\sqrt{-5}$ ein unzerlegbares Element, und $(m + n\sqrt{-5})(m - n\sqrt{-5})$ ist die (eindeutig bestimmte) Faktorisierung der Norm $N = m^2 + 5n^2$. Es folgt, dass die Norm eines unzerlegbaren Elementes eine rationale Primzahl oder ein Quadrat einer rationalen Primzahl ist, denn jede andere Annahme würde zu einer anderen Faktorisierung von N im Bereich der Zahlen $a + b\sqrt{-5}$ Anlass geben. Es sei nun

$$x + \sqrt{-5}y = (x_1 + y_1\sqrt{-5}) \cdots (x_r + y_r\sqrt{-5})$$

die Faktorzerlegung von $x + y\sqrt{-5}$. Dann folgt für die Norm

$$x^2 + 5y^2 = \left(x_1^2 + 5y_1^2\right) \cdots \left(x_r^2 + 5y_r^2\right),$$

[3] Die berühmte *Vollständige Anleitung zur Algebra* hat der fast völlig erblindete Euler gegen Ende seines Lebens bekanntlich einem Schneidergesellen diktiert.

wobei jedes $x_j^2 + 5y_j^2$ eine rationale Primzahl oder ein Quadrat einer rationalen Primzahl ist. Wenn nun $x^2 + 5y^2$ eine quadratfreie rationale ganze Zahl ist, so ergibt sich nach dieser Überlegung eine Darstellung dieser Zahl als Produkt von unzerlegbaren Faktoren der Form $x_j^2 + 5y_j^2$. Wie die Theorie von Lagrange zeigt, gibt es dazu Gegenbeispiele. So ist die Zahl 6 von der Form $x^2 + 5y^2$, aber deren Faktoren 2 und 3 sind es nicht.

Die eindeutige Primfaktorzerlegung gilt nicht allgemein!

Die Entdeckung, dass es in Ringen ganz algebraischer Zahlen im allgemeinen keine eindeutige Primfaktorzerlegung gibt, wird gewöhnlich Eduard Kummer zugeschrieben.[4] In der Tat war er offenbar der erste, der diese Tatsache explizit in einer Veröffentlichung formulierte, nämlich in seiner Arbeit *De numeris complexis qui radicibus unitatis et numeris integris realibus constant*. Kummer war damals in Breslau tätig; die Arbeit erschien 1844 in der Gratulationsschrift der Universität in Breslau an die Universität in Königsberg zu deren 300-jährigen Jubiläum (siehe [14]). – Ihre Vorgeschichte und die damit verbundenen Begebenheiten sind so interessant, dass sich ein Verweilen lohnt. Dies wollen wir in der Tat tun; dabei folgen wir im wesentlichen der Chronologie der Ereignisse (siehe die einleitend zitierten Arbeiten von H.M. Edwards, O. Neumann, R. Bölling und F. Lemmermeyer).

Gemäss einer eigenhändigen Datierung stellte Kummer am 20. April 1844 ein Manuskript mit dem Titel *Ueber die complexen Primfactoren der Zahlen, und deren Anwendung in der Kreistheilung* fertig und reichte es bei der Preussischen Akademie der Wissenschaften ein.[5] Darin beschäftigte er sich mit der folgenden Frage, die wir der Einfachheit halber in der heutigen Sprache beschreiben. Es sei α eine primitive λ-te Einheitswurzel, $\alpha^\lambda = 1$, wo λ eine ungerade Primzahl ist. Kummer betrachtet komplexe Zahlen, die sich als ganzzahlige Linearkombinationen von α und seinen Potenzen, also als ganzzahlige Polynome in α schreiben lassen. Heute sprechen wir vom Ring $\mathbb{Z}[\alpha]$ der ganzen Zahlen im Körper $\mathbb{Q}(\alpha)$. Er stellt dann die Frage, wie eine Primzahl p der Form $m\lambda + 1$ in ein Produkt von Primelementen von $\mathbb{Z}[\alpha]$ zerfällt. In der *Commentatio secunda* hatte Gauss die analoge Frage in $\mathbb{Z}[i]$ behandelt, also den Fall $\lambda = 4$. Dabei ergaben sich überraschende Beziehungen zu den Reziprozitätsgesetzen[6] und zur Frage der Darstellung einer Primzahl als Summe von zwei Quadraten. In seiner Arbeit behauptete Kummer für die Primzahlen der Form $m\lambda + 1$ eine eindeutige Faktorisierung in $\lambda - 1$ Faktoren: er „bewies", dass sich jedes derartige p als Norm (im Sinne der Galoistheorie) eines Elementes $f(\alpha)$ in $\mathbb{Z}[\alpha]$ schreiben lässt. Es war zur Zeit der Arbeit von Kummer schon bekannt, dass nur (ungerade) Primzahlen p von der Form $m\lambda + 1$ in

[4] Siehe die in der Einleitung angegebenen Literaturstellen [12] und [10].

[5] Das Manuskript ist als Appendix I in der unter [7] zitierten Arbeit von 1977 von H.M. Edwards, S. 388–393 abgedruckt.

[6] Das berühmte quadratische Reziprozitätsgesetz, das auf Euler und Legendre zurückgeht, aber erstmals von Gauss in seinen *Disquisitiones arithmeticae* bewiesen wurde, beschäftigt sich mit der Frage, ob eine Primzahl q modulo einer gegebenene Primzahl p ein Quadrat sei. Das Reziprozitätsgesetz stellt eine enge und völlig überraschende Verbindung her zur Frage, ob umgekehrt p modulo q ein Quadrat sei.

$\mathbb{Z}[\alpha]$ in dieser Art zerfallen können.[7] Ferner hatte Jacobi kurz vorher für diese Primzahlen eine nichttriviale Zerfällung in ein Produkt von *zwei* Faktoren angeben können.

Die Arbeit wurde gemäss einer Notiz von Ch.G. Ehrenberg vom 13. Mai 1844 zur Publikation angenommen. Eine weitere Notiz von J.F. Encke vom 10. Juli 1844 besagt dann aber: *Zufolge einer späteren Zuschrift des Herrn Prof. Kummer ist die Abhandlung nicht gedruckt worden nach seinem Wunsche.* Zwischen den beiden Daten muss sich folglich etwas Schwerwiegendes abgespielt haben. Auf Grund des vorhandenen Archivmaterials lässt sich der Vorgang fast vollständig rekonstruieren: Am 17. Juni kehrt C.G. Jacobi von seinem Aufenthalt in Rom zurück, wo er einige Monate mit P.G. Lejeune Dirichlet und einigen Mitgliedern der Familie Mendelssohn verbracht hatte.[8] Er muss das Manuskript von Kummer kurz darauf in die Hand bekommen und auf einen darin enthaltenen gravierenden Fehler aufmerksam gemacht haben. In einem etwas später geschriebenen Brief von Jacobi an Dirichlet ist nämlich folgender Absatz zu finden:[9]

Kaum hatte ich bei meiner Rückkehr von Rom einen Fuss hierher gesetzt, als ich den Druck einer Abhandlung von Kummer in den Monatsberichten inhibieren musste. Der gute Junge hatte ohne Weitres die Zerfällbarkeit von $p = \lambda n + 1$ in complexe von den λt. [λ-ten] Einheitswurzel α abhängigen Zahlen angenommen und daraus allgemeine Sätze abgeleitet.[10]

[7] Wir beweisen dies wie folgt. Der Ring $\mathbb{Z}[\alpha]$ ist bekanntlich isomorph zu $\mathbb{Z}[x]/(1+x+\cdots+x^{\lambda-1})$. Es gelte für die Primzahl p,

$$p \equiv f(x)\,f(x^2)\cdots f(x^{\lambda-1}) \mod (1+x+\cdots+x^{\lambda-1}),$$

also $p = f(x)\,f(x^2)\cdots f(x^{\lambda-1}) + m(x)(1+x+\cdots+x^{\lambda-1})$ für ein gewisses ganzzahlige Polynom $m(x)$. Setzt man in dieser Gleichung $x = 1$, so erhält man $p = f(1)^{\lambda-1} + m(1)\lambda$. Modulo λ folgt dann mit Hilfe des kleinen Satzes von Fermat $p \equiv 1 \mod \lambda$. Dies war zu beweisen.

[8] Zum Italienaufenthalt von Dirichlet vergleiche man das Buch [11].

[9] Gemäss Datierung von Jacobi wurde der Brief am 4. Januar 1845 begonnen und am 13. Januar fertiggestellt. Er ist als Appendix II in der unter [7] zitierten Arbeit von 1977 von H.M. Edwards, S. 393–394 teilweise abgedruckt.

[10] Es gibt zu diesem Vorgang auch einen Brief von Gotthold Eisenstein an den Mathematiker Moritz Abraham Stern in Göttingen. (Moritz Abraham Stern (1807–1894) studierte Philologie in Heidelberg und Mathematik in Göttingen. Nach Promotion (1829) und Habilitation in Göttingen wurde er dort 1848 ausserordentlicher und 1859 ordentlicher Professor.) Der vollständige Brief ist zu finden in [8, Band II, S. 791–795]. Er ist teilweise abgedruckt in der unter [7] zitierten Arbeit von 1975 von H.M. Edwards, S. 233. – Der Brief ist nicht datiert, wurde aber – wie aus den Umständen zu schliessen ist – im Juli oder Anfang August 1844 geschrieben. *Prof. Kummer hat zum Glück seine schöne Theorie der complexen Zahlen noch bei Zeiten durch Encke von der Akademie zurücknehmen lassen; denn sie enthielt zuviel Revolutionsstoff, ich wäre z. B. rasend geworden; man kann durch dieselbe beweisen, dass zu jeder Determinante nur eine quadratische Form gehört und dergl. Unsinn mehr. [...] Gibt man den Satz zu, dass das Product zweier complexer Zahlen nicht anders durch eine Primzahl teilbar sein kann, als wenn wenigstens ein Factor durch die Primzahl teilbar ist, was ganz evident erscheint, so hat man die ganze Theorie auf einen Schlag; aber dieser Satz ist total falsch, und man muss also ganz neue Principien anwenden.* Es geht aus diesen Worten hervor, dass Eisenstein im Sommer 1844 bereits wusste, dass die eindeutige Faktorzerlegung im allgemeinen nicht gilt, und ferner, dass die Theorie der quadratischen Formen in sehr enger Beziehung steht zu den quadratischen Zahlkörpern. Man vergleiche dazu die Bemerkung zu Lagrange weiter oben.

Da das Manuskript von Kummer noch vorhanden ist, kann man die Sache nachprüfen.[11] Kummer scheint darin in der Tat an mehreren Stellen die *eindeutige* Primfaktorzerlegung im Ring $\mathbb{Z}[\alpha]$ stillschweigend vorausgesetzt zu haben. Entweder war er damals von deren Richtigkeit überzeugt oder – was wahrscheinlicher ist – er hat, ohne es zu bemerken, eine unmittelbare Folgerung daraus in seinen Beweisen verwendet. Wir werden weiter unten Gelegenheit haben, auf einen solche Stelle hinzuweisen.

Nach dem Rückzug seiner Arbeit hat Kummer offenbar rasch versucht, seinen Fehler zu verbessern. Die korrigierte Version seiner Arbeit ist – wie bereits bemerkt – noch im selben Jahr 1844 in der Gratulationsschrift der Universität in Breslau an die Universität in Königsberg zu deren 300-jährigen Jubiläum erschienen.[12] Kummer musste darin den Gültigkeitsbereich seiner früheren Behauptungen stark einschränken: Er betrachtete nun nur Primzahlen kleiner 1000 und untersuchte, wie sich für gegebenes λ diejenigen Primzahlen der Form $m\lambda+1$ verhalten. Er zeigte, dass die Zerfällung in $\lambda-1$ Faktoren für diese Primzahlen und für $\lambda = 5, 7, 11, 13, 17, 19$ gültig ist. Für $\lambda = 23$ hingegen bewies er, dass für gewisse Primzahlen (darunter 47) keine Zerfällung in 22, sondern nur eine in 11 Faktoren möglich ist.

In seiner Arbeit zieht Kummer daraus explizit den Schluss, dass im Ring $\mathbb{Z}[\alpha]$ mit $\alpha^{23} = 1$ die eindeutige Faktorzerlegung nicht allgemein gilt. Darauf gehen wir weiter unten noch genauer ein. Aber zuerst wenden wir uns dem Gegenbeispiel zur Zerfällung in 22 Faktoren zu. In unserer Darstellung machen wir dabei Gebrauch von der Galoistheorie, die uns heute natürlich als starkes Hilfsmittel zur Verfügung steht; zur Zeit Kummers existierte diese Theorie aber noch nicht, so dass damals der Beweis mit Hilfe von umfangreichen Rechnungen geführt werden musste.[13] Kummers ursprüngliche Behauptung besagt, dass für jede Primzahl p mit $p \equiv 1 \mod 23$ im Ring der 23-ten Einheitswurzeln ein Element $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{22}\alpha^{22}$ existiert, dessen Norm $N(f(\alpha)) = f(\alpha)\, f(\alpha^2) \cdots f(\alpha^{22})$ gleich p ist. Dies ist eine Faktorisierung von p in ein Produkt von 22 unzerlegbaren Elementen. Wir werden zeigen, dass diese Annahme für gewisse Primzahlen p zu einem Widerspruch führt.[14]

Die Galoisgruppe Γ der Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ ist die multiplikative Gruppe von $\mathbb{Z}/(23)$. Darin liefert -2 ein erzeugendes Element, es ist ein *primitives Element* des Körpers $\mathbb{F}_{23} = \mathbb{Z}/(23)$. Damit ist $4 \mod 23$ in dieser Gruppe ein Element der Ordung 11. Wir betrachten das durch $\alpha \mapsto \alpha^4$ definierte Element der Galoisgruppe Γ und die Summe ϑ_1 der unter der iterierten Anwendung dieses Elementes aus α entstehenden Potenzen von α. Es gilt:

$$\vartheta_1 = \alpha + \alpha^4 + \alpha^{-7} + \alpha^{-5} + \alpha^3 + \alpha^{-11} + \alpha^2 + \alpha^8 + \alpha^9 + \alpha^{-10} + \alpha^6.$$

[11] Dies hat Reinhard Bölling in [1] in ausserordentlich sorgfältiger Weise getan.

[12] Die Wahl, die Kummer hier für seine Veröffentlichung getroffen hat, steht wohl im Zusammenhang mit der Tatsache, dass Jacobi eng mit der Universität Königsberg verbunden war. Man darf dies als eine Referenz an Jacobi auffassen, der sich ebenfalls intensiv mit den von Kummer behandelten zahlentheoretischen Fragen befasste.

[13] H.M. Edwards vertritt in der unter [7] zitierten Arbeit von 1977 die Auffassung, dass das Gegenbeispiel von Jacobi stamme.

[14] Zum hier gegebenen Beweis vergleiche man die unter [7] zitierten Arbeiten von H.M. Edwards.

Für die Summe der aus α^{-1} entstehenden Potenzen erhalten wir

$$\vartheta_2 = \alpha^{-1} + \alpha^{-4} + \alpha^7 + \alpha^5 + \alpha^{-3} + \alpha^{11} + \alpha^{-2} + \alpha^{-8} + \alpha^{-9} + \alpha^{10} + \alpha^{-6}.$$

Offensichtlich sind ϑ_1 und ϑ_2 zueinander konjugierte komplexe Zahlen. Sowohl ϑ_1 wie ϑ_2 sind unter $\alpha \mapsto \alpha^4$ invariant, also unter einer Untergruppe vom Index zwei der Galoisgruppe Γ. Sie liegen deshalb in einem quadratischen Erweiterungskörper K von $\mathbb{Q}$, $K = \mathbb{Q}(\vartheta_1) = \mathbb{Q}(\vartheta_2)$. Das Minimalpolynom von ϑ_1 (bzw. ϑ_2), also

$$x^2 - (\vartheta_1 + \vartheta_2)x + \vartheta_1\vartheta_2,$$

lässt sich angeben. Es gilt $\vartheta_1 + \vartheta_2 = \alpha + \alpha^2 + \cdots + \alpha^{22} = -1$, weil α eine 23-te Einheitswurzel ist; eine direkte Rechnung zeigt ausserdem $\vartheta_1\vartheta_2 = 6$. Das Minimalpolynom lautet also[15]

$$x^2 + x + 6.$$

Es sei nun p eine Primzahl der Form $23 \cdot m + 1$. Es existiere gemäss der ursprünglichen Behauptung von Kummer ein Element $f(\alpha) \in \mathbb{Q}[\alpha]$, so dass dessen Norm p ist:

$$p = N(f(\alpha)) = f(\alpha)\, f(\alpha^2) \cdots f(\alpha^{22}).$$

Daraus wollen wir für gewisse Primzahlen einen Widerspruch herleiten. Zu diesem Zweck schreiben wir $N(f(\alpha))$ als Produkt von zwei Faktoren, indem wir einerseits die Faktoren zusammenfassen, die zu den in ϑ_1 vorkommenden Potenzen von α gehören, und andererseits diejenigen, die zu den in ϑ_2 vorkommenden Potenzen gehören. Da beide dieser Faktoren unter dem Galoisautomorphismus $\alpha \mapsto \alpha^4$ invariant bleiben, liegen sie beide im quadratischen Erweiterungskörper K. Wir können deshalb den ersten Faktor schreiben als $A + B\vartheta_1$ und den zweiten als $A + B\vartheta_2$, wobei A und B ganze Zahlen sind. Damit erhält man

$$N(f(\alpha)) = (A + B\vartheta_1)(A + B\vartheta_2) = A^2 - AB + 6B^2,$$

oder

$$4N(f(a)) = (2A - B)^2 + 23B^2.$$

Dies führt nun aber zum Beispiel für $p = 47$ zu einem Widerspruch. Es kann nämlich $4 \cdot 47 = 188$ nicht als ein Quadrat plus 23 mal ein Quadrat geschrieben werden! Damit kann die Primzahl 47, die kongruent 1 modulo 23 ist, entgegen der ursprünglichen Behauptung von Kummer in $\mathbb{Z}[\alpha]$ in der vorgegebenen Art *nicht* in 22 Faktoren zerfallen.

Kummer zieht aus diesem Resultat explizit den Schluss, dass es in Ringen von n-ten Einheitswurzeln eine eindeutige Faktorzerlegung im allgemeinen nicht gilt. Er sagt:

[15] Man vergleiche dazu das Vorgehen, das Gauss im Zusammenhang mit der Konstruierbarkeit des regelmässigen 17-Ecks bei der Faktorisierung des Polynoms $x^n - 1$ benützt hat.

Quia numeri primi reales formae $m\lambda+1$ non semper tanquam [sic] producta $\lambda-1$ factorum complexorum repraesentari possunt, multis etiam numerorum integrorum realium proprietatibus simplicibus numeri complexi carent. Pro iis generaliter non valet propositio fundamentalis ut quilibet numerus sit productum factorum complexorum simplicium, qui neglectis unitatibus complexis semper iidem sind, re enim vera nonnumquam idem numerus compositus pluribus modis diversis in factores simplices complexos diffindi potest.[16]

Kummer beweist hierzu, dass aus der Annahme der eindeutigen Faktorzerlegung zwingend folgt, dass im Ring $\mathbb{Z}[\alpha]$ mit $\alpha^\lambda = 1$ alle Primzahlen p der Form $m\lambda+1$ in der vorgegebenen Art in $\lambda-1$ unzerlegbare Faktoren zerfallen. Diesen Nachweis erbringt Kummer wie folgt:[17]

Man bezeichne mit ξ eine Zahl, welche die Gleichung

$$1+\xi+\xi^2+\cdots+\xi^{\lambda-1} \equiv 0 \mod p$$

erfüllt; man sieht leicht, dass es immer $\lambda-1$ solche Zahlen ξ mit $\xi < p$ gibt. Im Ring $\mathbb{Z}[\alpha]$, wo α eine λ-te Einheitswurzel ist, ist dann der Ausdruck

$$(\xi-\alpha)(\xi-\alpha^2)\cdots(\xi-\alpha^{\lambda-1})$$

durch p teilbar. *Unter der Voraussetzung der eindeutigen Primfaktorzerlegung* muss dann ein Primfaktor von p notwendigerweise einen der aufgeführten Faktoren teilen. (Diesen Beweisschritt verwendet Kummer explizit in seiner zurückgezogenen Arbeit!) Wegen der Transitivität der Galoisoperation können wir dabei annehmen, dass dies der erste Faktor $\xi-\alpha$ ist. Es sei $f(\alpha)$ dieser (Prim-)Faktor, dann ist offensichtlich $f(\alpha^2)$ ein gemeinsamer Faktor von p und $(\xi-\alpha^2)$, usw. Ferner sind die Faktoren $f(\alpha^\mu)$ und $f(\alpha^\nu)$ zu verschiedenen μ und ν verschieden, denn sonst müsste der Faktor $F = f(\alpha^\mu)$ gleichzeitig $\xi-\alpha^\mu$ und $\xi-\alpha^\nu$ teilen, also auch die Differenz $\alpha^\nu-\alpha^\mu$. Es müsste also F eine Potenz von α teilen oder eine Differenz $1-\alpha^\kappa$. Beides ist nicht möglich; die Norm einer Potenz von α ist stets 1, und für die Norm von $1-\alpha^\kappa$ erhält man

$$(1-\alpha)(1-\alpha^2)\cdots(1-\alpha^{\lambda-1}) = \lambda.$$

Der Faktor F müsste deshalb die Norm 1 – in diesem Fall ist F eine Einheit – oder λ besitzen. Da p von der Form $m\lambda+1$ ist, kann somit F kein Teiler von p sein, denn seine Norm müsste ja p teilen. Wir erhalten somit $p = f(\alpha)\cdot f(\alpha^2)\cdots f(\alpha^{\lambda-1})\cdot M$. Da die Norm von $f(\alpha)$ eine reelle Zahl sein muss, die verschieden von 1 ist, folgt daraus $M = 1$. Damit besitzt p eine Faktorisierung in $\lambda-1$ (Prim-)Faktoren.[18]

[16] Eine deutsche Übersetzung lautet etwa so: *Da die reellen Primzahlen der Form $m\lambda+1$ nicht immer in dieser Weise als Produkt von $\lambda-1$ Faktoren dargestellt werden können, so besitzen auch die komplexen Zahlen [i. e. die komplexen Elemente von $\mathbb{Z}[\alpha]$] viele der einfachen Eigenschaften der ganzen Zahlen nicht. Für sie gilt im allgemeinen der fundamentale Satz nicht, dass jede Zahl Produkt einfacher komplexer Zahlen [i. e. unzerlegbarer Zahlen] ist, die bis auf Einheiten immer die gleichen sind, in der Tat kann es nämlich vorkommen, dass die gleiche zusammengesetzte Zahl auf mehrere verschiedene Arten in einfache komplexe Faktoren zerlegt werden kann.*

[17] Wir stützen uns hier auf einen Abschnitt der zurückgezogenen Arbeit von Kummer. Wie oben machen wir allerdings wieder von elementaren Resultaten der Galoistheorie Gebrauch.

[18] Wie oben (siehe Fussnote 7) bereits bemerkt, folgt aus der Tatsache, dass die reelle Primzahl p, $p \neq \lambda$, in $\mathbb{Z}[\alpha]$ in $\lambda-1$ (Prim-)Faktoren zerfällt, stets, dass p von der Form $m\lambda+1$ ist.

Kummer fährt in seiner Arbeit dann mit folgender (berühmt gewordenen) Bemerkung fort:

Maxime dolendum videtur, quod haec numerorum realium virtus, ut in factores primis dissolvi possint qui pro eodem numero semper iidem sint, non eadem est numerorum complexorum, quae si esset tota haec doctrina, quae magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci posset.[19]

Trotz der Schwierigkeiten, denen Kummer bei der Faktorisierung in Ringen von Einheitswurzeln begegnete, gab er seine Bestrebungen nicht auf, Licht in diesen Fragenkomplex zu bringen. Im Jahre 1847 veröffentlichte er seine Arbeit *Zur Theorie der complexen Zahlen* (siehe [15]), in der er eine – in einem gewissen Sinn – vollständige Lösung präsentiert. Sie basiert auf sogenannten *idealen Zahlen*. Es sind dies neue Objekte, die zwar in die Betrachtungen einbezogen werden, die aber im eigentlichen Sinn nicht existieren, sondern nur durch ihr Verhalten gegenüber den anderen Zahlen definiert sind. Kummer bemerkt hierzu: *Der Einführung solcher idealen komplexen Zahlen liegt derselbe einfache Gedanke zu Grunde, wie der Einführung der imaginären Formeln in die Algebra und Analysis; namentlich bei der Zerfällung der ganzen rationalen Functionen in ihre einfachsten Factoren, die linearen.*[20] Es gelang Kummer auf diese Weise, in Ringen von Einheitswurzeln die eindeutige (Prim-)Faktorzerlegung zu „retten“, indem jedes Element nun bis auf Einheiten in eindeutiger Weise als Produkt von echten bzw. idealen (Prim-)Faktoren geschrieben werden kann.

In dieser Arbeit bemerkt Kummer auch, dass man seine Theorie sinngemäss auf quadratische Körper anwenden könne. Damit ergebe sich eine zur Gaussschen Theorie der quadratischen Formen äquivalente Theorie. Kummer machte dazu keine weiteren Angaben, und er kam meines Wissens auf diesen Punkt später nie zurück. Der Grund dürfte in den unerwarteten Schwierigkeiten zu suchen sein, die bei der Ausarbeitung dieses Programms auftreten. Diese hat erst Richard Dedekind überwinden können. Seine Theorie wurde in den Supplementen der zweiten Auflage von 1871 der *Vorlesungen über Zahlentheorie* von Dirichlet erstmals veröffentlicht.[21] Darin sind zwei wesentliche Neuerungen eingeführt: Zum einen ersetzt Dedekind in seinen Betrachtungen die Kummerschen *idealen Zahlen* durch *Ideale*. Zum zweiten erkannte er – wohl als erster – die wesentliche Rolle, welche den *ganz algebraischen Zahlen* in dieser Frage zukommt.[22] Sein Hauptresultat lautet, dass in Ringen ganz algebraischer Zahlen stets die *eindeutige Primidealzerlegung* gilt. Für Kreisteilungskörper ist seine

[19] Eine deutsche Übersetzung lautet etwa so: *Es muss sehr bedauert werden, dass diese Eigenschaft der reellen Zahlen [i. e. der rationalen ganzen Zahlen], in Primfaktoren zerlegbar zu sein, die für eine gegebene Zahl immer dieselben sind, für komplexe Zahlen [i. e. Elemente von $\mathbb{Z}[\alpha]$] nicht gilt. Wäre sie gültig, so wäre diese ganze Theorie, die so grosse Schwierigkeiten verursacht, leicht durchzuführen und zu einem Ende zu bringen.*

[20] Analoges liesse sich auch von der Einführung von unendlich fernen geometrischen Objekten in der projektiven Geometrie sagen.

[21] In den nachfolgenden Auflagen der Dirichlet's *Vorlesungen über Zahlentheorie* von 1879 und 1894 hat Dedekind seine Theorie weiter entwickelt. – Siehe dazu auch das Büchlein von Richard Dedekind: *Sur la théorie des nombres entiers algébriques*, 1877; darin geht Dedekind auf die Schwierigkeiten, die bei quadratischen Körpern auftreten, in detaillierter Weise ein.

[22] Siehe dazu aber die neueren Untersuchungen von Franz Lemmermeyer [21]. Lemmermeyer weist in diesem interessanten Artikel u. a. auf bisher wenig beachtete Spuren hin, welche in Arbeiten (und Vor-

Theorie äquivalent zur Kummerschen Theorie der idealen Zahlen, für allgemeinere, etwa quadratische Zahlkörper, ist sie wesentlich transparenter und leistungsfähiger. In der weiteren Entwicklung der Mathematik hat sich Dedekinds Standpunkt vollständig durchgesetzt.

Beziehungen zur Fermat-Vermutung

Die Fortsetzung unserer Geschichte handelt von der Vermutung von Fermat, also der Vermutung, dass die Gleichung $x^n + y^n = z^n$ für $n \geq 3$ keine nichttrivialen ganzzahligen Lösungen besitzt. Diese Vermutung wurde von Fermat, Euler, Dirichlet, Legendre für einzelne kleine Primzahlexponenten n bewiesen, wobei mit wachsendem n die Beweise zunehmend komplizierter und umfangreicher wurden. Unmittelbar vor der Zeit, in der sich unsere Geschichte abspielt, gelang dem französischen Mathematiker Gabriel Lamé ein weiterer grosser Schritt, als er im Jahre 1839 in einer komplizierten Arbeit einen Beweis der Fermat-Vermutung für den Exponenten $n = 7$ liefern konnte (siehe [19]).

Am 1. März 1847, also im gleichen Jahr, in dem Kummer seine idealen Zahlen einführte, kündigte Lamé an der Versammlung der Akademie in Paris einen Beweis für den allgemeinen Fall an (siehe [20]). Seine wesentliche Beweisidee bestand darin, n-te Einheitswurzeln zu benützen. Wenn wir für die ungerade Primzahl n

$$X^n + 1 = (X + 1)(X + r) \cdots (X + r^{n-1})$$

schreiben – die Elemente $-1, -r, \ldots, -r^{n-1}$ sind also die n-ten Einheitswurzeln –, so lässt sich mit $X = x/y$ die linke Seite $x^n + y^n$ in die Form

$$(x + y)(x + ry) \cdots (x + r^{n-1}y)$$

bringen. Die weiteren Überlegungen von Lamé, auf die wir hier nicht eingehen wollen, verwenden dann, ohne dass dies ausdrücklich erwähnt würde, die eindeutige Primfaktorzerlegung im Ring der n-ten Einheitswurzeln. An der Sitzung der Akademie nahm Joseph Liouville teil, der nach der Ankündigung Zweifel am Beweis von Lamé anbrachte. Er wies zuerst darauf hin, dass die Verwendung von Einheitswurzeln im Zusammenhang mit der Fermatschen Vermutung schon bei Lagrange zu finden sei, und dass sich auch Gauss und Jacobi mit den komplexen Zahlen der hier auftretenden Form (Einheitswurzeln) beschäftigt haben. Zweitens machte er darauf aufmerksam, dass die Verwendung der eindeutigen Primfaktorzerlegung in diesen Bereichen, eine Rechtfertigung benötige, die Lamé nicht geliefert habe. Auch Cauchy ergriff nach Liouville das Wort: Er habe selber seit einigen Monaten eine Idee, wie die Vermutung von Fermat bewiesen werden könne, aber er habe bis jetzt noch keine Zeit gehabt, sie weiter zu verfolgen. Es dürfte klar, sein, dass Cauchy hier versuchte, einen Teil der Lorbeeren für den Beweis der Fermatschen Vermutung zu erhaschen, wenn es sich denn herausstellen sollte, dass Lamés Beweis korrekt war. Es folgte eine

lesungen) von Jacobi und Eisenstein zu finden sind und die Entwicklung der Kummerschen Theorie und deren Verallgemeinerung betreffen.

Zeit, in der in Paris hektisch versucht wurde, die Lücke im Zusammenhang mit der eindeutigen Primfaktorzerlegung zu schliessen.

So hat Pierre Laurent Wantzel (siehe [27]) noch im Laufe desselben Monats März der Akademie eine Arbeit vorgelegt, in der er für den Ring der *dritten* Einheitswurzeln einen Euklidischen Algorithmus beschreibt. Daraus ergibt sich – wie damals schon bekannt war – die eindeutige Primfaktorzerlegung sofort. Am Schluss seiner Arbeit sagt er: *On voit facilement que le même mode de démonstration s'applique aux nombres complex de forme plus compliquée qui dépendent des racines de* $r^n = 1$ *pour n quelconque.*

Es war Cauchy der in der darauffolgenden Sitzung der Akademie vom 22. März darauf aufmerksam machte, dass die direkte Verallgemeinerung auf Zahlen $n > 3$ nicht möglich ist, und er gibt für $n = 7$ ein Gegenbeispiel zu einer Überlegung von Wantzel an (siehe [3]).

Im Notizbuch von Liouville ist ferner eine offenbar um den 13. März 1847 herum eingetragene Notiz zu finden:

$$13 \cdot 13 = 169 = (4 + 3\sqrt{-17})(4 - 3\sqrt{-17}).$$

Liouville hatte also zu dieser Zeit ein explizites Gegenbeispiel zur eindeutigen (Prim-) Faktorzerlegung im Bereich der Zahlen $\mathbb{Z}(\sqrt{-17})$ zur Hand.

Im Mai 1847 erhielt Liouville dann einen Brief von Kummer. Offenbar war Dirichlet auf die Vorgänge an der Akademie in Paris aufmerksam geworden, möglicherweise durch eine Mitteilung von Liouville, mit dem Dirichlet befreundet war, und hat dann Kummer informiert. Dirichlet und Kummer kannten sich persönlich sehr gut, waren doch ihre Ehefrauen Cousinen.[23] In seinem Brief vom 28. April 1847 an Liouville sagte Kummer (siehe [16]):

Quant à la proposition élémentaire pour ces nombres complexes [i. e. Elemente von $\mathbb{Z}[\alpha]$*], qu'un nombre complexe composé ne peut être décomposé en facteurs premiers que d'une seule manière, que vous regrettez très-justement dans cette démonstration [von Lamé], défectueuse en outre en quelques autres points, je puis vous assurer qu'elle n'a pas lieu généralement [...]*

In der Tat hatte Kummer diese Tatsache – wie wir gesehen haben – schon 1844 ausdrücklich festgehalten. Es ist wahr, dass Kummers Arbeit nicht in einer wissenschaftlichen Zeitschrift, sondern „nur" in der Gratulationsschrift der Universität Breslau an die Universität Königsberg veröffentlicht wurde, aber die Unkenntnis im Bereich der *Académie Française* und bei so berühmten Leuten wie Liouville und Cauchy muss doch erstaunen![24] Dies gilt umso mehr, als Kummer im Jahre 1846 auch in den Monatsberichten der Akademie in Berlin eine entsprechende Notiz veröffentlicht hatte (siehe [15]). Liouville erkannte allerdings nun die Leistung

[23] Dirichlet war bekanntlich verheiratet mit Rebekka Mendelssohn, der Schwester von Felix Mendelssohn und Tochter von Abraham Mendelssohn. Kummer war mit Ottilie Mendelssohn verheiratet, der Tochter von Nathan Mendelssohn, der ein Bruder von Abraham Mendelssohn war. Ottilie starb 1848 an Nervenfieber; mit diesem Wort bezeichnete man damals gewöhnlich die Erkrankung an Typhus.

[24] Heutzutage werden Personen vom Berühmtheitsgrad von Cauchy und Liouville beauftragt, Evaluationen von Fachbereichen an Universitäten durchzuführen und Gutachten zu schreiben, die über die Karriere der Begutachteten entscheiden. Kann man darauf vertrauen, dass der Kenntnisstand dieser Personen heute besser ist als damals bei Cauchy und Liouville?

von Kummer sofort: Er verlas in der nächsten Sitzung der Akademie den Brief von Kummer vom 28. April 1847 und veröffentlichte ihn umgehend auch in „seinem" Journal (siehe [16]). Der Veröffentlichung stellte er die folgende Bemerkung voran, ein veritables Meisterstück der Diplomatie:[25]

Note de M. Liouville. – Le Mémoire de M. Kummer, dont il est d'abord question dans cette Lettre, et qui porte la date de 1844, est écrit en latin, sous ce titre: De numeris complexis qui radicibus unitatis et numeris integris realibus constant. *Celui de M. Kronecker, qui y fait suite et qui est intitulé:* De unitatibus complexis, *traite spécialement des diviseurs complexes du nombre* 1*; il a paru en 1845, et l'auteur annonce qu'il reprendra la question avec plus de détails dans le Journal de M. Crelle. Le Mémoire de M. Kummer offrant beaucoup d'intérêt et ne paraissant pas avoir été jusqu'ici connu en France, nous le donnerons en entier dans un prochain cahier, à la suite d'un travail de M. Lamé, sur le même sujet, qui est imprimé depuis quelques temps déja. On devra consulter, en outre, le Journal de M. Crelle, les Comptes rendus de l'Académie de Berlin, et enfin ceux de notre Académie des Sciences qui contiennent des recherches étendues de M. Cauchy. Nous n'avons pas à examiner ici en quoi les auteurs que nous citons s'accordent ou diffèrent, ni quels sont les droits de chacun à l'antériorité de telle ou telle découverte. C'est au temps à fixer la valeur de leurs travaux et à mettre toute chose à sa place.*

Ein Abdruck der vollständigen Arbeit von Kummer aus dem Jahre 1844 erschien in der Tat unmittelbar darauf in Liouville's Journal (siehe [14]). Man könnte sich denken, dass Lamé auf Grund dieser Sachlage auf die Publikation seiner eigenen Arbeit verzichtet hätte. Dem ist aber nicht so: die Arbeit von Kummer, die zeigt, dass die eindeutige Primfaktorzerlegung im Bereich der Ringe von Einheitswurzeln allgemein nicht gilt, und diejenige von Lamé, welche von dieser eindeutigen Primfaktorzerlegung für den Beweis der Fermatschen Vermutung implizit Gebrauch macht, sind im gleichen Heft des Liouvilleschen Journals abgedruckt!

Auch die Reaktion von Cauchy ist bemerkenswert. In der nachfolgenden Sitzung der Akademie liess er verlauten (siehe [4]):

Dans la dernière séance, M. Liouville a parlé de travaux de M. Kummer, relatifs aux polynômes complexes. Le peu qu'il en a dit me persuade que les conclusions auxquelles M. Kummer est arrivé sont, au moins en partie, celles auxquelles je me trouve conduit moi-même par les considérations précédentes. Si M. Kummer a fait faire à la question quelques pas de plus, si même il était parvenu à lever tous les obstacles, j'aupplaudirais le premier au succès de ses efforts; car ce que nous devons surtout désirer, c'est que les travaux de tous les amis de la science concourent à faire connaître et à propager la vérité.

Cauchy hat in der Folge mehrfach versprochen, seine eigenen Überlegungen bekannt zu machen und zu denjenigen von Kummer in Beziehung zu setzen. Dies hat er nicht in dem Ausmass getan, das man von einem Mathematiker vom Range Cauchys erwarten würde. Er kam zwar in der Folge in zahlreichen grösseren und kleineren Abhandlungen, die er der Akademie einreichte, auf die Sache zurück, blieb aber weit von den umfassenden Resultaten von Kummer entfernt. Immer-

[25] Edwards sagt in seinen Arbeiten (siehe [7]), dass diese Bemerkung bei der Präsentation des Briefes von Kummer vor der Akademie gemacht worden sei. Dies wird durch die Unterlagen nicht gestützt.

hin hat er in einer kurz darauf der Akademie präsentierten Arbeit (siehe [5]) das oben beschriebene Beispiel von Kummer dargestellt, das zeigt, dass es im Ring $\mathbb{Z}[\alpha]$, α eine 23-te Einheitswurzel keine eindeutige (Prim-)Faktorzerlegung gibt.

Wohl motiviert durch die „Misstritte" der Pariser Akademie, verzeichnete Kummer im Sommer 1847 auch in der Frage der Fermatschen Vermutung einen grossen Fortschritt. Er zeigte, dass die Vermutung für sogenannte *reguläre* Primzahlen richtig ist.[26] Eine Primzahl p heisst dabei regulär, wenn die Klassenzahl des Ringes $\mathbb{Z}[\alpha]$, α eine p-te Einheitswurzel, nicht durch p teilbar ist.[27] Kummer konnte anschliessend von vielen Primzahlen zeigen, dass sie regulär sind; von der Primzahl 37 zeigte er, dass sie irregulär ist. Dieses Resultat über die Fermatsche Vermutung blieb für mehr als ein Jahrhundert das umfassendste. Erst der *volle* Beweis der Vermutung durch von Andrew Wiles und Richard Taylor im Jahre 1995 (siehe [29] und [26]) ging wesentlich über die Erkenntnisse von Kummer hinaus.[28]

Epilog

Die Geschichte hat einen einigermassen versöhnlichen Schlusspunkt: Im Jahre 1857 hat die französische Akademie einen einige Jahre vorher ausgeschriebenen Preis für den Beweis der Fermatschen Vermutung Ernst Eduard Kummer zuerkannt. Das Gutachten des Preiskomitees, dem sowohl Cauchy wie Lamé angehörten, stammt aus der Feder von Cauchy.[29] Der Entscheid des Komitees scheint aber nicht ohne Schwierigkeiten zustande gekommen sein. In einem Brief[30] an Dirichlet vom 27. Januar 1857 schreibt Liouville: *C'est M. Cauchy, qui a fait le rapport, bien qu'opposé, au fond, à la proposition contre laquelle il n'a d'abord présenté que des raisons fort mauvaises; [...]* Cauchy habe allerdings auch auf einen Punkt in Kummers Arbeit von 1847 (die Liouville 1851 ebenfalls in „sein" Journal aufgenommen hatte) hingewiesen, der bis jetzt nicht habe geklärt werden können. Liouville bat deshalb Dirichlet um Hilfe. Dieser antwortete am 1. Februar, dass die Lücke von Richard Dedekind schon vor einiger Zeit bemerkt und von diesem habe geschlossen werden können. Ferner teilte er Liouville mit, dass Kummer vor kurzem eine Arbeit fertiggestellt habe, in der er die-

[26] Die entsprechende Arbeit von Kummer (siehe [17]) datiert vom 16. September 1847.

[27] Dies entspricht nicht der ursprünglichen Definition von Kummer, sondern orientiert sich an der heute üblichen Terminologie. Hat $\mathbb{Z}[\alpha]$ die Klassenzahl 1, so bedeutet dies bekanntlich, dass darin die eindeutige Primfaktorzerlegung gilt. Die zugehörige Primzahl ist gemäss Definition regulär.

[28] Für eine Darstellung des Beweisganges vergleiche man auch die beiden Beiträge von J. Kramer [13].

[29] In C. R. Acad. Sci. Paris 54 (1857) ist unter 158. Sitzung vom 2. Februar festgehalten: *Rapport sur le concours pour le grand prix de sciences mathématiques. Déja remis au concours pour 1853 et prorogé jusqu'en 1856. La commission, n'ayant trouvé parmi les pièces adressées au concours, aucun travail qui lui ait paru digne du prix, a proposé à l'Académie de l'accorder à M. Kummer, pour ses belles recherches sur les nombres complexes composés de racines de l'unité et de nombres entiers. L'Académie a adopté cette proposition.* – Auf S. 573 desselben Bandes folgt die Notiz: *M. Kummer remercie l'Académie qui lui a décerné un des grands prix de sciences mathématiques de 1856, pour ses Recherches sur les nombres complexes composés de racines de l'unité et de nombres entiers.*

[30] Siehe dazu die in der unter [7] zitierte Arbeit von H.M. Edwards von 1975. Dort ist auf S. 231–232 der Briefentwurf von Liouville abgedruckt.

sen Punkt vollständig aufkläre.[31] Der Preis der Akademie wurde allerdings schon am 2. Februar vergeben, also vor dem Erscheinen der Ergänzung von Kummer und sehr wahrscheinlich auch vor Eintreffen der Antwort von Dirichlet bei Liouville.

Literatur

1. Bölling, R.: Kummer vor der Erfindung der „idealen complexen Zahlen“: Das Jahr 1844. Acta Hist. Leopold. **27**, 145–157 (1997)
2. Bölling, R.: From reciprocity laws to ideal numbers: An (un)known manuscript by E.E. Kummer. In: Goldstein, C., Schappacher, N., Schwermer, J. (eds.) The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithemticae, pp. 271–290. Springer, Berlin (2007)
3. Cauchy, A.: Mémoire sur de nouvelle formules relative à la théorie des polynômes radicaux, et sur le dernier théorème de Fermat. C. R. Acad. Sci., Paris **24**, 469–481 (1847)
4. Cauchy, A.: C. R. Acad. Sci., Paris **24**, 887 (1847)
5. Cauchy, A.: Sur la décomposition d'un nombre entier en facteurs radicaux. C. R. Acad. Sci., Paris **24**, 1022–1030 (1847)
6. Cox, D.: Primes of the Form $x^2 + ny^2$, Class Field Theory and Complex Multiplication. Wiley, New York (1997)
7. Edwards, H.M.: The background of Kummer's proof of Fermat's last theorem for regular primes. Arch. Hist. Exact Sci. **14**, 219–236 (1975) (Postscript to: The background of Kummer's proof .... Arch. Hist. Exact Sci. **17**, 381–393 (1977))
8. Eisenstein, G.: Mathematische Werke. Chelsea Publ. Co., New York (1975)
9. Gauss, C.F.: Theoria Residuorum Biquadraticorum, Commentatio Secunda. Werke II, S. 93–148; zugehörige Selbstanzeige, Werke II, S. 169–178
10. Hensel, K.: Kummer und sein Lebenswerk. Gedächtnisrede auf Ernst Eduard Kummer. In: Festschrift zur Feier des 100. Geburtstages Eduard Kummers mit Briefen an seine Mutter und an Leopold Kronecker. Teubner (1910); Kummers Ges. Abh., Band I, S. 31–133. Springer, Berlin (1975)
11. Hensel, S.: Die Familie Mendelssohn, 1729–1847, nach Briefen und Tagebüchern herausgegeben von Sebastian Hensel. Erstmals erschienen 1879. Insel Taschenbuch 1671. Frankfurt a. Main (1995)
12. Hilbert, D.: Mathematische Probleme. Vortrag am Intern. Mathematikerkongress, Paris 1900; in erweiterter Fassung abgedruckt in Ges. Abh. Band III, S. 290–329
13. Kramer, J.: Über den Beweis der Fermat'schen Vermutung I, II. Elem. Math. **50**, 11–25 (1995) (Elem. Math. **53**, 45–60 (1998))
14. Kummer, E.E.: De numeris complexis qui radicibus unitatis et numeris integris realibus constant. J. Math. Pures Appl. **12**, 185–212 (1847) (siehe auch Kummers Ges. Abh. Band I, S. 165–192. Springer, Berlin (1975))

[31] H.M. Edwards vertritt in seiner unter [7] zitierten Arbeit von 1975 die Meinung, dass es sich bei dem von Cauchy und Liouville erwähnten Punkt um eine gravierende Lücke in der Arbeit von Kummer handle, der die Einführung der idealen Zahlen in grundlegender Weise betreffe. Wie aber O. Neumann in [25] nachweist, lässt sich die Lücke durch einen Hinweis auf die schon 1839 erschienene Arbeit von Theodor Schönemann *Theorie der symmetrischen Functionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen, nebst einigen Anwendungen derselben*, J. Reine Angew. Math. 19 (1839), 231–243, 289–308 ohne weiteres schliessen. Diese Arbeit muss Kummer wohlbekannt gewesen sein, denn sein Schüler Leopold Kronecker hatte in seiner Dissertation von 1845 *De unitatibus complexis*, Universität Berlin (1845), §2; siehe Kronecker Werke, Bd. 1, S. 5–73, darauf verwiesen. Auch Eisenstein hatte in einer Arbeit von 1850 *Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, J. Reine Angew. Math. 39 (1850) 160–179, 224–287; Math. Werke II (1975) 536–555, 556–619 auf Schönemanns Arbeit hingewiesen. Interessant ist allerdings, dass Dirichlet darüber Liouville nichts mitteilte! – Bei der von Dirichlet erwähnten Arbeit von Kummer handelt es sich um *Über die Gaussischen Perioden der Kreistheilung entsprechenden Congruenzwurzeln*, J. Reine Angew. Math. 53 (1857), 142–148. Darin findet sich ein vollständiger und neuer Beweis für das in Frage stehende Resultat.

15. Kummer, E.E.: Zur Theorie der complexen Zahlen. Monatsber. Akad. Wiss. Berlin, 87–96 (1846); auch in: J. Reine Angew. Math. **35**, 319–326 (1847); Kummers Ges. Abh. Band I. S. 203–210. Springer, Berlin (1975)
16. Kummer, E.E.: Extrait d'une lettre de M. Kummer à M. Liouville. C. R. Acad. Sci., Paris **24**, 899–900 (1847) (Siehe auch J. Math. Pures Appl. **12**, 136 (1847); Kummers Ges. Abh. Band I, S. 298. Springer, Berlin (1975))
17. Kummer, E.E.: Beweis des Fermatschen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl von Primzahlen λ. Monatsber. Akad. Wiss. Berlin 132–139 (1847)
18. Lagrange, J.L.: Recherches d'arithmétiques. Nouv. Mém. de l'acad. sci. Berlin, pp. 256 ff. (1773); Oeuvres, vol. 3, pp. 695–795
19. Lamé, G.: C. R. Acad. Sci., Paris **9**, 45–46 (1839); J. Math. Pures Appl. **5**, 195–211 (1840)
20. Lamé, G.: Démonstration générale du théorème de Fermat. C. R. Acad. Sci., Paris **24**, 310–315 (1847)
21. Lemmermeyer, F.: Jacobi and Kummer's Ideal Numbers. Preprint (2008)
22. Neumann, O.: Bemerkungen aus heutiger Sicht über Gauss' Beiträge zur Zahlentheorie, Algebra und Funktionentheorie. Schriftenreihe für Gesch. Naturwiss. Technik, Med. **16**(2), 22–39 (1979)
23. Neumann, O.: Zur Genesis der algebraischen Zahlentheorie, 2. Teil. Schriftenreihe für Gesch. Naturwiss. Technik, Med. **17**(1), 32–48 (1980)
24. Neumann, O.: Zur Genesis der algebraischen Zahlentheorie, 3. Teil. Naturwiss. Technik, Med. **17**(2), 38–58 (1980) (Die drei Teile [22–24] bilden einen zusammenhängenden Beitrag, auch wenn der erste Teil einen aus dem Rahmen fallenden Titel trägt.)
25. Neumann, O.: Über die Anstösse zu Kummers Schöpfung der „Idealen Complexen Zahlen". In: Dauben, J.W. (ed.) Mathematical Perspectives, pp. 179–199. Academic Press, London (1981)
26. Tayor, R., Wiles, A.: Ringtheoretic properties of certain Hecke algebras. Ann. Math. **141**, 553–572 (1995)
27. Wantzel, P.L.: Note sur la théorie des nombres complexes. C. R. Acad. Sci., Paris **24**, 430–434 (1847)
28. Weil, A.: Two lectures on number theory, past and present. Enseign. Math. **XX**, 87–110 (1974)
29. Wiles, A.: Modular elliptic curves and Fermat's last theorem. Ann. Math. **141**, 443–551 (1995)