Ramsauer Nina

Fermats letzter Satz

Schriftliche Hausarbeit zur Zulassung zur Ersten Saatsprüfung
für das Lehramt an Realschulen nach LPO I

Universität Regensburg
Mathematik

Betreuer: Prof. Dr. Rolf Waldi
Abgabetermin: 16.12.2004

Inhaltsverzeichnis

Einleitung

Sobald man sich mit der Geschichte der Mathematik befasst, stößt man unweigerlich auf Fermats letzten Satz. Dieser stammt aus dem 17. Jahrhundert, berührt alle großen Themen der Zahlentheorie und reicht weit in die Geschichte der Mathematik zurück. Da es sich bei Fermats letztem Satz um eine Abwandlung des Satzes des Pythagoras handelt, liegt dessen Ursprung im sechsten Jahrhundert vor Christus bei Pythagoras. Fermat hat damit ein Problem geschaffen, an dem sich viele Mathematiker mehr oder weniger erfolgreich versucht haben.[1]

An dieser Stellen eine kleine Zusammenstellung der Mathematiker, die Erfolge bei der Lösung des Problems verbuchen konnten:

Fermat (1601-1665) Vermutlich um 1637 Problemstellung; Beweis für $n = 4$, und später andeutungsweise für $n = 3$.

Euler (1707-1783) $n = 3$: Beweis unvollständig

Gauß (1777-1850) $n = 3$: vollständiger Beweis

Dirichlet (1805-1859) $n = 5$: 1825 in der Akademie Paris; Dirichlets Beweis war zunächst unvollständig; nach Kritik durch Legendre gab er einen Ansatz zur Vervollständigung; dieser wurde 1828 in Crelles Journal ausführlich publiziert.

Dirichlet $n = 14$: 1832 in Crelles Journal

Lamé (1795-1870) $n = 7$: 1839 in Liouvilles Journal

Lamé n beliebig: 1841 in Liouvilles Journal (Beweis erschien unvollständig; Kritik durch Liouville)

Kummer (1810-1893) 1844 in der Festschrift für das Königsberger Universitätsjubiläum: Die Lücke im Beweis bei Lamé

[1] vgl. [4], S.19

kann nicht geschlossen werden! Der Beweisversuch von Lamé ist also endgültig als falsch zu bewerten.

Kummers monumentales Theorem: 1850 in Crelles Journal: Beweis für alle Primzahlexponenten $n = p$, bei denen p eine sogenannte „reguläre Primzahl“ ist.[2]

Den letztendlich größten Erfolg bei der Problemlösung leistete jedoch 1995 Andrew Wiles, indem es ihm gelang Fermats letzten Satz vollständig zu beweisen.

Die Arbeit ist in drei große Kapitel unterteilt. Zu Beginn der Arbeit (Kapitel I) wird ein Einblick in den geschichtlichen Rahmen des Fermatschen Problems gewährt. Es werden Informationen über die Entstehung, über die verschiedenen Ansätze zur Lösung und schließlich über die endgültige Lösung des Problems durch den Mathematiker Andrew Wiles gegeben.[3]

Die Grundlagen für die Beweise, die in Kapitel III behandelt werden, sind in Kapitel II zusammengefasst. Somit ist dem Leser das nötige Material zum Erarbeiten und Verstehen der Beweise gegeben. Der Inhalt dieses Kapitels beruht auf der Vorlesung „Elemente der Zahlentheorie und Aufbau des Zahlensystems“ von Prof. Dr. Rolf Waldi (vgl. [5]).

In Kapitel III wird zuerst der Fall $n = 2$ untersucht. Es wird gezeigt, dass die Gleichung $X^2 + Y^2 = Z^2$ unendlich viele positive ganzzahlige Lösungen mit teilerfremden x, y und z hat. Nach dem Satz des Pythagoras bedeutet dies bekanntlich, dass es unendlich viele nicht zueinander ähnliche rechtwinklige Dreiecke mit ganzzahligen Seitenlängen gibt. Die Formel $a^2 + b^2 = c^2$ ist wohl diejenige Formel, die jedem aus seiner Schulzeit in Erinnerung bleibt, auch wenn er sonst nicht mehr viel mit der Mathematik zu tun hat. Der Satz des Pythagoras ist also ein Teil des Problems, um das es in dieser Arbeit geht.
Im Anschluß daran wird Fermats letzter Satz für die Fälle $n = 3$ und $n = 4$ bewiesen. Fermat selbst erbrachte bereits den Beweis für $n = 4$. Den Beweis für den Fall $n = 3$, konnte er zwar andeuten, endgültig bewiesen wurde er aber erst ca. 100 Jahre später durch Gauß.

[2] vgl. [7]
[3] vgl. [4], Vorbemerkung

Kapitel I.
Die Problemgeschichte von Fermats letztem Satz

Fermats Leben

Abbildung 1: Pierre de Fermat

Pierre de Fermat wurde am 20. August 1601 in der südwestfranzösischen Stadt Beaumont de Lomagne als Sohn eines wohlhabenden Lederhändlers geboren. Nach einer vorzüglichen Schulbildung im Franziskanerkloster Grandselve studierte er an der Universität von Toulouse.
Auf Drängen der Familie schlug Fermat eine juristische Laufbahn ein und wurde 1631 zum *Conseiller au Parlement de Toulouse* ernannt, wo er als Hofrat an der Petitionskammer tätig war. Fermat war ein tüchtiger Staatsdiener und darüber hinaus als Richter tätig. Er strebte nicht nach Anerkennung und Ruhm, sondern bevorzugte es, in aller Ruhe neue mathematische Sätze zu

postulieren ohne dabei die Fragen seiner Kollegen beantworten zu müssen.[4] Gemeinsam mit Pascal war Fermat nicht nur der Schöpfer der Wahrscheinlichkeitstheorie, sondern er trug auch wesentlich zur Begründung der Differentialrechnung bei. Dies hätte bei weitem gereicht, um Fermat einen Platz unter den großen Mathematikern der Geschichte zu sichern. Doch er befasste sich noch mit einem weiteren Gebiet der Mathematik, der Zahlentheorie. Fermat untersuchte mit leidenschaftlichem Interesse die Eigenschaften der Zahlen und ihre Beziehungen untereinander.[5]
Nachdem Fermat am 12. Januar 1665 verstarb, verbrachte sein Sohn Clément-Samuel die darauffolgenden fünf Jahre damit, sämtliche Aufzeichnungen und Briefe seines Vaters sowie dessen Randnotizen in seiner Ausgabe der *Arithmetica* zu sammeln. Diese veröffentlichte er schließlich in einer besonderen Ausgabe der *Arithmetica*. Diese enthielt achtundvierzig Bemerkungen Fermats, wobei die Zweite als Fermats letzter Satz oder als Fermatsche Vermutung bekannt werden sollte.[6]

Die Entstehung des Problems

Der Ursprung von Fermats letztem Satz liegt im Satz des Pythagoras. Der Satz des Pythagoras besagt, dass zu den ganzzahligen Lösungen (x, y, z) der Gleichung $X^2 + Y^2 = Z^2$ ein rechtwinkliges Dreick mit den Seiten x, y und z gehört (z.B. $3^2 + 4^2 = 5^2$ oder $5^2 + 12^2 = 13^2$). Solche x, y und z, die diese Gleichung lösen, nennt man Pythagoras-Tripel. Das Problem Pythagoras-Tripel zu finden, bezeichnet man heute, nach Diophantos von Alexandria, als diophantisches Problem. Diophantos war der letzte große Vertreter der griechischen Mathematiktradition. Leider ist über diesen Mathematiker so gut wie nichts bekannt, so weiß man nichts über seinen Geburtsort, und die Zeit seines Wirkens in Alexandria lässt sich nur ungefähr auf die Zeit um 250 n. Chr. schätzen. Er befasste sich v.a. mit Fragen, die ganzzahlige Lösungen erforderten. Während seiner Zeit in Alexandria sammelte er die schon klar gelösten Probleme und erfand neue, die er zu einer großen Abhandlung mit dem Titel *Arithmetica* zusammenstellte. Sieben Bücher dieses Werkes gingen auf Grund einer Reihe tragischer Geschehnisse verloren und warfen die Mathematik bis in die Ära der Babylonier zurück. Die verbleibenden sechs Bücher inspirierten die Mathematiker der Renaissance, unter ihnen auch

[4] vgl. [4], S.59 ff.
[5] vgl. [4], S.68 f.
[6] vgl. [4], S.88

Pierre de Fermat.[7]
In der Mathematik ist es üblich von einem bereits existierenden Problem auszugehen und auf ein allgemeineres zu schließen, obwohl die richtige Verallgemeinerung oft nur schwer zu finden ist. So verhielt es sich auch, als Fermat Diophantos Buch las.[8]

„Anstelle des Satzes von Pythagoras,

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

sann Fermat über eine Abwandlung nach:

$$x^3 + y^3 = z^3.“[9]$$

Indem Fermat die Potenz von 2 auf 3 erhöhte, erhielt er eine neue Gleichung, die, wie Euler und Gauß später bewiesen, keine ganzzahlige Lösung besaß. Fermat untersuchte auch noch höhere Potenzen, konnte jedoch nie eine Lösung finden. Schließlich kam er zu dem Schluss, dass es keine ganzzahlige Lösung für die folgende Gleichung gibt:

$$x^n + y^n = z^n \text{ mit } n = 3, 4, 5, \ldots$$

Daher schrieb er an den Rand seiner Ausgabe der *Arithmetica*:

„Es ist 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.“[10]

Fermat glaubte diese Behauptung beweisen zu können und fügte noch eine weitere Bemerkung hinzu:

„Ich habe hierfür einen wahrhaft wunderbaren Beweis, doch ist dieser Rand hier zu schmal, um ihn zu fassen.“[11]

Obwohl Fermat nie jemandem seine Beweise mitteilte, wurde Fermats letzter oder großer Satz trotzdem berühmt.

---

[7] vgl. [4], S.76 ff.
[8] vgl. [4], S.86
[9] [4], S.86
[10] [4], S.87
[11] [4], S.87

Die Suche nach dem Beweis

Über drei Jahrhunderte lang haben viele große Mathematiker versucht, Fermats verlorenen Beweis wiederzuentdecken, doch keinem einzigen ist es gelungen. Nach Fermats Tod suchte man immer wieder in seinem Haus, in der Hoffnung, eine entscheidende Notiz zu finden. Doch nie entdeckte man einen Hinweis, wie Fermats Beweis ausgesehen haben mochte.[12]
Bereits zu Beginn des neunzehnten Jahrhunderts war Fermats letzter Satz das berüchtigste Problem der Zahlentheorie und seit Euler den Fall $n = 3$ beweisen konnte, wurden keine weiteren Fortschritte mehr erbracht. Doch die Arbeit einer jungen Französin sollte die Suche nach Fermats verlorenem Beweis stark vorantreiben.
Sophie Germain lebte in einer von Chauvinismus und Vorurteilen gegen Frauen geprägten Zeit. Doch trotzdem gelang es ihr als einziger Frau, sich den Zwängen der französischen Gesellschaft zu entziehen und eine große Zahlentheoretikerin zu werden. Mit ihrer Arbeit ermöglichte sie einen großen Fortschritt in der Forschung zu Fermats letztem Satz. Sie leistete einen größeren Beitrag als ihre männlichen Vorgänger.[13]
Sophie Germain wurde am 1. April 1776 als Tochter des Kaufmanns Ambroise-Francois Germain geboren. Ihr Interesse für die Mathematik wurde durch Jean-Étienne Montuclas Buch *Histoire de la Mathématique*, das sie zufällig in der Bibliothek ihres Vaters entdeckte, geweckt. Sie machte sich sofort daran, sich selbst die Grundlagen der Zahlentheorie und der Analysis beizubringen und studierte bald bis spät in die Nacht hinein die Werke von Euler und Newton. Germain arbeitete viele Jahre lang allein, weil es in der Familie keinen Mathematiker gab, der sie in die neuesten Ideen einführen konnte. Außerdem nahmen ihre Tutoren sie nicht ernst, da man in Frankreich der Auffassung war, dass die Mathematik für Frauen nicht geeignet und jenseits ihrer geistigen Fähigkeiten sei.[14]
1794 wurde in Paris die École Polytechnique eröffnet. Da diese Institution nur Männern vorbehalten war entschloß sich Germain, unter einem falschen Namen an der École zu studieren und nahm die Identität eines ehemaligen Studenten der Akademie an. Auf Grund ihrer brillianten Leistungen musste Germain ihre wahre Identität jedoch ihrem Fachbeauftragten Joseph-Louis Lagrange preisgeben. Trotz seines großen Erstaunens fand Lagrange Gefallen an der jungen Frau und wurde ihr Mentor und Freund. Germain gewann zusehends an Selbstvertrauen und beschäftigte sich bald nur noch mit unerforsch-

[12] vgl. [4], S.55 f.
[13] vgl. [4], S.125 ff.
[14] vgl. [4], S.130 f.

ten Gebieten der Mathematik. Sie interessierte sich v.a. für die Zahlentheorie und so stieß sie schließlich auch auf Fermats letzten Satz. Mehrere Jahre lang arbeitete sie an dem Problem, bis sie der Meinung war, einen bedeutenden Durchbruch erzielt zu haben. Nun brauchte sie einen Kollegen auf dem Feld der Zahlentheorie, mit dem sie ihre Ideen erörtern konnte. Daher entschloß sie sich, sich an den deutschen Mathematiker Carl Friedrich Gauß zu wenden. Als er Sophie Germains Brief erhielt, war er von ihrer bahnbrechenden Leistung sehr beeindruckt und began sie bei ihrer Arbeit zu unterstützten.[15] Im Jahr 1825 konnte sie dank Johann Peter Gustav Lejeune-Dirichlet und Adrien-Marie Legendre mit ihrer Methode den ersten richtigen Erfolg verbuchen. Zwischen diesen beiden Mathematikern lag eine ganze Generation. Legendre war bereits in den Siebzigern und Dirichlet hingegen war ein junger Zahlentheoretiker, der gerade zwanzig geworden war. Beide konnten unabhängig voneinander aufgrund Sophie Gemains Vorarbeit beweisen, dass der Fall $n = 5$ keine Lösungen hat. Vierzehn Jahre später gelang es dem Franzosen Gabriel Lamé Germains Verfahren auf geniale Weise zu ergänzen und so Fermats Vermutung für die Primzahl $n = 7$ zu beweisen. Germain hatte den Zahlentheoretikern gezeigt, wie eine ganze Gruppe von Primzahlfällen zu erledigen war, und nun lag es an ihnen, Fermats letzten Satz Fall für Fall zu beweisen. Sophie Germains Arbeit an Fermats letztem Satz war ihr größter Beitrag zur Mathematik.
Als sich Gauß von der Zahlentheorie abwandte, brach bald darauf sein Briefkontakt zu Germain ab. Auf Grund der fehlenden Unterstützung wandte auch sie sich wenig später von der reinen Mathematik ab und begann eine erfoglreiche Laufbahn als Physikerin.[16]
„Pierre de Fermats beiläufige Randnotiz in Diophantos' *Arithmetica* war zum haarsträubendsten Rätsel der Mathematikgeschichte geworden.“[17] Obwohl inzwischen Skeptiker der Meinung waren, man sei womöglich hinter einem nichtexistenten Beweis her, waren immer noch ganze Generationen von Mathematikern von Fermats letztem Satz besessen. Sie alle wollten der Herausforderung, die dieses Problem darstellte, standhalten und sie träumten davon, dieses Rätsel, an dem schon so viele andere vor ihnen gescheitert waren, zu lösen.
Die Sehnsucht, ein mathematisches Problem zu lösen, wird v.a. durch die Neugier geweckt, und die Belohnung ist die schlichte, aber überwältigende Befriedigung, die die Lösung eines jeden Rätsels mit sich bringt. Im Falle der Fermatschen Vermutung mangelte es sicher nicht an Neugier. Auch die

[15] vgl. [4], S.131 f.
[16] vgl. [4], S.133 ff.
[17] [4], S.179

Zweifel, ob das Problem überhaupt lösbar sei, reichten nicht aus, um die Mathematiker zu entmutigen. Viel enttäuschender war hingegen die Tatsache, dass die Mathematiker in den dreißiger Jahren nahezu all ihre Techniken erschöpft hatten und daher zur Lösung des Problems etwas Neues benötigten.[18]

Die Shimura-Taniyama-Vermutung und ihre Verknüpfung mit Fermats letztem Satz

Im September 1955 fand in Tokio ein internationales Symposium statt. Vier der dort gestellten Fragen stammten von Taniyama. Diese Fragen gründeten auf der Idee, dass jede elliptische Gleichung mit einer Modulform verwandt ist. Diese Idee wurde aber von den damaligen Mathematikern nur als merkwürdige Beobachtung abgetan.[19]
Taniyamas einziger verbündeter war Shimura, der an die Idee seines Freundes glaubte. Nach dem Symposium machten sie sich gemeinsam auf die Suche nach mehr Material, um ihre Vermutung zu beweisen. 1957 wurde die Zusammenarbeit vorübergehend unterbrochen, da Shimura an das Institut for Advanced Study in Princeton eingeladen wurde. Nach seinen zwei Jahren als Gastprofessor in Amerika wollte er die Arbeit mit Taniyama fortsetzen. Doch dazu kam es nicht mehr, da sich Yutaka Taniyama am 17. November 1958 das Leben nahm.[20]
Die Fragen über elliptische Gleichungen und Modulformen, die Taniyama auf dem Symposium aushändigte, enthielten seine großartigste Einsicht. Doch den gewaltigen Einfluss seiner Entdeckung auf die Zahlentheorie erlebte er nicht mehr.
Nach Taniyamas Tod konzentrierte sich Shimura darauf, die genaue Beziehung zwischen elliptischen Gleichungen und Modulformen zu klären. Er gewann dabei immer mehr die Überzeugung, dass jede einzelne elliptische Gleichung mit einer Modulform verwandt sein müsse. Andere Mathematiker hatten immer noch Zweifel. Da aber Shimura immer deutlichere Hinweise fand, gewann seine Theorie über elliptische Gleichungen und Modulformen immer mehr Anerkennung. Er konnte sie zwar nicht beweisen, doch zumindest war sie jetzt mehr als nur Wunschdenken. Daher erhielt seine Theorie den Titel einer Vermutung. Anfangs bezeichnete man sie als Taniyama-Shimura-Vermutung, in Anerkennung des Mannes, der sie angeregt, und seines Kolle-

[18] vgl. [4], S.179 ff.
[19] vgl. [4], S.216 ff.
[20] vgl. [4], S.219

gen, der sie vollständig ausgearbeitet hatte.[21]
André Weil übernahm schließlich die Vermutung und verbreitete sie auch im Westen. Da Weil bei seinen Untersuchungen der Idee von Shimura und Taniyama weitere solide Hinweise zu ihren Gunsten fand, wurde die Hypothese oft auch als Taniyama-Shimura-Weil-Vermutung bezeichnet.[22]
In den späten sechziger Jahren testeten ganze Scharen von Mathematikern immer wieder die Taniyama-Shimura-Vermutung und in jedem einzelnen Fall hatte die elliptische Gleichung tatsächlich eine zugehörige Modulform. Man war dadurch von der Richtigkeit der Taniyama-Shimura-Vermutung immer mehr überzeugt. Obwohl ein echter Beweis noch immer fehlte, tauchte die Vermutung häufig in mathematischen Forschungspapieren auf. Dort wurde spekuliert, was geschehen würde, wenn sie bewiesen werden könnte. Natürlich waren diese Ergebnisse nur hypothetischer Natur, aber auf diese Art und Weise entstand eine Überfülle mathematischer Arbeiten, die auf der Wahrheit der Taniyama-Shimura-Vermutung beruhten. Die Mathematiker hofften, dass eines Tages einer kommen würde und durch den Beweis der Taniyama-Shimura-Vermutung all ihre Arbeiten für richtig erklären würde. Andererseits fürchteten sie auch immer, dass jemand beweisen könnte, dass Taniyama und Shimura falsch gelegen hatten, und damit zwei Jahrhunderte Forschungsarbeit zerstört werden.[23]
Im Herbst 1984 versammelte sich eine erlesene Gruppe von Zahlentheoretikern zu einem Symposium im Schwarzwald. Einer der Referenten, der Saarbrücker Mathematiker Gerhard Frey, konnte zwar keinen Beweis der Vermutung liefern, stellte aber die Behauptung auf, falls jemand die Taniyama-Shimura-Vermutung beweisen könnte, wäre damit auch Fermats letzter Satz bewiesen. Fermats letzter Satz lautet, dass es keine positiven ganzzahligen Lösungen für die Gleichung $x^n + y^n = z^n$, mit n gößer als 2, gibt. Frey beschäftigte sich jedoch mit der Frage, was wäre, wenn diese Vermutung falsch wäre und es mindestens eine Lösung gäbe. Durch die Umformung der Fermatschen Gleichung in eine elliptische Gleichung, hatte Frey die Fermatsche Vermutung mit der Taniyama-Shimura-Vermutung verknüpft.[24]

„Freys Argument lautete wie folgt:

(1) Wenn und nur wenn Fermats letzter Satz falsch ist, existiert Freys elliptische Gleichung.

[21] vgl. [4], S.222 f.
[22] vgl. [4], S.223
[23] vgl. [4], S.224 ff.
[24] vgl. [4], S.228 f.

(2) Freys elliptische Gleichung ist so abwegig, dass sie nie modular sein kann.

(3) Die Taniyama-Shimura-Vermutung besagt, dass jede elliptische Gleichung modular sein muss.

(4) Deshalb muss die Taniyama-Shimura-Vermutung falsch sein!

Andererseits jedoch, und folgenträchtiger, konnte Frey sein Argument auch rückwärts aufziehen:

(1) Wenn die Taniyama-Shimura-Vermutung bewiesen werden kann, muss jede elliptische Gleichung modular sein.

(2) Wenn jede elliptische Gleichung modular sein muss, dann darf die Freysche elliptische Gleichung nicht existieren.

(3) Wenn die Freysche elliptische Gleichung nicht existiert, dann kann es keine Lösung der Fermatschen Gleichung geben.

(4) Deshalb ist die Fermatsche Vermutung richtig!“[25]

Zum ersten Mal in über hundert Jahren sah das härteste mathematische Problem wieder angreifbar aus. Freys Publikum war von seiner Einsicht beeindruckt, doch fast jeder der Anwesenden, außer Frey selbst, hatte einen elementaren Fehler bemerkt. Er hatte nicht bewiesen, dass seine elliptische Gleichung hinreichend abwägig war. Und solange der Fehler nicht behoben war, war Freys Arbeit unvollständig. Eine Reihe von Mathematikern bemühte sich, die Verbindung der Taniyama-Shimura-Vermutung mit der Fermatschen Vermutung zu beweisen und zu vervollständigen. Dazu gehörte auch Ken Ribet, Professor an der Universität von Kalifornien in Berkeley. Er war es schließlich auch, der als erster den vollständigen Beweis gefunden hat. Damit war Fermats letzter Satz unauflöslich mit der Taniyama-Shimura-Vermutung verknüpft. Dreieinhalb Jahrhunderte lang war die Fermatsche Vermutung ein abgeschottetes Problem gewesen. Nun hatte Ken Ribet, angeregt von Gerhard Frey, das wichtigste Problem des siebzehnten Jahrhunderts mit dem bedeutendsten Problem des zwanzigsten Jahrhunderts verknüpft.[26]
Zunächst regte sich neue Hoffnung, Fermats letzten Satz dadurch beweisen zu können. Doch dann wurde deutlich, dass die Mathematiker bereits dreißig Jahre lang versuchten, Taniyama-Shimura zu beweisen und daran bisher gescheitert waren. Warum sollte dies also jetzt gelingen? „Andrew Wiles war

[25] [4], S.230
[26] vgl. [4], S.230 ff.

vermutlich einer der wenigen Menschen auf der Welt, die davon träumten, man könne wirklich hergehen und diese Vermutung beweisen.“[27]

Andrew Wiles, der Eremit in der Dachkammer

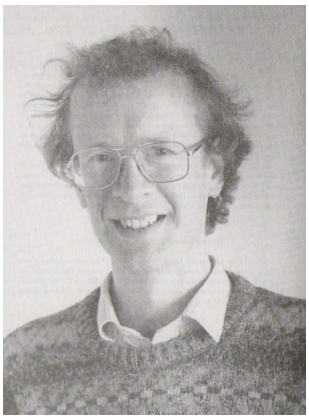

Abbildung 2: Andrew Wiles

Um überhaupt eine Chance zu haben, die Taniyama-Shimura-Vermutung beweisen zu können, musste Wiles sich tief in das Problem versenken. Zu diesem Zweck las er die neuesten Zeitschriftenbeiträge und übte die modernsten mathematischen Verfahren so lange, bis er sie im Schlaf beherrschte. Außerdem machte er sich mit allem vertraut, was nur im entferntesten etwas mit elliptischen Gleichungen und Modulformen zu tun hatte.[28]
Wiles gab alle Arbeiten auf, die nicht direkt im Zusammenhang mit dem Beweis der Fermatschen Vermutung standen. Er ging nur noch seinen Verpflichtungen an der mathematischen Fakultät in Princeton nach. Wann immer möglich arbeitete er zu Hause, wo er sich in seine Dachkammer zurückzog. In dem Moment, indem er entschloß sich mit dem Beweis auseinanderzusetzen, fasste Wiles auch den Entschluss, in völliger Abgeschiedenheit zu arbeiten und kein Wort darüber zu reden. Ein Grund für die Entscheidung, über seine Arbeit nicht zu sprechen, war das Bedürfnis, in Ruhe gelassen zu werden. Ein weiterer Grund war sicher auch das Verlangen nach Ruhm. Er befürchtete, eines Tages den Beweis schon fast geschafft zu haben, ohne den letzten Schritt der Rechnung beenden zu können. Sollte an diesem Punkt etwas über seine Arbeit nach außen dringen, gäbe es nichts, was einen Rivalen abhalten

[27] [4], S.235
[28] vgl. [4], S.239

würde, den Beweis zu vervollständigen und den Preis zu erhalten.[29]
In den folgenden Jahren gelangen Wiles eine Reihe außergewöhnlicher Entdeckungen, von denen aber keine veröffentlicht werden sollte, solange der Beweis noch nicht vollständig war. Selbst vertraute Kollegen wussten nichts von diesen Forschungen. Die einzige, die Wiles' Geheimnis kannte, war seine Frau Nada.[30]

Fermats letzter Satz ist bewiesen

Nach sieben Jahren harter Arbeit hatte Wiles einen Beweis der Taniyama-Shimura-Vermutung zustande gebracht und damit endlich Fermats letzten Satz bewiesen. Nun war es an der Zeit, dem Rest der Welt davon Mitteilung zu machen. Dazu nutzte er eine Konferenz in Cambridge am Isaac Newton Institut, die für Ende Juni 1993 angekündigt war. Als Wiles in Cambridge ankam, hatte er noch zweieinhalb Wochen bis zu seinen Vorträgen. In dieser Zeit wollte er den Beweis mit ein oder zwei Experten durchsprechen. Nach sieben Jahren energischer Arbeit war Wiles nun bereit, der Welt seinen Beweis zu verkünden. Wiles erinnert sich an die Atmosphäre gegen Ende seines Vortrags: „Obwohl die Presse schon Wind von dem Vortrag bekommen hatte, war sie glücklicherweise nicht dabei. Doch im Publikum saßen eine Menge Leute, die gegen Ende Fotos machten, und der Institutdirektor war gut vorbereitet mit einer Flasche Champagner gekommen. Während ich den Beweis vortrug, herrschte das typische würdevolle Schweigen, und dann schrieb ich einfach Fermats letzten Satz an die Tafel. Ich denke, das genügt, meinte ich dann, und es gab langen Beifall.“[31]
Nach Wiles' Vortrag wurde sofort das Wolfskehl-Komitee über den Beweis informiert. Bevor der Preis jedoch verliehen werden konnte, musste er erst, laut den Wettbewerbsregeln, von anderen Mathematikern bestätigt und formell veröffentlicht werden. Daher reichte Wiles sein Manuskript bei der Zeitschrift *Inventiones Mathematicae* ein. Um die Überprüfung des Beweises zu vereinfachen, unterteilte man den zweihundertseitigen Beweis in sechs Abschnitte, für die jeweils ein Gutachter zuständig war. Wiles hatte den Beweis schon mehrfach geprüft, bevor er ihn an die Gutachter weitergeleitet hatte, und er erwartete daher nur harmlose Irrtümer, die er umstandslos würde korrigieren können. Anfänglich verhielt es sich auch so. Aber dann tauchte eine Frage auf, bei der es sich um einen elementaren Fehler handelte. Das Problem bestand

[29] vgl. [4], S.239 ff.
[30] vgl. [4], S.241 f.
[31] [4], S.281

darin, dass es keine Garantie dafür gab, dass die Kolywagin-Flach-Methode im Sinne von Wiles funktionierte.[32]
Ein paar Wochen zuvor wurde Wiles in den Zeitungen als „der brillanteste Mathematiker der Welt“[33], der nach 350 Jahren endlich die Oberhand über Pierre de Fermat errungen hatte, gefeiert. Nun stand Wiles kurz davor, einen Fehler eingestehen zu müssen. Bevor er aber seinen Irrtum zugab, wollte er noch einmal alles versuchen, um die Lücke zu schließen. Daher beschloß er zu seiner alten Arbeitsweise zurückzukehren und sich völlig von der Außenwelt abzuschotten. Lange war Wiles davon überzeugt, dass der Fehler schnell behoben sei. Doch mit der Zeit wurde das Problem immer unbezwingbarer. Kaum ein halbes Jahr nach seinem Vortrag am Newton Institute lag Wiles' Beweis in Fetzen. Sein Kindheitstraum hatte sich in einen Alptraum verwandelt. Trotz des steigenden Drucks weigerte sich Wiles, das Manuskript freizugeben. Sieben Jahre seines Lebens hatte er daran gearbeitet, und nun war er nicht bereit, sich zurückzulehnen und jemand anderem dabei zuzusehen, wie er den Beweis vervollständigte. Denn nicht derjenige, der am meisten Arbeit in die Sache gesteckt hatte, würde Fermats letzten Satz beweisen, sondern derjenige, der den endgültigen und vollständigen Beweis lieferte. Wiles versuchte erneut sich so wie damals, als er den ursprünglichen Beweis erarbeitet hatte, abzuschotten. Er zog sich also in die Dachkammer zurück, um konzentriert zu arbeiten.[34]
Obwohl die Taniyama-Shimura-Vermutung und damit auch Fermats letzter Satz nicht bewiesen war, hatte Wiles den Mathematikern eine ganze Reihe neuartiger Verfahren und Strategien geliefert. Wiles' Scheitern wäre demnach keine Schande gewesen und allmählich begann er sich mit der möglichen Niederlage abzufinden. Wiles beschloß, sich ein letztes Mal das ganze Gefüge der Kolywagin-Flach-Methode anzusehen und ausfindig zu machen, warum sie nicht funktionierte. Glücklich erinnerte er sich an diesen Tag: „Eines Montagmorgens, es war der 19. September, saß ich am Schreibtisch und untersuchte die Kolywagin-Flach-Methode. Nicht, dass ich geglaubt hätte, sie flottmachen zu können, vielleicht konnte ich wenigstens erklären, warum sie nicht funktionierte. Mir kam es vor, als klammerte ich mich an einen Strohhalm, doch ich wollte mich einfach vergewissern. Plötzlich, völlig unerwartet, hatte ich diese unglaubliche Eingebung. Die Kolywagin-Flach-Methode funktionierte zwar nicht richtig, sie war jedoch alles, was ich brauchte, um die ursprüngliche Iwasawa-Theorie in Gang zu setzen. Ich sah, dass ich die Kolywagin-Flach-Methode gut genug beherrschte, um meinen ursprünglichen, vor drei Jahren

[32] vgl. [4], S.287 ff.
[33] Singh 2003, S.290
[34] vgl. [4], S.290 ff.

verfolgten Ansatz gelingen zu lassen. Aus der Asche der Kolywagin-Flach-Methode tauchte also gleichsam die wahre Antwort auf das Problem auf.“[35] Beide Theorien alleine waren also unzulänglich, aber zusammen funktionierten sie hervorragend. Wiles hatte sich damit nicht nur einen Kindheitstraum erfüllt, sondern hatte auch der Welt sein Genie bewiesen.
Diesmal gab es am Beweis nichts zu rütteln. Die beiden Artikel waren die am gründlichsten geprüften Manuskripte in der Geschichte der Mathematik und wurden schließlich in den *Annals of Mathematics* (Mai 1995) veröffentlicht. Wiles hatte in achtjähriger harter Arbeit alle bahnbrechenden Erkenntnisse der Zahlentheorie des zwanzigsten Jahrhunderts zusammengetragen und sie in seinen Beweis eingebaut. Er hatte vollkommen neue mathematische Verfahren entwickelt und sie mit den herkömmlichen verflochten und so gelang es ihm schließlich Fermats letzten Satz zu beweisen.[36]

[35] [4], S.305 f.
[36] vgl. [4], S.311 f.

Kapitel II.
Das Rechnen mit ganzen und komplexen Zahlen

§1 Grundlegende Regeln und Prinzipien

Es wird vorausgesetzt, dass der Leser mit ganzen Zahlen rechnen kann und mit der Mengenschreibweise vertraut ist. Bis auf weiteres bedeuten kleine Buchstaben

$$a, b, c, \ldots, x, y, z$$

ganze Zahlen, das heißt sie stehen für

$1, 2, 3 \ldots$	(positive ganze Zahlen)
0	(Null)
$-1, -2, -3, \ldots$	(negative Zahlen)

Die **natürlichen Zahlen** sind bei uns die Zahlen

$$0, 1, 2, 3, \ldots$$

Ihre Gesamtheit wird mit $\mathbb{N}$ bezeichnet. $\mathbb{Z}$ steht für die Gesamtheit aller ganzen Zahlen

$$\ldots, -3, -2, -1, 0, 1, 2, 3 \ldots$$

Wir werden von den folgenden **Regeln** für das Rechnen mit ganzen Zahlen Gebrauch machen:

Verknüpfungsregeln der Addition

(1) $(a + b) + c = a + (b + c)$ (Assoziativgesetz)

(2) $a + b = b + a$ (Kommutativgesetz)

(3) $a + (-a) = 0$ ($-a$ ist **inverses Element** zu a bzgl. $+$)

(4) $0 + a = a$ (0 ist **neutrales Element** bzgl. $+$)

Daraus ergibt sich

1.1 Satz: Jede Gleichung $X + a = b$ mit $a, b \in \mathbb{Z}$ hat in $\mathbb{Z}$ eine Lösung, und nur eine.
Das soll heißen: Zu jedem Paar a, b ganzer Zahlen gibt es genau eine Zahl $x \in \mathbb{Z}$, so dass $x + a = b$.

Beweis:
Existenz: Setze $x := b + (-a)$. Dann ist (nach den Regeln (1) bis (4))

$$x + a = (b + (-a)) + a = b + ((-a) + a) = b + (a + (-a)) = b + 0 = 0 + b = b.$$

Eindeutigkeit: Sei $y \in \mathbb{Z}$ beliebig mit $y + a = b$. Dann ist

$$b + (-a) = (y + a) + (-a) = y + (a + (-a)) = y + 0 = y.$$

Verknüpfung der Multiplikation

(5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativgesetz)

(6) $a \cdot b = b \cdot a$ (Kommutativgesetz)

(7) $1 \cdot a = a$ (1 ist **neutrales Element** bzgl. $\cdot$)

(8) $a \cdot b = 0$ dann und nur dann, wenn $a = 0$ oder $b = 0$

Distributivgesetz

(9) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Für $a + (-b)$ schreibt man auch $a - b$. Dann gilt auch

$$a \cdot (b - c) = (a \cdot b) - (a \cdot c)$$

Wir verwenden gelegentlich die Abkürzungen
„$\Longrightarrow$“ für „daraus folgt“,
„$\Longleftrightarrow$“ für „genau dann wenn“ und
„$:=$“ für „ist definitionsgemäß gleich“.

1.2 Kürzungsregel: Aus $a \cdot b = a \cdot c$ und $a \neq 0$ folgt $b = c$.

Beweis: Aus $a \cdot b = a \cdot c$ folgt $(a \cdot b) - (a \cdot c) = (a \cdot c) - (a \cdot c) = 0$ und daraus ergibt sich $a \cdot (b - c) \overset{(9)}{=} (a \cdot b) - (a \cdot c) = 0$. Wegen (8) gilt $b - c = 0$ und daraus folgt $c = (b - c) + c = b + ((-c) + c) = b + 0 = b$.
Da für Addition und Multiplikation das Assoziativgesetz gilt, kann man sich viele Klammern sparen: Schreibe:

$$\begin{array}{rll} a + b + c & \text{für} & (a + b) + c \\ a \cdot b \cdot c & \text{für} & (a \cdot b) \cdot c \end{array}$$

Damit lassen sich auch endliche Summen und Produkte ohne Klammern erklären:
$a_1 + a_2 + a_3 + a_4 := (a_1 + a_2 + a_3) + a_4$
$\vdots$
$a_1 + a_2 + \ldots + a_{n-1} + a_n := (a_1 + \ldots + a_{n-1}) + a_n$
$a_1 \cdot a_2 \cdot a_3 \cdot a_4 := (a_1 \cdot a_2 \cdot a_3) \cdot a_4$
$\vdots$
$a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} \cdot a_n := (a_1 \cdot \ldots \cdot a_{n-1}) \cdot a_n$

Durch die Regelung „Punktrechnung geht vor Strichrechnung“ können weitere Klammern eingespart werden:

$$a \cdot b + c \cdot d \text{ steht für } (a \cdot b) + (c \cdot d)$$

Ferner wird der Malpunkt oft weggelassen und man verwendet die abkürzende Schreibweise

$$\sum_{n=1}^{k} a_n := a_1 + \ldots + a_k; \prod_{n=1}^{k} a_n := a_1 a_2 \ldots a_n; a^n = \underbrace{a \cdot \ldots a}_{n-mal}$$

Wichtig ist die
Formel für die endliche geometrische Reihe:

$$(1 + x + x^2 + ... + x^{n-1})(1 - x) = 1 - x^n$$

Beweis:

$$\begin{array}{r} (1 + x + ... + x^{n-1})(1 - x) = \\ 1 + x + x^2 + ... + x^{n-2} + x^{n-1} \\ -(x + x^2 + ... + x^{n-2} + x^{n-1} + x^n) \\ \hline = 1 \qquad\qquad\qquad\qquad -x^n \end{array}$$

Anordnung der ganzen Zahlen: $\mathbb{Z}$ ist in natürlicher Weise angeordnet:

$$\ldots -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots$$

Definition: a heißt **kleiner** als b („$a < b$“), wenn a in der obigen Reihung links von b steht. Schreibe auch $a > b$ (a **größer** b) falls $b < a$. Damit gilt offensichtlich: $a > 0$ genau dann, wenn $-a < 0$.

Anordnungsregeln:

(1) Es gilt entweder $a > b$ oder $a = b$ oder $a < b$

(2) Aus $a > b$ und $b > c$ folgt $a > c$

(3) Aus $a > b$ folgt $a + c > b + c$

(4) Aus $a > b$ und $c > 0$ folgt $ac > bc$

Schreibweisen:
$a \geq b$ steht für „$a > b$ oder $a = b$“.
$a \leq b$ steht für „$a < b$ oder $a = b$“.

Definition: Für $a \in \mathbb{Z}$ definiert man den **Betrag** $|a|$ von a als

$$|a| := \begin{cases} a, & \text{falls } a \geq 0 \\ -a, & \text{falls } a < 0 \end{cases}$$

Betragsregeln:

(1) $|a| \geq 0$; $|a| = 0$ genau dann, wenn $a = 0$

(2) $|ab| = |a||b|$

(3) $|a + b| \leq |a| + |b|$

Minimum und Maximum: Seien $a_1, ..., a_n$ ganze Zahlen. Die kleinste der Zahlen $a_1, ..., a_n$ heißt das **Minimum** und die größte das **Maximum** von $a_1, ..., a_n$. Schreibe dafür $\text{Min}(a_1, ..., a_n)$ bzw. $\text{Max}(a_1, ..., a_n)$.

Grundprinzipien: Wir wollen das folgende Prinzip anerkennen.

(P) **Prinzip vom kleinsten Element.** Jede nicht leere Menge A von natürlichen Zahlen besitzt ein kleinstes Element, d.h.:
Es gibt ein Element $a_0 \in A$, so dass $x \geq a_0$ für alle $x \in A$. Schreibe dann $a_0 = \mathrm{Min}A$.
Aus diesem Prinzip lassen sich weitere Grundsätze ableiten:
$A(x)$ bezeichne eine Aussage, die für eine natürliche Zahl x zutreffen kann, d.h.:
Für $x \in \mathbb{N}$ gilt entweder $A(x)$ oder $A(x)$ gilt nicht.

(G) **Prinzip vom kleinsten Gegenbeispiel.** Sei $A(x)$ eine Aussage über natürliche Zahlen $x \geq a_0$. Ist $A(x)$ nicht allgemein gültig, so gibt es dafür ein kleinstes Gegenbeispiel. Das soll heißen:
Ist $A(x)$ falsch für wenigstens ein $x \geq a_0$, so gibt es eine Zahl $a \geq a_0$, so dass gilt:

(1) $A(a)$ ist falsch.

(2) $A(x)$ ist richtig für alle $x \in \mathbb{N}$ mit $a_0 \leq x < a$.

(G) ergibt sich leicht aus dem Prinzip vom kleinsten Element:
Sei $N = \{x \mid x \in \mathbb{N}, x \geq a_0 \text{ und } A(x) \text{ ist falsch}\}$. Nach Voraussetzung ist N nicht die leere Menge $\emptyset$. Nach (P) existiert daher das Minimum $a = \mathrm{Min}N$.
Zeige nun, dass a die Bedingungen (1) und (2) erfüllt.
Zu (1): Wegen $a \in N$ ist $A(a)$ falsch.
Wegen $a = \mathrm{Min}N$ ist

$(*)$ $x \geq a$ für alle $x \in N$.

Zu (2): Sei $x \in \mathbb{N}$ mit $a_0 \leq x < a$. Wegen $(*)$ ist dann $x \notin N$. Nach Definition von N bedeutet dies, dass $A(x)$ richtig ist.
Aus dem Prinzip vom kleinsten Gegenbeispiel ergibt sich leicht das wichtigere Prinzip der vollständigen Induktion.

(V) **Prinzip der vollständigen Induktion.** Sei $A(x)$ eine Aussage über natürliche Zahlen x mit folgenden beiden Eigenschaften:

(i) $A(0)$ ist richtig.

(ii) Für alle $n \in \mathbb{N}$ folgt aus der Richtigkeit von $A(n)$ schon die Richtigkeit von $A(n+1)$.

Dann ist A eine allgemein gültige Aussage, d.h.

$$A(x) \text{ ist richtig für alle } x \in \mathbb{N}.$$

Das Induktionsprinzip (V) lässt sich aus (G) herleiten:
Sei $A(x)$ eine Aussage mit den Eigenschaften (i) und (ii). Angenommen A wäre nicht allgemein gültig. Dann gibt es gemäß (G) zu A ein kleinstes Gegenbeispiel a, d.h.: $A(a)$ ist falsch und $A(b)$ ist richtig für alle $b < a$. Wegen (i) ist dann $a > 0$, also $a - 1 \geq 0$ ist eine natürliche Zahl. Nach Wahl von a ist ferner $A(a-1)$ richtig. Wende nun (ii) auf $n = a-1$ an: Aus der Richtigkeit von $A(a-1)$ folgt die Richtigkeit der Aussage $A((a-1)+1) = A(a)$, Widerspruch!
Also ist die Annahme „A ist nicht allgemein gültig“ falsch, d.h. A **ist** allgemein gültig. Die Gültigkeit des folgenden Beweisprinzips ergibt sich ebenfalls aus dem Prinzip vom kleinsten Gegenbeispiel.

Schema eines Beweises durch vollständige Induktion. Sei $A(x)$ eine Aussage über natürliche Zahlen x mit $x \geq a_0$. Es soll gezeigt werden, dass $A(x)$ für alle $x \geq a_0$ richtig ist. Dazu geht man folgendermaßen vor:

(a) Man zeigt, dass $A(a_0)$ richtig ist (**Induktionsbeginn**).

(b) Man nimmt an, dass $A(x)$ gilt für alle $x \in \mathbb{N}$ mit $a_0 \leq x \leq n$ (**Induktionsannahme** (Induktionsbehauptung)).

(c) Man schließt aus (a) und (b), dass auch $A(n+1)$ gilt (**Induktionsschluss**).

§2 Teilbarkeit in $\mathbb{Z}$

Bis auf weiteres stehen kleine Buchstaben für ganze Zahlen.
Teilbarkeit: Sei $a \neq 0$. Eine Zahl b heißt durch a **teilbar**, wenn es ein q gibt mit $b = qa$. Wir sagen dann auch: a teilt b (a ist ein **Teiler** von b) und b ist ein **Vielfaches** von a.
Wir schreiben dafür: $a \mid b$.
Wenn a die Zahl b nicht teilt, schreiben wir: $a \nmid b$.
Ist $a \mid b$ und $b = qa$, so ist $q = \frac{b}{a}$ eindeutig durch das Paar a, b bestimmt.
Die **trivialen Teiler** von b sind $\pm b$ und ± 1 ($b = 1 \cdot b = b \cdot 1$ und $b = (-1)(-b) = (-b)(-1)$).

2.1 Regeln:

(a) Aus $a \mid b$ folgt $a \mid -b$ und $-a \mid b$ und $-a \mid -b$ und $|a| \mid |b|$.

(b) Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.

(c) Aus $a \mid b$ und $c \mid d$ folgt $ac \mid bd$ (insbesondere: aus $a \mid b$ folgt $ac \mid bc$).

(d) Aus $a \mid b$ und $a \mid c$ folgt $a \mid bx + cy$ für beliebige x, y.

(e) Aus $ac \mid bc$ und $c \neq 0$ folgt $a \mid b$.

Beweis:

(a) Aus $b = qa$ folgt $-b = (-q)a, b = (-q)(-a), -b = q(-a), |b| = |q||a|$.

(b) Wegen $b = qa$ und $c = rb$ gilt $c = r(qa) = (rq)a$ und daraus folgt $a \mid c$.

(c) $b = qa$ und $d = rc$, daher gilt $bd = (qa)(rc) = (qr)(ac)$. Folglich gilt $ac \mid bd$.

(d) Aus $b = qa$ und $c = ra$ folgt $bx + cy = qax + ray = (qx + ry)a$. Und daraus ergibt sich $a \mid bx + cy$.

(e) Da $bc = q(ac)$ und $c \neq 0$ gilt nach 1.2 $b = qa$ und folglich gilt auch $a \mid b$.

Ist $a \neq 0$, so kann man b durch a immer mit Rest dividieren.

2.2 Division mit Rest: Sei $a \neq 0$ und b beliebig. Dann gibt es zu a, b genau ein Zahlenpaar p, r mit

$$(*) \qquad b = qa + r \text{ und } 0 \leq r < |a|$$

($a \mid b$ genau dann, wenn $r = 0$).
Man nennt q den unvollständigen Quotienten von b durch a, und r den Divisionsrest (Rest bei der Division von b durch a).

Beweis:
1. Existenz: Es genügt dies für $a > 0$ zu zeigen, denn: Wenn $a < 0$, so ist $-a > 0$. Aus $b = \tilde{q}(-a) + r$ mit $0 \leq r < |a| = |-a|$ folgt: $b = qa + r$, wobei $q := -\tilde{q}$.
Für $u_0 = -|b|$ ist $b - u_0 a = b + |b|a \geq 0$. Also ist die Menge $M := \{b - ua \mid u \in \mathbb{Z} \text{ und } b - ua \geq 0\} \subseteq \mathbb{N}$ nicht leer. Nach dem Prinzip vom kleinsten Element existiert somit eine kleinste natürliche Zahl r der Form

$$r = b - qa, q \in \mathbb{Z}.$$

Wegen der Minimalität von r ist $r - a = b - (q+1)a < 0$, also $r < a$. Damit ist, wie gefordert

$$b = qa + r \text{ und } 0 \leq r < a.$$

2. Eindeutigkeit: Sei $b = qa + r = q'a + r'$ mit $0 \leq r < |a|$ und $0 \leq r' < |a|$. Dann ist $(q - q')a = r' - r$ und $|r' - r| < |a|$. Es folgt $q - q' = 0$ und $r' - r = 0 \cdot a = 0$, also $r' = r$.

Der größte gemeinsame Teiler von zwei Zahlen.

2.3 Bemerkung: Ist $a \neq 0$ und $b \mid a$, so ist $|b| \leq |a|$. Insbesondere kommen als Teiler von a nur die endlich vielen Zahlen $\pm 1, \pm 2, ..., \pm a$ in Frage.

Beweis: Aus $b \mid a$ folgt $a = qb$. Da $a \neq 0$ ist, muss auch $q \neq 0$ sein. Also ist $|q| \geq 1$ und daraus ergibt sich schließlich $|a| = |q||b| \geq |b|$.

Nach dieser Bemerkung gibt es einen größten gemeinsamen Teiler von zwei Zahlen a und b, welche nicht beide Null sind. Schreibe für den größten gemeinsamen Teiler (a, b) oder $ggT(a, b)$. Mit anderen Worten:
Der **größte gemeinsame Teiler** (a, b) **von** a **und** b ist die eindeutig bestimmte natürliche Zahl d mit folgenden Eigenschaften:

(i) $d \mid a$ und $d \mid b$.

(ii) Gilt $t \mid a$ und $t \mid b$, so ist $t \leq d$.

Ist $ggT(a, b) = 1$, so heißen a und b **teilerfremd**. In der Tat sind dann $+1$ und -1 die einzigen gemeinsamen Teiler von a und b.

2.4 Satz: Seien a und b nicht beide 0 und $d = ggT(a, b)$. Dann gilt:

(a) d ist die kleinste positive Zahl der Form $ax + by$.

(b) Ist $ggT(a, b) = 1$, so gibt es Zahlen x und y mit

$$ax + by = 1.$$

(c) Ist t gemeinsamer Teiler von a und b, so ist t ein Teiler von d.

Beweis: $M_+ = \{ax + by \mid x, y \text{ ganz und } ax + by > 0\}$ ist nicht leer, da $a^2 + b^2 \in M_+$. Sei $\delta = \text{Min}M_+$. Zeige zunächst:

(1) $\delta \mid a$ und $\delta \mid b$.

(2) Aus $t \mid a$ und $t \mid b$ folgt $t \mid \delta$.

Sei $\delta = ax + by$.

Zu (1): Dividiere a durch δ mit Rest, dann erhält man $a = q\delta + r$ mit $0 \leq r < \delta$. Folglich gilt $r = a - q\delta = a - q(ax + by) = a(1 - qx) + b(-qy) = ax' + by'$. Es folgt $r = 0$, da $\delta = \text{Min}M_+$, und daher gilt $a = q\delta$, d.h. $\delta \mid a$. Analog zeigt man, dass auch $\delta \mid b$ gilt.

Zu (2): $t \mid a$ und $t \mid b$, daher gilt nach 2.1 $t \mid ax + by = \delta$.
Speziell gilt (2) für $t = d$, so dass $d \mid \delta$. Folglich ist dann $d \leq \delta$. Nach (1) ist δ gemeinsamer Teiler von a und b, somit $\delta \leq d$. Es folgt $d = \delta$, und (a) ist bewiesen.
(b) folgt aus (a).
Wegen (2) und $\delta = d$ gilt auch (c).

2.5 Regeln für den größten gemeinsamen Teiler. Sei $a \neq 0$.

(a) $1 \leq ggT(a, b) \leq \text{Min}(|a|, |b|)$, falls auch $b \neq 0$ (folgt aus 2.3)

(b) $ggT(a, 1) = 1$ (folgt aus (a))

(c) $ggT(a, 0) = |a|, ggT(-a, b) = ggT(a, b) = ggT(b, a)$ (klar)

(d) Für $c > 0$ ist $ggT(ac, bc) = c \cdot ggT(a, b)$

(e) $ggT\left(\frac{a}{ggT(a,b)}, \frac{b}{ggT(a,b)}\right) = 1$

(f) $ggT(a, b + ax) = ggT(a, b)$ für alle x

(g) Aus $b \mid a$ folgt $ggT(a,b) = |b|$

(h) Aus $a \mid bc$ und $ggT(a,b) = 1$ folgt $a \mid c$

Beweis:

(d) Sei $d = ggT(a,b)$, dann gilt $d \mid a$ und $d \mid b$. Folglich gilt dann auch $dc \mid ac$ und $dc \mid bc$. Nach 2.4 gilt daher $dc \mid ggT(ac,bc) =: \delta$.

Ferner folgt nach 2.4 aus $c \mid ac$ und $c \mid bc$, dass $c \mid \delta$ und schließlich auch $\frac{\delta}{c}$ ist ganz. Es folgt: $\delta \mid ac$ und daher gilt $\frac{\delta}{c} \mid a$ und wegen $\delta \mid bc$ gilt $\frac{\delta}{c} \mid b$.

Aus $\frac{\delta}{c} \mid a$ und $\frac{\delta}{c} \mid b$ folgt nach 2.4 $\frac{\delta}{c} \mid d$ und daher auch $\delta \mid dc$.

Wegen $dc \mid \delta$ und $\delta \mid dc$ gilt $dc = \delta$.

(e)
$$\begin{aligned} ggT(a,b) &= ggT\left(\tfrac{a}{ggT(a,b)} \cdot ggT(a,b), \tfrac{b}{ggT(a,b)} \cdot ggT(a,b)\right) \\ &\overset{d)}{=} ggT(a,b) \cdot ggT\left(\tfrac{a}{ggT(a,b)}, \tfrac{b}{ggT(a,b)}\right). \end{aligned}$$

Kürzen ergibt die Behauptung.

(f) Aus $t \mid a$ und $t \mid b$ folgt nach 2.1 $t \mid a$ und $t \mid b + ax$. Erneut folgt nach 2.1 $t \mid a$ und $t \mid (b + ax) - ax = b$. Also haben die Paare a, b und $a, b + ax$ die gleichen gemeinsamen Teiler und daher gilt folglich $ggT(a,b) = ggT(a, b + ax)$.

(g) Da $a = bq$ gilt $ggT(a,b) = ggT(bq, b \cdot 1) \overset{c),d)}{=} |b| ggT(q,1) \overset{b)}{=} |b|$.

(h) Für $c = 0$ gilt $a \mid c$. Für $c \neq 0$ gilt $a \mid ac$ und nach Voraussetzung gilt $a \mid bc$. Daher gilt $a \mid ggT(ac,bc)$. Da $ggT(ac,bc) = |c| \cdot ggT(a,b) = |c|$ und $a \mid ggT(ac,bc)$, gilt folglich $a \mid c$.

§3 Primzahlen

Die Zahl 1 hat nur einen positiven Teiler, nämlich 1. Jede Zahl $a > 1$ hat mindestens zwei positive Teiler: 1 und a.

Definition: Eine **Primzahl** ist eine Zahl $a > 1$, welche nur die Teiler 1 und a hat.

Im Folgenden ist der Buchstabe p den Primzahlen vorbehalten; ebenso bedeuten $p_1, p_2, \ldots$ oder $p', p'_j, p''_j, \ldots$ stets Primzahlen.

3.1 Satz: Jedes $a > 1$ ist als Produkt von Primzahlen darstellbar (Primfaktorzerlegung von a):

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_r = \prod_{n=1}^{r} p_n, r \geq 1$$

Beweis: Für $a = p$ ist die Aussage offenbar wahr. Wir beweisen 3.1 durch vollständige Induktion nach a.

Induktionsbeginn: $a = 2$ ist eine Primzahl.

Induktionsannahme: Sei $a \geq 3$ und 3.1 bereits bewiesen für alle b mit $1 < b < a$.

Induktionsschluss: Ist a eine Primzahl, so ist 3.1 richtig für a. Sonst gibt es eine Zerlegung $a = a_1 a_2$ mit $1 < a_1 < a$ und $1 < a_2 < a$.
Nach Induktionsannahme haben a_1 und a_2 eine Primfaktorzerlegung; also gilt dies auch für $a = a_1 a_2$.

3.2 Satz: (Euklid) Es gibt unendlich viele Primzahlen.

Beweis: Es ist zu zeigen: Zu jeder endlichen Menge von Primzahlen kann man eine weitere Primzahl finden. Seien also $r \geq 1$ paarweise verschiedene Primzahlen $p_1, \ldots, p_r$ vorgegeben.
Setze

$$a := 1 + p_1 \cdot \ldots \cdot p_r$$

Dann ist $a > 1$ und $p_1, \ldots, p_r$ sind keine Teiler von a (denn sonst wäre etwa p_i ein Teiler von $1 = a - p_1 \cdot \ldots \cdot p_r$, Widerspruch). Nach 3.1 ist aber a durch wenigstens eine Primzahl p teilbar. Diese kommt in der Menge $\{p_1, \ldots, p_r\}$ nicht vor.

3.3 Regeln:

(a) Aus $p \nmid a$ folgt: $ggT(p, a) = 1$.

(b) Aus $p \mid ab$ folgt: $p \mid a$ oder $p \mid b$.

(c) Für $q > 1$ gelte: Aus $q \mid ab$ folgt $q \mid a$ oder $q \mid b$. Dann ist q eine Primzahl.

(d) Aus $p \mid \prod_{n=1}^{r} a_n$ folgt: $p \mid a_n$ für mindestens ein n.

(e) Aus $p \mid \prod_{n=1}^{r} p_n$ folgt: $p = p_n$ für mindestens ein n.

Beweis:

(a) p hat nur die positiven Teiler 1 und p und $p \nmid a$. Es folgt $ggT(p, a) = 1$.

(b) Für den Fall $p \nmid a$ gilt nach (a) $ggT(p, a) = 1$. Ferner gilt aber auch $p \mid ab$ und daher gilt folglich nach 2.5 (h) $p \mid b$. Für $p \nmid b$ schließt man analog.

(c) Ist $q > 1$ keine Primzahl, so schreibt sich q nach 3.1 in der Form $q = pr$, p Primzahl, $r \geq 2$. Also ist $q \mid q = pr$ und $q > p$, $q > r$. Es folgt $q \nmid p$ und $q \nmid r$.

(d) folgt aus (b) durch Induktion.

(e) Aus $p \mid \prod_{n=1}^{r} p_n$ folgt nach (d) $p \mid p_n$ für ein n. Daher ist also $p = p_n$, da $p \neq 1$ und 1 und p_n die einzigen positiven Teiler von p_n sind.

Der größte gemeinsame Teiler von mehr als zwei Zahlen:

Bemerkung: Sind die Zahlen $a_1, \ldots, a_r (r \geq 1)$ nicht alle 0, so wird ihr größter gemeinsamer Teiler mit $ggT(a_1, \ldots, a_r)$ bezeichnet. $\delta = ggT(a_1, \ldots, a_r)$ ist also die größte Zahl mit $\delta \mid a_1, \ldots, \delta \mid a_{r-1}$ und $\delta \mid a_r$.

3.4 Satz: Seien $a_1 > 0, \ldots, a_r > 0, r \geq 2$. Dann gilt

(a) $ggT(a_1, \ldots, a_r) = ggT(ggT(a_1, \ldots, a_{r-1}), a_r)$.

(b) Jeder gemeinsame Teiler von $a_1, \ldots, a_r$ teilt $ggT(a_1, \ldots, a_r)$.

Beweis durch Induktion nach r:

Induktionsbeginn: Für $r = 2$ ist (a) trivial und (b) gilt nach 2.4.

Induktionsannahme: Sei $r \geq 3$, (a) und (b) bewiesen für alle k mit $2 \leq k \leq r-1$.

Induktionsschluss: Ist t gemeinsamer Teiler von $a_1, \ldots, a_r$, so auch von $a_1, \ldots, a_{r-1}$. Nach Induktionsannahme (b) ist daher t ein Teiler von $ggT(a_1, \ldots, a_{r-1}) = a'$. Ferner gilt $t \mid a_r$. Nach 2.4 ist daher $t \mid ggT(a', a_r) = ggT(ggT(a_1, \ldots, a_{r-1}), a_r)$. Setze $\delta := ggT(ggT(a_1, \ldots, a_{r-1}), a_r)$. Wegen $t \mid \delta$ ist $t \leq \delta$. Ferner gilt: $\delta \mid ggT(a_1, \ldots, a_{r-1})$ und $\delta \mid a_r$ und daher $\delta \mid a_1, \ldots, \delta \mid a_{r-1}$ und $\delta \mid a_r$, d.h.: δ ist gemeinsamer Teiler von $a_1, \ldots, a_r$. Damit ist gezeigt, dass δ der größte gemeinsame Teiler von $a_1, \ldots, a_r$ ist, und (a) ist bewiesen.
Im Beweis haben wir gesehen, dass jeder gemeinsame Teiler t von $a_1, \ldots, a_r$ auch δ teilt. Damit ist auch (b) bewiesen.

§4 Kongruenzrechnung

Sei $m > 0$ fest vorgegeben. Nach §2 wissen wir: Jede Zahl a lässt sich auf eindeutige Weise durch m mit Rest dividieren, d.h.: Es gibt genau ein Zahlenpaar q, r mit der Eigenschaft

$$(*) \quad a = qm + r, 0 \leq r < m$$

Definition: Zwei Zahlen heißen **kongruent modulo m**, wenn sie bei der Division durch m den gleichen Rest lassen.
Schreibe für „a ist kongruent zu b modulo m“ kurz

$$a \equiv b \bmod m.$$

Wenn klar ist, welches m gemeint ist auch: $a \equiv b$.
$a \not\equiv b \bmod m$ bedeutet, dass a und b nicht kongruent modulo m (oder „inkongruent modulo m“) sind.

Offenbar gilt

4.1 Bemerkung: „Kongruenz modulo m“ ist eine Äquivalenzrelation, d.h.

(a) $a \equiv a \bmod m$ (Reflexivität)

(b) Aus $a \equiv b \bmod m$ folgt $b \equiv a \bmod m$ (Symmetrie)

(c) Aus $a \equiv b \bmod m$ und $b \equiv c \bmod m$ folgt $a \equiv c \bmod m$ (Transitivität)

4.2 Bemerkung: Genau dann ist $a \equiv b \bmod m$, wenn m ein Teiler von $a - b$ ist.

Beweis: Sei $a = qm + r, 0 \leq r < m$.
„$\Longrightarrow$“ Wegen $a \equiv b \bmod m$ gilt $b = q'm + r$. Daher ist $a - b = (q - q')m$ und damit gilt $m \mid a - b$.
„$\Longleftarrow$“ Aus $m \mid a - b$ folgt $a - b = vm$. Daher ist $b = a - vm = (q - v)m + r$ und folglich gilt dann $a \equiv b \bmod m$.

Die möglichen Divisionsreste modulo m sind die m Zahlen $0, 1, \ldots, m - 1$. Wir können also die ganzen Zahlen nach ihren Divisionsresten in m Klassen einteilen:

Definition: Die **Restklasse von a modulo m** besteht aus allen Zahlen, welche modulo m den gleichen Divisionsrest haben wie a. Demnach gibt es genau m verschiedene Restklassen modulo m und verschiedene Klassen haben keine Elemente gemeinsam.

$$\begin{array}{lcl}
\text{Rest } 0 \text{ haben} & : & 0, \pm m, \pm 2m, \pm 3m, \ldots \\
\text{Rest } 1 \text{ haben} & : & 1, 1 \pm m, 1 \pm 2m, 1 \pm 3m, \ldots \\
\vdots & & \\
\text{Rest } r \text{ haben} & : & r, r \pm m, r \pm 2m, r \pm 3m, \ldots \text{ (für } 0 \leq r < m) \\
\vdots & & \\
\text{Rest } m-1 \text{ haben} & : & m-1, m-1 \pm m, m-1 \pm 2m, m-1 \pm 3m, \ldots
\end{array}$$

Definitionsgemäß gehören a und b zur gleichen Restklasse modulo m, wenn $a \equiv b \bmod m$.
Man spricht daher auch von **Kongruenzklassen modulo m** anstelle von Restklassen modulo m.
Nach 4.2 gilt: $a \equiv b \bmod m$ genau dann, wenn $m \mid a - b$, d.h.
es gibt ein $q \in \mathbb{Z}$ mit $b = a + qm$.

Damit gilt

4.3 Bemerkung: Die Restklasse von a modulo m ist die Menge

$$\{a + mq \mid q \in \mathbb{Z}\}.$$

Schreibe dafür auch $a + m\mathbb{Z}$ oder $a + (m)$.
Wir haben gesehen:

(1) Es gibt genau m verschiedene Restklassen modulo m.

(2) Jede Zahl gehört zu genau einer Restklasse modulo m.

Die Aussagen (1) und (2) zusammengenommen kann man auch so ausdrücken: Die Menge aller ganzen Zahlen ist die disjunkte Vereinigung der verschiedenen Restklassen modulo m.

Definition: Eine Menge von Zahlen $a_1, \ldots, a_m$ heißt **vollständiges Repräsentantensystem** (Restsystem) **modulo m** , wenn $a_1+(m), a_2+(m), \ldots$, $a_m + (m)$ gerade die m verschiedenen Restklassen modulo m sind, d.h. wenn

$$a_i \not\equiv a_j \bmod m, \text{ falls } i \neq j.$$

Beispiel: $0, 1, 2, \ldots, m-1$ ist ein vollständiges Repräsentantensystem modulo m. (Diese Zahlen sind selbst Divisionsreste und voneinander verschieden.)

4.4 Satz:

(a) Ist $a_1, \ldots, a_m$ ein vollständiges Restsystem modulo m, so gilt dies auch für $a_1 + c, \ldots, a_m + c$ ($c \in \mathbb{Z}$). Insbesondere gilt nach dem Beispiel: Je m aufeinander folgende Zahlen bilden ein vollständiges Restsystem modulo m. Ein solches System mit − dem Betrag nach − möglichst kleinen Elementen ist die Menge der ganzen Zahlen größer als $-\frac{m}{2}$ und kleiner oder gleich $+\frac{m}{2}$.

Für ungerades m sind dies die Zahlen

$$-\frac{m-1}{2}, -\frac{m-1}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2}$$

und für gerade m die Zahlen

$$-\frac{m}{2}+1, -\frac{m}{2}+2, \ldots, -1, 0, 1, \ldots, \frac{m}{2}$$

$m = 7 : -3, -2, -1, 0, 1, 2, 3$
$m = 8 : -3, -2, -1, 0, 1, 2, 3, 4$

(b) Ist $a_1, \ldots, a_m$ ein vollständiges Restsystem modulo m und ist $ggT(k, m) = 1$, so ist auch $a_1k, a_2k, \ldots, a_mk$ ein vollständiges Restsystem modulo m.

Beweis:

(a) Für $i \neq j$ ist $a_i \not\equiv a_j \bmod m$, also $m \nmid (a_i - a_j) = (a_i + c) - (a_j + c)$. Nach 4.2 folgt daraus $(a_i + c) \not\equiv (a_j + c) \bmod m$.

(b) Aus $a_ik \equiv a_jk \bmod m$ folgt $m \mid (a_ik - a_jk) = (a_i - a_j)k$, also $m \mid (a_i - a_j)k$ und $ggT(m, k) = 1$. Nach 2.5 (h) gilt daher $m \mid (a_i - a_j)$, d.h. $a_i \equiv a_j \bmod m$. Nach Voraussetzung ist dann $i = j$.

Im folgenden sei $m > 0$ fest vorgegeben, und „$a \equiv b$“ bedeutet immer $a \equiv b \bmod m$. Es soll gezeigt werden, dass man mit „ ≡ “ **wie mit einem Gleichheitszeichen** umgehen darf.

4.5 Satz:

(a) Aus $a \equiv b$ folgt $a \pm c \equiv b \pm c$.

(b) Aus $a \equiv b$ folgt $ac \equiv bc$.

(c) Aus $a \equiv b$ folgt $a^n \equiv b^n$ für alle $n \in \mathbb{N}$.

(d) Ist $f(x) = c_0 + c_1 x + \ldots + c_n x^n$ eine Polynomfunktion in der Variablen x, so folgt aus $a \equiv b$ schon $f(a) \equiv f(b)$.

Beweis:

(a) Wegen $a \equiv b$ gilt $m \mid (a-b) = (a \overset{+}{(-)} c) - (b \overset{+}{(-)} c)$ und daraus folgt $a \overset{+}{(-)} c \equiv b \overset{+}{(-)} c$.

(b) Da $a \equiv b$ gilt $m \mid a - b$, ferner gilt dann $m \mid (a-b)c = ac - bc$. Also gilt schließlich $ac \equiv bc$.

(c) (Induktion nach n) $n = 0 : a^0 = 1 \equiv 1 = b^0$
Induktionsannahmne: Sei $n \geq 1$ und $a^{n-1} \equiv b^{n-1}$ schon bewiesen.
Mit (b) folgt $a^n = a^{n-1}a \overset{(b)}{\equiv} a^{n-1}b \equiv b^{n-1}b = b^n$.

(d) Sei $a \equiv b$. Nach (b) und (c) gilt: $c_v a^v \equiv c_v b^v, v = 0, \ldots, n$
Induktion nach n: $n = 0 : f(x) = c_0$ für alle x und daraus folgt $f(a) = c_0 = f(b)$. Sei $n \geq 1$ und $c_0 + c_1 a + \ldots + c_{n-1}a^{n-1} \equiv c_0 + c_1 b + \ldots + c_{n-1}b^{n-1}$ schon gezeigt. Nach (a) gilt dann

$$\begin{aligned} f(a) &= (c_0 + c_1 a + \ldots + c_{n-1}a^{n-1}) + c_n a^n \\ &\equiv (c_0 + c_1 b + \ldots + c_{n-1}b^{n-1}) + c_n a^n \\ &\equiv (c_0 + c_1 b + \ldots + c_{n-1}b^{n-1}) + c_n b^n \\ &= f(b). \end{aligned}$$

4.6 Satz: Sei $c > 0$ und a, b beliebig.

(a) Wenn $ac \equiv bc \bmod m$ und $ggT(c, m) = 1$, dann gilt $a \equiv b \bmod m$.

(b) $a \equiv b \bmod m$ gilt genau dann, wenn $ac \equiv bc \bmod cm$ gilt.

(c) Aus $a \equiv b \bmod m$, $n \mid m$ und $n > 0$ folgt $a \equiv b \bmod n$.

(d) Gilt $a \equiv b \bmod m$, dann gilt auch $ggT(a, m) = ggT(b, m)$.

Beweis:

(a) Wegen $m \mid (ac - bc) = (a-b)c$ und $ggT(c, m) = 1$ gilt nach 2.5 (h) $m \mid a - b$ und daher gilt $a \equiv b \bmod m$.

(b) $m \mid (a-b)$ genau dann, wenn $cm \mid c(a-b) = ac - bc$. $cm \mid ac - bc$ gilt wiederum genau dann, wenn $ac \equiv bc \bmod cm$.

(c) Aus $m \mid (a-b)$ und $n \mid m$ folgt $n \mid (a-b)$, daher gilt dann auch $a \equiv b \mod n$.

(d) Da $b = a + mq$, gilt nach 2.8 (f) $ggT(b, m) = ggT(a + mq, m) = ggT(a, m)$.

§5 Der kleine Satz von Fermat

Polynomkongruenz modulo p. Sei p eine Primzahl, $n \geq 0$ und $c_0, \ldots, c_n \in \mathbb{Z}$. Wir betrachten die Kongruenz

$$(*) \qquad c_0 + c_1 X + \ldots + c_{n-1} X^{n-1} + c_n X^n \equiv 0 \bmod p$$

d.h.: Wir suchen alle $x \in \mathbb{Z}$ mit der Eigenschaft

$$c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} + c_n x^n \equiv 0 \bmod p$$

Diese Zahlen nennt man die Lösungen von $(*)$. Nach 4.5 gilt:

(1) Die Lösungsmenge ändert sich nicht, wenn man in $(*)$ die Koeffizienten $c_0, \ldots, c_n$ ersetzt durch $c_0', \ldots, c_n'$ mit $c_i \equiv c_i' \bmod p$.

(2) Mit einer Lösung x_0 von $(*)$ ist auch jedes y mit $y \equiv x_0 \bmod p$ eine Lösung von $(*)$. Also ist die Lösungsmenge von $(*)$ die Vereinigung von vollen Restklassen modulo p. Daher erklärt man:

Definition: Die Anzahl der Lösungen von $(*)$ ist die Anzahl der Restklassen modulo p, deren Elemente $(*)$ lösen. (Diese ist auch gleich der Anzahl der Lösungen x_0 mit $0 \leq x_0 < p$.)

5.1 Satz: Ist p kein Teiler von c_n, so hat $(*)$ höchstens n Lösungen.

Beweis durch vollständige Induktion:

Induktionsbeginn: Für $n = 0$ ist dies klar.

Induktionsannahme: 5.1 ist richtig für $n - 1$.

Induktionsschluß von n-1 auf n: Angenommen $(*)$ habe $n+1$ paarweise inkongruente Lösungen $x_0, x_1, \ldots, x_n$. Setzte für $x \in \mathbb{Z}$
$f(x) := c_0 + c_1 x + \ldots + c_n x^n$. Es gilt dann

$$\begin{aligned} f(x) - f(x_0) &= c_1(x - x_0) + \ldots + c_n(x^n - x_0^n) \\ &= (x - x_0)\left(\sum_{i=1}^{n} c_i(x^{i-1} + x_0 x^{i-2} + \ldots + x_0^{i-2} x + x_0^{i-1})\right) \\ &= (x - x_0) g(x), \end{aligned}$$

wobei $g(X)$ ein Polynom der Form

$$g(X) = b_0 + b_1X + \ldots + b_{n-1}X^{n-1} \text{ ist mit } b_{n-1} = c_n, p \nmid b_{n-1}.$$

Speziell gilt für $X = x_k, k = 1, \ldots, n$:
$(x_k - x_0)g(x_k) = f(x_k) - f(x_0) \equiv 0 - 0 \equiv 0 \bmod p$, und nach der Annahme ist $(x_k - x_0) \not\equiv 0 \bmod p$. Also gilt $p \mid (x_k - x_0)g(x_k), p \nmid x_k - x_0$ und daraus folgt, dass $p \mid g(x_k)$, d.h. die Kongruenz

$$g(X) \equiv 0 \bmod p$$

hat n paarweise inkongruente Lösungen $x_1, \ldots, x_n$. Dies widerspricht der Induktionsannahme. Also ist die Annahme falsch, dass $(*)$ $n + 1$ inkongruente Lösungen hat.

Defintion: Die zahlentheoretische Funktion

$$\begin{array}{rcl} \varphi : \mathbb{N}\backslash\{0\} & \to & \mathbb{N}\backslash\{0\} \\ m & \mapsto & \text{Anzahl der zu } m \text{ teilerfremden Zahlen } b \text{ mit } 1 \leq b \leq m \end{array}$$

heißt **Eulersche φ-Funktion.**

Definition: Ein **reduziertes Restsystem modulo m** ist ein System von $\varphi(m)$ paarweise inkongruenten Zahlen mod m, welche zu m teilerfremd sind. Man erhält es aus einem vollständigen Restsystem modulo m, indem man alle Zahlen weglässt, die mit m einen Teiler $t > 1$ gemeinsam haben.

5.2 Bemerkung: Ist $a_1, \ldots, a_{\varphi(m)}$ ein reduziertes Restsystem mod m und ist $ggT(a, m) = 1$, so ist auch $a_1a, \ldots, a_{\varphi(m)}a$ ein solches. Dies ergibt sich sofort aus 4.6.

5.3 Der kleine Satz von Fermat: Sei $m > 1$. Dann gilt $ggT(a, m) = 1$ genau dann, wenn $a^{\varphi(m)} \equiv 1 \bmod m$.

Beweis: „$\Longleftarrow$“: Sei $a^{\varphi(m)} \equiv 1 \bmod m$. Nach 4.6 ist dann $1 = ggT(1, m) = ggT(a^{\varphi(m)}, m)$, also auch $ggT(a, m) = 1$.
„$\Longrightarrow$“: Sei $ggT(a, m) = 1$ und $a_1, \ldots, a_{\varphi(m)}$ ein reduziertes Restsystem mod m. Dann ist nach 5.2 auch $aa_1, \ldots, aa_{\varphi(m)}$ ein solches.
Nach 4.6 folgt: $\prod_{n=1}^{\varphi(m)}(aa_n) \equiv \prod_{n=1}^{\varphi(m)} a_n \bmod m$, also $a^{\varphi(m)} \prod_{n=1}^{\varphi(m)} a_n \equiv 1 \cdot \prod_{n=1}^{\varphi(m)} a_n \bmod m$. Kürzen ergibt $a^{\varphi(m)} \equiv 1 \bmod m$. (Kürzen ist nach 4.6 wegen $ggT(a_1 \cdot \ldots \cdot a_{\varphi(m)}, m) = 1$ erlaubt.)

Mit $\varphi(p) = p - 1$ ergibt sich:

5.4 Korollar: Für $p \nmid a$ ist $a^{p-1} \equiv 1 \bmod p$. Also gilt

$$a^p \equiv a \bmod p \text{ für jedes } a \in \mathbb{Z}.$$

5.5 Satz: Sei d ein positiver Teiler von $p-1$. Dann hat die Kongruenz $X^d \equiv 1 \bmod p$ genau d Lösungen.

Beweis: Sei $e \in \mathbb{N}$ mit $de = p - 1$. Nach der Formel für die geometrische Reihe ist

$$X^{p-1} - 1 = (X^d - 1)\left(1 + X^d + (X^d)^2 + \ldots + (X^d)^{e-1}\right) = (X^d - 1)g(X)$$

Wegen $(X^d)^{e-1} = X^{d(e-1)}$ ist $g(X)$ ein Polynom vom Grad $d(e-1)$. Es folgt

(1) $g(X) \equiv 0 \bmod p$ hat **höchstens** $d(e-1)$ Lösungen (5.1).

(2) $X^{p-1} - 1 \equiv 0 \bmod p$ hat **genau** $\varphi(p) = p - 1$ Lösungen (5.3).

a löst $X^{p-1} - 1 \equiv 0 \bmod p$. Daraus folgt $p \mid a^{p-1} - 1 = (a^d - 1)g(a)$ und daher gilt entweder $p \mid a^d - 1$ oder $p \mid g(a)$. Folglich löst a entweder $X^d - 1 \equiv 0 \bmod p$ oder a löst $g(x) \equiv 0 \bmod p$. Also gilt

(3) a ist Lösung von $X^{p-1} - 1 \equiv 0 \bmod p$. Daher ist a Lösung von $g(X) \equiv 0 \bmod p$ oder von $X^d - 1 \equiv 0 \bmod p$.

Aus (1) und (3) folgt: $X^d - 1 \equiv 0 \bmod p$ hat **mindestens** $p - 1 - d(e-1)$ Lösungen. Aber $p - 1 - d(e-1) = d$ und nach 5.1 gilt auch

(4) $X^d - 1 \equiv 0 \bmod p$ hat **höchstens** d Lösungen.

5.6 Korollar: Sei $p \geq 3$. Dann hat $X^{\frac{p-1}{2}} \equiv 1 \bmod p$ genau $\frac{p-1}{2}$ Lösungen, nämlich die Restklassen von $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.

Beweis: $(a^2)^{\frac{p-1}{2}} \equiv a^{p-1} \equiv 1 \bmod p$ für $a \not\equiv 0 \bmod p$ nach 5.3. Nach 5.5 ist noch zu zeigen: $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ sind paarweise inkongruent modulo p.

Angenommen es existieren a, b mit $1 \leq a < b \leq \frac{p-1}{2}$ mit $a^2 \equiv b^2 \bmod p$. Dann ist $(p-a)^2 \equiv (-a)^2 \equiv a^2 \bmod p$ und die Kongruenz $X^2 \equiv a^2 \bmod p$ hat die drei Lösungen a, b und $p - a$, wobei

$$p > p - a \geq p - \frac{p-1}{2} = \frac{p+1}{2} > b > a \geq 1,$$

im Widerspruch zu 5.1.

5.7 Korollar: Sei $p \geq 3$. Die Kongruenz $X^2 \equiv -1 \bmod p$ hat eine Lösung (das ist ein x mit $p \mid x^2 + 1$), wenn $p \equiv 1 \bmod 4$ und keine Lösung, wenn $p \equiv 3 \bmod 4$.

Beweis: Ist $a^2 \equiv -1 \bmod p$, so ist nach 5.3

$$(-1)^{\frac{p-1}{2}} \equiv a^{p-1} \equiv 1 \bmod p.$$

Dann muss $(-1)^{\frac{p-1}{2}} = 1$ sein, da $-1 \not\equiv 1 \bmod p$ für $p \geq 3$. Es folgt: $\frac{p-1}{2}$ ist gerade, d.h. $4 \mid p-1$, d.h. $p \equiv 1 \bmod 4$. Ist umgekehrt $p \equiv 1 \bmod 4$, so ist $(-1)^{\frac{p-1}{2}} \equiv 1 \bmod p$ und daher $-1 \equiv a^2 \bmod p$ mit $1 \leq a \leq \frac{p-1}{2}$ nach 5.6.

§6 Ringe und Körper

Für das Rechnen in $\mathbb{Z}$ haben wir in Kapitel II, §1 Regeln aufgestellt, welche auch in $\mathbb{Q}$ und $\mathbb{R}$ gelten. Damit werden $\mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ zu **Ringen** im folgenden Sinne:

Sei R eine Menge, auf der zwei Verknüpfungen, $+$ („plus“, Addition) und $\cdot$ („mal“, Multiplikation), erklärt sind.

Definition: R, zusammen mit den Operationen $+$ und $\cdot$, (kurz „$(R, +, \cdot)$“) heißt ein **Ring**, wenn Addition und Multiplikation den folgenden sechs Axiomen genügen:

Addition „+“	**Multiplikation „$\cdot$“**

1. Eindeutige Ausführbarkeit

Zu je zwei Elementen $a, b \in R$ existiert in R in eindeutiger Weise

die Summe $a + b$	das Produkt $a \cdot b$

Für $a, b, c \in R$ gelten die folgenden Gesetze:

2. Assoziativgesetze

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

3. Kommutativgesetze

$a + b = b + a$	$a \cdot b = b \cdot a$

4. Existenz neutraler Elemente

Es gib ein Element $n \in R$, so dass für jedes $a \in R$ gilt:	Es gibt ein Element $e \in R$, so dass für jedes $a \in R$ gilt:
$a + n = a$	$a \cdot e = a$

Es ist $e \neq n$.

Bezeichnung: n nennt man Nullelement und e Einselement des Rings R.

Bemerkung: Sind 3. und 4. erfüllt, so hat R genau ein Nullelement und genau ein Einselement. Wir bezeichnen diese (wie in $\mathbb{Z}$) mit 0 („Null“) und 1 („Eins“).

Beweis: Sind n und $\tilde{n}$ Nullelemente, so gilt wegen 3. und 4. $\tilde{n} = \tilde{n} + n = n + \tilde{n} = n$. Entsprechend schließt man für Einselemente.

5. Umkehrung der Addition
Zu jedem $a \in R$ gibt es ein Element $a' \in R$, so dass gilt

$$a + a' = 0$$

a' heißt ein **Negatives** von a

Bemerkung: Zu jedem a gibt es genau ein Negatives. Wir bezeichnen es mit $-a$.
Schreibe für $a + (-b)$ auch $a - b$ und nenne $a - b$ die **Differenz** zwischen a und b.

Beweis: Seien a' und $\tilde{a}$ Negative von a. Dann gilt $a + a' = 0 = a + \tilde{a}$. Daraus folgt $\tilde{a} = \tilde{a} + 0 = \tilde{a} + (a + a') = (\tilde{a} + a) + a' = (a + \tilde{a}) + a' = 0 + a' = a' + 0 = a'$.

6. Das Distributivgesetz

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

für alle $a, b, c \in R$.
Zur Vereinfachung der Schreibweise führen wir folgende **Konventionen** ein:
Schreibe ab für $a \cdot b$.
Punktrechnung geht vor Strichrechnung, d.h.

$$\begin{aligned} ab + c &:= (a \cdot b) + c, \\ a + bc &:= a + (b \cdot c). \end{aligned}$$

Damit schreibt sich das Distributivgesetz in der Form

$$(a + b)c = ac + bc.$$

Bei mehrfachen Summen bzw. Produkten werden Klammern weggelassen (weil es wegen der Assoziativgesetze nicht auf die Art der Klammerung ankommt.) Also

$$a + b + c := (a + b) + c, abc := (a \cdot b) \cdot c \text{ usw.}$$

Definition: Ein Ring R heißt **Integritätsbereich**, wenn zusätzlich gilt:

7. Nullteilerfreiheit: Aus $ab = 0$ folgt $a = 0$ oder $b = 0$.

Definition: Ein Ring heißt **Körper**, wenn zusätzlich zu den Axiomen 1 bis 6 noch gilt:

8. Umkehrbarkeit der Multiplikation: Zu jedem $a \neq 0$ aus R gibt es ein Element $\tilde{a}$ mit $a\tilde{a} = 1$.

Bemerkung: In einem Körper gibt es zu jedem $a \in R, a \neq 0$ genau ein $\tilde{a} \in R$ mit $a\tilde{a} = 1$.

Wir bezeichnen dieses Element mit a^{-1} und nennen es das zu a **reziproke** Element (**Kehrwert** von a).

Beweis: $a\tilde{a} = 1 = a\tilde{\tilde{a}}$. Daraus folgt $\tilde{\tilde{a}} = \tilde{\tilde{a}} \cdot 1 = \tilde{\tilde{a}}a\tilde{a} = a\tilde{\tilde{a}}\tilde{a} = 1 \cdot \tilde{a} = \tilde{a} \cdot 1 = \tilde{a}$.

Wir schreiben für a^{-1} auch $\frac{1}{a}$ und für $b \cdot a^{-1}$ auch $\frac{b}{a}$.

Unterring: Sei R ein Ring und $S \subseteq R$ eine Teilmenge mit $1 \in S$. Man nennt S einen **Unterring von R**, wenn S abgeschlossen ist unter Addition, Multiplikation und der Bildung des Negativen, d.h.: Sind $a, b \in S$, so sind auch $-a, a + b$ und ab aus S. Offenbar ist jeder Unterring eines Rings selbst ein Ring.

§7 Die komplexen Zahlen

Wir betrachten eine Polynomgleichung

$$X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = 0$$

mit reellen Koeffizienten $a_0, a_1, \ldots, a_{n-1}, n \geq 2$. *Sie hat im Allgemeinen* **keine reelle Lösung** *, d.h. es gibt* **kein** $y \in \mathbb{R}$ *mit*

$$y^n + a_{n-1}y^{n-1} + \ldots + a_1y + a_0 = 0.$$

Um diesen Mangel zu beheben, haben Euler und Andere die **komplexen Zahlen** *erfunden. Sie bilden eine Erweiterung von* $\mathbb{R}$*, in der* **alle** *Gleichungen obigen Typs Lösungen haben. Die komplexen Zahlen werden mit* $\mathbb{C}$ *bezeichnet.*

Zum Beispiel ist die Gleichung $X^2 + 1 = 0$ *in* $\mathbb{R}$ *unlösbar und in* $\mathbb{C}$ *lösbar. Die Lösungen bezeichnet man gewöhnlich mit* i *und* $-i$. *Der Bereich* $\mathbb{C}$ *wird ein Körper sein, der* $\mathbb{R}$ *umfasst, „möglichst klein" ist und* i *enthält. Genauer wird gelten:* $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ *mit einer „imaginären" Größe* i*, welche die Bedingung* $i^2 = -1$ *erfüllt.*

Konstruktion von $\mathbb{C}$: Die Menge $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ der Paare reeller Zahlen bilden bekanntlich einen Vektorraum vermöge der Operationen

$$\begin{array}{ll} (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) & \text{(Vektoraddition)} \\ \lambda(x, y) = (\lambda x, \lambda y) \text{ für alle } \lambda \in \mathbb{R} & \text{(Skalarmultiplikation)} \end{array}$$

(i) Die dem Körper $\mathbb{C}$ zugrunde liegende Menge ist $\mathbb{R}^2$ („$\mathbb{C} = \mathbb{R}^2$").

(ii) Die **Addition** auf $\mathbb{C}$ ist die Vektoraddition auf $\mathbb{R}^2$.

(iii) Die **Multiplikation** von Elementen aus $\mathbb{C}$ ist erklärt durch

$$(x_1, y_1) \cdot (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

7.1 Bemerkung:

(1) $(\mathbb{C}, +)$ ist eine abelsche Gruppe (denn $(\mathbb{R}^2, +, \cdot)$ ist sogar ein Vektorraum).

(2) Die Multiplikation ist kommutativ und $(1, 0) \cdot (x, y) = (x, y)$, d.h. $1_{\mathbb{C}} := (1, 0)$ ist neutrales Element der Multiplikation.

(3) Für die Multiplikation gilt das Assoziativgesetz.

(4) Jedes $(x, y) \neq (0, 0)$ hat ein Inverses bezüglich der Multiplikation:

$$\left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}\right) \cdot (x, y) = (1, 0) = 1_{\mathbb{C}}$$

(5) Es gilt das Distributivgesetz in $\mathbb{C}$.

Mit anderen Worten bedeuten (1) bis (5): $\mathbb{C}$ ist ein Körper mit Eins = (1,0) und Null = (0,0).

Die Gültigkeit von (2), (3) und (5) prüft man leicht nach. Wir wollen noch $\mathbb{R}$ als einen Unterring von $\mathbb{C}$ auffassen:

„Einbettung" von $\mathbb{R}$ in $\mathbb{C}$. Die Abbildung

$$\varphi : \mathbb{R} \to \mathbb{C} = \mathbb{R}^2 \quad x \mapsto (x, 0)$$

ist injektiv. Sie ist mit Addition und Multiplikation verträglich, d.h.

$$\varphi(x + y) = \varphi(x) + \varphi(y) \text{ und } \varphi(x \cdot y) = \varphi(x)\varphi(y).$$

Wir identifizieren $x \in \mathbb{R}$ mit $(x, 0) \in \mathbb{C}$. Damit wird $\mathbb{R}$ zu einem Unterring von $\mathbb{C}$. Insbesondere ist dann $1 = (1, 0)$ und $0 = (0, 0)$:

$$\mathbb{R} \subsetneq \mathbb{C}, \quad x \hat{=} (x, 0) \text{ für } x \in \mathbb{R}$$

(6) $(0, 1)^2 = (0, 1) \cdot (0, 1) = (-1 \cdot 1, 0) = -(1, 0) = -1$
Setze nun $i = (0, 1)$. Dann gilt

(α) $i^2 + 1 = 0$, d.h. i löst die Gleichung $X^2 = 1$.

(β) Jedes $(x, y) \in \mathbb{C}$ schreibt sich eindeutig in der Form

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (0, 1)(y, 0) = x + iy; x, y \in \mathbb{R}.$$

Damit ist $\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$.

Ist $z = (x, y) = x + iy \in \mathbb{C}$ mit $x \in \mathbb{R}, y \in \mathbb{R}$, so heißt x der **Realteil** und y der **Imaginärteil** von z. Schreibe dafür $x = \mathrm{Re}z$ und $y = \mathrm{Im}z$.

z heißt **rein imaginär**, wenn Re $z = 0$, also $z = iy, y \in \mathbb{R}$.

Konjugation: Für $x, y \in \mathbb{R}$ heißt

$$\bar{z} := x - iy \text{ die zu } z = x + iy \textbf{ konjugierte} \text{ Zahl.}$$

Die Länge des Vektors (x, y) heißt **Betrag** der komplexen Zahl $z = x + iy$, d.h. nach Pythagoras

$$|z| := \sqrt{x^2 + y^2}, \text{ wenn } z = x + iy \text{ mit } x, y \in \mathbb{R}.$$

7.2 Regeln: Für komplexe Zahlen z und w gilt

a) $\overline{\bar{z}} = z$;

b) $\bar{z} = z$ genau dann, wenn $z \in \mathbb{R}$;

c) $\overline{z + w} = \bar{z} + \bar{w}, \overline{zw} = \bar{z} \cdot \bar{w}$;

d) $|z|^2 = z\bar{z}$;

e) Für $z \neq 0$ ist $z^{-1} = \frac{1}{|z|^2}\bar{z}$;

f) $|zw| = |z||w|$;

Beweis: a) und b) sind klar nach Definition.

c) Seien $z = (x, y)$ und $w = (u, v)$.
$\overline{z + w} = \overline{(x + u) + i(y + v)} = x + u - iy - iv = x - iy + u - iv = \bar{z} + \bar{w}$;
$\overline{zw} = \overline{(xu - yv) + i(xv + yu)} = (xu - yv) - i(xv + yu)$.
Ferner gilt $\bar{z}\bar{w} = (x - iy)(u - iv) = xu - i(xv + yu) + i^2yv = (xu - yv) - i(xv + yu) = \overline{zw}$;

d) $z\bar{z} = (x + iy)(x - iy) = x^2 - i^2y^2 = x^2 + y^2 = |z|^2$;

e) folgt aus d);

f) $|zw|^2 = (zw)\overline{zw} = (zw)(\bar{z}\bar{w}) = (z\bar{z}) \cdot w\bar{w} = |z|^2|w|^2$ nach den vorangegangenen Regeln.

Kapitel III.
Die Gleichung $X^n + Y^n = Z^n$

§1 Der Fall $n = 2$

1.1 Satz: (Pythagoras) In einem rechtwinkligem Dreieck (einem sogenannten Pythagoras-Dreieck) mit den Katheten x, y und der Hypothenuse z gilt

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

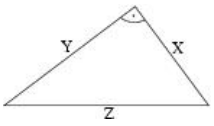

Abbildung 3: Pythagoras-Dreieck

Definition: Ein Tripel (x,y,z) aus positiven ganzen Zahlen, wobei $x^2 + y^2 = z^2$ wird Pythagoras-Tripel genannt. Zum Beispiel (3,4,5) mit $3^2 + 4^2 = 5^2$ stellt ein solches Tripel dar (Zimmermannsregel).

1.2 Bemerkung: Sei x, y, z ein Pythagoras-Tripel. Dann gilt:

(a) x und y sind nicht beide ungerade.

(b) Für alle $\lambda \geq 1$ aus $\mathbb{N}$ ist auch λx, λy, λz ein Pythagoras-Tripel.

(c) Teilt t die Zahlen x, y und z, so ist auch $\frac{x}{t}, \frac{y}{t}, \frac{z}{t}$ ein Pythagoras-Tripel.

Beweis:

(a) Angenommen x und y sind ungerade, dann gilt:

(i) Ist $x \equiv 1 \bmod 4$, so ist $x^2 \equiv 1 \bmod 4$.

(ii) Ist $x \equiv 3 \bmod 4$, so ist $x^2 \equiv 9 \equiv 1 \bmod 4$.

Also gilt $x^2 \equiv y^2 \equiv 1 \bmod 4$. Daher ist dann $x^2 + y^2 \equiv 2 \bmod 4$. Ferner gilt allgemein für eine gerade Zahl z:

(iii) Ist $z \equiv 2 \bmod 4$, so ist $z^2 \equiv 4 \equiv 0 \bmod 4$.

(iv) Ist $z \equiv 0 \bmod 4$, so ist $z^2 \equiv 0 \bmod 4$.

Daraus folgt $x^2 + y^2$ ist kein Quadrat. Dies ist ein Widerspruch zur Annahme, dass x, y, z ein Pythagoras-Tripel ist.

(b) und (c) sind offensichtlich richtig.

Demnach genügt es, diejenigen Pythagoras-Tripel zu finden mit

(i) x, y, z sind (paarweise) teilerfremd,

(ii) x ist gerade und y ungerade.

Die übrigen Pythagoras-Tripel entstehen aus solchen durch Streckung und evtl. Vertauschung von x und y.

1.3 Satz: (Indische Formeln für Pythagoras-Tripel)

(a) Sind $a \geq 1, b \geq 1$ mit $a > b, a - b$ ungerade und $ggT(a, b) = 1$, so bilden $x = 2ab, y = a^2 - b^2, z = a^2 + b^2$ ein Pythagoras-Tripel mit den Eigenschaften (i) und (ii) (ein sogenanntes „normiertes“ Pythagoras-Tripel).

(b) Jedes normierte Pythagoras-Tripel x, y, z ist von der Form $x = 2ab, y = a^2 - b^2, z = a^2 + b^2$ mit $a \geq 1, b \geq 1, a - b$ ungerade und $ggT(a, b) = 1$.

(c) Es gibt unendlich viele normierte Pythagoras-Tripel.

Beweis:

(a) Seien a, b, x, y, z wie in (a) beschrieben. Dann ist x gerade und

$$x^2 + y^2 = 4a^2b^2 + a^4 - 2a^2b^2 + b^4 = a^4 + 2a^2b^2 + b^4 = (a^2 + b^2)^2 = z^2$$

Wegen $a - b$ ungerade ist auch $a + b$ ungerade und daher ist $y = (a + b)(a - b)$ ungerade.

Noch zu zeigen: x und y sind teilerfremd.

Angenommen die Primzahl p teilt x und y, dann ist p ungerade und $p^2 \mid x^2 + y^2 = z^2$. Folglich gilt p ungerade und $p \mid z$. Daher gilt auch $p \mid y + z = 2a^2$ und $p \mid y - z = -2b^2$. Da p ungerade ist muss $p \mid a$ und $p \mid b$ gelten, im Widerspruch zu $ggT(a, b) = 1$.

(c) a durchlaufe alle ungeraden Primzahlen p und $b := 2$. Das Paar a, b erfüllt dann die Voraussetzung von (a).

Also ist nach (a) $4p, p^2 - 4, p^2 + 4$ ein normiertes Pythagoras-Tripel für alle Primzahlen $p \geq 3$.

(b) Sei x, y, z ein normiertes Pythagoras-Tripel, dann gilt $z^2 = x^2 + y^2$ ist ungerade und daher ist auch z ungerade; Da z und y ungerade sind, gilt $z \pm y$ ist gerade. Folglich gilt $x^2 = z^2 - y^2 = (z - y)(z + y) = 4x_0^2$. Somit gilt $x = 2x_0$, $x_0^2 = \frac{z-y}{2} \cdot \frac{z+y}{2}$, $x_0 \geq 1$.

Behauptung: $ggT\left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 1$

Beweis: Angenommen die Primzahl p teil $\frac{z \pm y}{2}$, dann gilt $p \mid \frac{z+y}{2} - \frac{z-y}{2} = y$ und $p^2 \mid (z - y)(z + y) = z^2 - y^2 = x^2$.
Es folgt $p \mid y$ und $p \mid x$, im Widerspruch zur Voraussetzung. Also ist $ggT\left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 1$ und $\frac{z-y}{2} \cdot \frac{z+y}{2} = x_0^2$ ist ein Quadrat. Somit gilt $\frac{z-y}{2} = b^2$, $\frac{z+y}{2} = a^2, a \geq 1, b \geq 1$.
Folglich ist $x_0^2 = a^2 b^2$ und damit ist $x_0 = ab$. Hieraus ergibt sich $x = 2x_0 = 2ab, y = \frac{z+y}{2} - \frac{z-y}{2} = a^2 - b^2, z = \frac{z+y}{2} + \frac{z-y}{2} = a^2 + b^2$. Daher gilt nun $ggT(a, b) \mid x$ und $ggT(a, b) \mid y$. Da $ggT(x, y) = 1$ gilt $ggT(a, b) = 1$.
Wegen $y = a^2 - b^2 = (a + b)(a - b)$ ungerade, ist auch $a - b$ ungerade.

Die nicht trivialen Lösungen von 1.1 nach dem steigenden Wert von z angeordnet sind:

$$(4, 3, 5), (12, 5, 13), (8, 15, 17), (24, 7, 25).$$

Eine nicht triviale, d.h. eine von Null verschiedene Lösung für 1.1 zu finden, läuft also darauf hinaus, herauszufinden, welche ungeraden ganzen Zahlen die Summen aus zwei Quadraten sind und für jeden Fall all diese Darstellungen aufzuschreiben.

Fermat bewies:
Genau dann ist $n > 0$ eine Summe aus zwei Quadraten, wenn jeder Primfaktor von n, der Form $p \equiv 3 \bmod 4$, bei der Primfaktorzerlegung von n in einer geraden Potenz erscheint (siehe folgender Beweis).
Für jedes ganzzahlige n, das die Summe aus zwei ganzzahligen Quadraten ist, sei $r(n)$ die Anzahl der geordneten Paare (a, b), wobei $a^2 + b^2 = n$ und a, b ganze Zahlen sind (nicht unbedingt positiv), z.B. $r(1) = 4$, $r(5) = 8$.
Sowohl Jakobi als auch Gauss bewiesen unabhängig voneinander, dass

$$r(n) = 4(d_1(n) - d_3(n)),$$

wobei $d_1(n)$ (bzw. $d_3(n)$) die Anzahl der Teiler von n sind, welche kongruent zu 1 (bzw. 3) modulo 4 sind (vgl. [1]). Mit dieser Formel ist es möglich die primitiven Pythagoras-Tripel (x, y, z) eindeutig zu bestimmen.

Im Folgenden soll nun Fermats Beweis, der von historischer Bedeutung ist, beschrieben werden.
Zu Beginn notieren wir die Gleichung

$$(1) \quad \begin{aligned}(a^2+b^2)(c^2+d^2) &= (ac+bd)^2+(ad-bc)^2 \\ &= (ac-bd)^2+(ad+bc)^2.\end{aligned}$$

Zunächst wollen wir zeigen:

1.4 Satz: Eine Primzahl p ist eine Summe aus zwei Quadraten, genau dann, wenn $p = 2$ oder $p \equiv 1 \bmod 4$.

Beweis:
„$\Longrightarrow$“ Angenommen $p \neq 2$ und $p = a^2 + b^2$, dann kann nicht sowohl a als auch b gerade sein, da sonst $4 \mid p$ gilt.
Seien also a und b beide ungerade, dann gilt

$$p \equiv 1 + 1 = 2 \bmod 4,$$

da jedes ungerade Quadrat kongruent zu 1 modulo 4 ist:

(i) Ist $x \equiv 1 \bmod 4$, so ist $x^2 \equiv 1 \bmod 4$.

(ii) Ist $x \equiv 3 \bmod 4$, so ist $x^2 \equiv 9 \equiv 1 \bmod 4$.

Daher ist die Annahme falsch und es muss $p = 2$ gelten.
Sei nun a gerade und b ungerade, dann gilt

$$p \equiv 0 + 1 = 1 \bmod 4.$$

„$\Longleftarrow$“ Für $2 = 1^2 + 1^2$ ist der Fall klar.
Also nehmen wir an $p \equiv 1 \bmod 4$. Nach Kapitel II Korollar 5.7 ist -1 ein Quadrat modulo p, so dass ein x existiert mit $1 \leq x \leq p-1$, so dass $x^2+1 \equiv 0 \bmod p$. Folglich ist $x^2 + 1 = mp$ mit $1 \leq m \leq p - 1$. Demnach ist die Menge $\{m \mid 1 \leq m \leq p - 1$, mit $mp = x^2 + y^2$ für gewisse ganze Zahlen x, $y\}$ nicht leer.
Sei m_0 die kleinste ganze Zahl dieser Menge, mit $1 \leq m_0 \leq p-1$. Wir zeigen nun durch einen Widerspruch, dass $m_0 = 1$ gilt und somit p die Summe von zwei Quadraten ist.

Annahme: $1 < m_0$
Ferner sei:

$$x = cm_0 + x_1$$

$$y = dm_0 + y_1$$

mit $\frac{-m_0}{2} < x_1, y_1 \leq \frac{m_0}{2}$ und c, d seien ganze Zahlen.
Wir nehmen an, dass enweder x_1 oder y_1 von Null verschieden ist. Sonst würde $m_0^2 \mid x^2 + y^2 = m_0 p$ gelten und damit würde auch gelten $m_0 \mid p$ und somit wäre $m_0 = p$, was ein Widerspruch ist.
Wir wissen

$$0 < x_1^2 + y_1^2 \leq \frac{m_0^2}{4} + \frac{m_0^2}{4} = \frac{m_0^2}{2} < m_0^2$$

und

$$x_1^2 + y_1^2 \equiv x^2 + y^2 \equiv 0 \bmod m_0.$$

Folglich gilt $x_1^2 + y_1^2 = m_0 m'$ mit $1 \leq m' \leq m_0$.
Da $m_0 p = x^2 + y^2$ und $m_0 m' = x_1^2 + y_1^2$,
gilt folglich:

$$\begin{aligned} m_0^2 m' p &= (x^2 + y^2)(x_1^2 + y_1^2) \\ &= (xx_1 + yy_1)^2 + (xy_1 - x_1 y)^2. \end{aligned}$$

Wir wissen außerdem

$$\begin{aligned} xx_1 + yy_1 &= x(x - cm_0) + y(y - dm_0) \\ &= (x^2 + y^2) - m_0(cx + dy) \\ &= m_0 t, \end{aligned}$$

$$\begin{aligned} xy_1 - x_1 y &= x(y - dm_0) - y(x - cm_0) \\ &= -m_0(xd - yc) \\ &= m_0 u, \end{aligned}$$

für zwei beliebige ganze Zahlen t und u.
Folglich gilt $m' p = t^2 + u^2$ mit $1 \leq m' < m_0$. Dies ist ein Widerspruch zu der Tatsache, dass m_0 das kleinste Element sein sollte, und führt deshalb zum Beweis.

1.5 Satz: Eine natürliche Zahl n ist die Summe von zwei ganzzahligen Quadraten, genau dann, wenn jeder Primfaktor p von n, mit $p \equiv 3 \bmod 4$, bei der Primfaktorzerlegung von n in einer geraden Potenz erscheint.

Beweis:
„$\Longleftarrow$“ Sei $n = p_1^{k_1} \dots p_j^{k_j}$ und k_i sei gerade, wenn $p_i \equiv 3 \bmod 4$. Dann gilt: $n = n_0^2 n_1$ mit $n_0 \geq 1$, $n_1 \geq 1$ und n_1 ist das Produkt aus voneinander verschiedenen Primzahlen, die entweder gleich 2 sind, oder kongruent zu 1 modulo 4.
Nach 1.4 ist jeder Faktor von n_1 eine Summe aus zwei Quadraten. Nach der Identität (1) ist n_1 und daher auch n die Summe aus zwei Quadraten.

„$\Longrightarrow$“ Sei $n = x^2 + y^2$.
1.Fall: $x = 0$ oder $y = 0$; Beweis: klar;
2. Fall: Seien x und y von Null verschieden und sei $d = ggT(x, y)$. Damit gilt $d^2 \mid n$.
Sei nun $n = d^2 n'$, $x = dx'$ und $y = dy'$, dann ist $ggT(x', y') = 1$ und $n' = x'^2 + y'^2$.
Wenn $p \mid n'$, dann gilt $p \nmid x'$, denn sonst würde auch $p \mid y'$ gelten. Dies ist aber wegen $ggT(x', y') = 1$ nicht möglich. Nach Kap.II, 4.4 b) gibt es ein $k \in \mathbb{N}$, so dass $kx' \equiv y' \bmod p$ gilt. Dann ist $x'^2 + y'^2 \equiv x'^2(1 + k^2) \equiv 0 \bmod p$.
Folglich gilt $p \mid 1 + k^2$, wegen $p \nmid x'^2$, d.h. -1 ist ein Quadrat modulo p, daher ist $p = 2$ oder $p \equiv 1 \bmod 4$ nach Kap.II, 5.7.
Wenn $p_i \equiv 3 \bmod 4$ und $p_i \nmid n'$, dann gilt $p_i \mid d$ und daher muss der Exponent gerade sein.

Interessant ist auch die Lösung des **Problems**

$$(2) \quad x^2 + y^2 \quad = \quad 1.$$

Die Lösungen für die ganzen Zahlen sind nur die Paare $(\pm 1, 0)$, $(0, \pm 1)$.
Wir wollen nun die Menge $S = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} | x^2 + y^2 = 1\}$ der rationalen Lösungen der Gleichung (2) bestimmen. Dies sind gerade die Punkte auf dem Einheitskreis mit rationalen Koordinaten.

Sei $T = \mathbb{Q} \cup \infty$, $\varphi : T \to \mathbb{Q} \times \mathbb{Q}$ die folgende Funktion:

$$\begin{aligned} (3) \quad \varphi(\infty) &= (0; -1), \\ \varphi(t) &= \left(\tfrac{2t}{1+t^2}; \tfrac{1-t^2}{1+t^2}\right) \quad \text{für } t \in \mathbb{Q}. \end{aligned}$$

1.6 Behauptung: φ ist eine injektive Funktion mit Bild S.

Beweis: Wegen

$$\begin{aligned}\left(\frac{2t}{1+t^2}\right)^2+\left(\frac{1-t^2}{1+t^2}\right)^2 &= \frac{4t^2+(1-t^2)^2}{(1+t^2)^2}\\ &= \frac{1+2t^2+t^4}{(1+t^2)^2}\end{aligned}$$

$$\begin{aligned}&= \frac{(1+t^2)^2}{(1+t^2)^2}\\ &= 1\end{aligned}$$

ist $\varphi(t) \in S$ für jedes $t \in \mathbb{Q}$. Außerdem ist $(0,-1) \in S$ und damit gilt $\varphi(T) \subseteq S$.
Wenn $t \in \mathbb{Q}$, dann ist $\frac{1-t^2}{1+t^2} \neq -1$, da $1+1 \neq 0$.

Jetzt zeigen wir noch:

(a) Für $t_1 \neq t_2$ aus $\mathbb{Q}$ gilt $\varphi(t_1) \neq \varphi(t_2)$.

(b) $\varphi(T) = S$.

zu (a): Aus

$$\varphi(t_1) = \left(\frac{2t_1}{1+t_1^2}, \frac{1-t_1^2}{1+t_1^2}\right) = \left(\frac{2t_2}{1+t_2^2}, \frac{1-t_2^2}{1+t_2^2}\right) = \varphi(t_2)$$

folgt wegen $1+t_i^2 \neq 0$ für $i = 1, 2$,

$$\begin{aligned}&\text{(i)} && t_1(1+t_2^2) &&= t_2(1+t_1^2) && \text{und}\\ &\text{(ii)} && (1-t_1^2)(1+t_2^2) &&= (1-t_2^2)(1+t_1^2), && \text{d.h.}\\ & && 1-t_1^2+t_2^2-t_1^2t_2^2 &&= 1-t_2^2+t_1^2-t_2^2t_1^2, && \text{d.h.}\\ & && t_2^2-t_1^2 &&= t_1^2-t_2^2, && \text{d.h.}\\ & && 2(t_2^2-t_1^2) &&= 0.\end{aligned}$$

Es folgt $t_2^2 = t_1^2$. Eingesetzt in (i) ergibt sich

$$t_1(1+t_1^2) = t_2(1+t_1^2).$$

Kürzen ergibt schließlich $t_1 = t_2$ und daher gilt (a).

zu (b): $(0,-1) = \varphi(\infty)$ ist klar!
Sei $(x,y) \in S$, $(x,y) \neq (0,-1)$. Ist dann $x = 0$, dann ist $y = 1$ und $(0,1) = \varphi(0)$.
Ist nun $x \neq 0$ und $t := \frac{1-y}{x}$, so gilt:

$$\begin{aligned}
1+t^2 &= 1 + \frac{(1-y)^2}{x^2} \\
&= \frac{x^2+1-2y+y^2}{x^2} \\
&= \frac{2-2y}{x^2} \\
&= \frac{2(1-y)}{x^2} \\
1-t^2 &= 1 - \frac{(1-y)^2}{x^2} \\
&= \frac{x^2-1+2y-y^2}{x^2} \\
&= \frac{2y-2y^2}{x^2} \\
&= \frac{2y(1-y)}{x^2}
\end{aligned}$$

und

$$\begin{aligned}
\frac{2t}{1+t^2} &= \frac{\frac{2-2y}{x}}{\frac{2-2y}{x^2}} = x \\
\frac{1-t^2}{1+t^2} &= \frac{\frac{2y(1-y)}{x^2}}{\frac{2(1-y)}{x^2}} = y
\end{aligned}$$

folglich ist $(x,y) = \varphi(t)$ und daraus folgt schließlich die Behauptung.

§2 Der Fall $n = 3$

2.1 Satz: Die Gleichung

$$X^3 + Y^3 + Z^3 = 0$$

besitzt keine ganzzahlige Lösung (x, y, z) mit $xyz \neq 0$.

Beweis: Angenommen x, y und z sind von Null verschiedene, paarweise teilerfremde ganze Zahlen, so dass $x^3 + y^3 + z^3 = 0$ gilt. Dann müssen sie paarweise verschieden sein (da 2 keine dritte Potenz ist) und genau eine von diesen ganzen Zahlen ist gerade. Sei also x, y ungerade und z gerade. Von den ganzen existierenden Lösungen, die diese Bedingungen erfüllen, wählen wir die Lösung mit minimalem $|z|$ aus.
Wir werden von Null verschiedene, paarweise teilerfremde ganze Zahlen l, m, n finden, mit $l^3 + m^3 + n^3 = 0$, n gerade und $|z| > |n|$. Dies ist dann ein Widerspruch zur Minimalität von $|z|$.

Da $x+y$ und $x-y$ gerade sind, existieren ganze Zahlen a, b, so dass $2a = x+y$ und $2b = x - y$. Somit ist dann $x = a + b$, $y = a - b$ und demnach ist $a \neq 0$, $b \neq 0$, $ggT(a, b) = 1$ und a, b sind von verschiedener Parität. Folglich ist

$$\begin{aligned} -z^3 &= x^3 + y^3 \\ &= (a+b)^3 + (a-b)^3 \\ &= a^3 + 3a^2b + 3ab^2 + b^3 + a^3 - 3a^2b + 3ab^2 - b^3 \\ &= 2a^3 + 6ab^2 \\ &= 2a(a^2 + 3b^2). \end{aligned}$$

Aber $a^2 + 3b^2$ ist ungerade und z ist gerade. Folglich gilt $8 \mid z^3$, also gilt auch $8 \mid 2a$ und damit ist a gerade und b ungerade.
Wir zeigen nun, dass $ggT(2a, a^2+3b^2)$ entweder 1 oder 3 ist. Wenn p^k $(k \geq 1)$ die Potenz einer Primzahl p ist, die $2a$ und a^2+3b^2 teilt, dann gilt $p^k \mid a$ und folglich auch $p^k \mid 3b^2$, wegen $p \neq 2$. Aber $p \nmid b$, da $ggT(a, b) = 1$, daher ist $k = 1$ und $p = 3$. Nun unterscheiden wir zwei Fälle:

1.Fall: $ggT(2a, a^2 + 3b^2) = 1$
Wegen $ggT(2a, a^2 + 3b^2) = 1$ gilt $3 \nmid a$. Aus $-z^3 = 2a(a^2 + 3b^2)$ folgt, wegen der eindeutigen Primfaktorzerlegung ganzer Zahlen, dass $2a$ und $a^2 + 3b^2$ dritte Potenzen sind:

$$\begin{aligned} 2a &= r^3, \\ a^2 + 3b^2 &= s^3, \end{aligned}$$

wobei s ungerade und kein Vielfaches von 3 ist.
Wir benutzen nun eine Tatsache, die wir erst später beweisen werden:

2.2 Lemma: Sei s ungerade mit $s^3 = a^2 + 3b^2$ und $ggT(a, b) = 1$. Dann gibt es $u, v \in \mathbb{Z}$ mit

$$\begin{aligned} s &= u^2 + 3v^2, \\ a &= u(u^2 - 9v^2), \\ b &= 3v(u^2 - v^2). \end{aligned}$$

Dann ist v ungerade und u gerade (weil b ungerade ist), $u \neq 0$ und $3 \nmid u$ (da $3 \nmid a$) und $ggT(u, v) = 1$. Folglich sind $2u$, $u + 3v$, $u - 3v$ paarweise teilerfremd und aus $r^3 = 2a = 2u(u - 3v)(u + 3v)$ folgt, dass $2u$, $u - 3v$ und $u + 3v$ dritte Potenzen sind:

$$\begin{aligned} 2u &= -n^3, \\ u - 3v &= l^3, \\ u + 3v &= m^3, \end{aligned}$$

mit l, m, n verschieden von Null (wegen $3 \nmid u$) und paarweise teilerfremd. Wir schließen, dass

$$l^3 + m^3 + n^3 = 0,$$

wobei n gerade ist. Nun zeigen wir noch, dass $|z| > |n|$. In der Tat gilt

$$\begin{aligned} |z|^3 &= |2a(a^2 + 3b^2)| \\ &= |2u(u^2 - 9v^2)|(a^2 + 3b^2) \\ &= |-n^3(u^2 - 9v^2)|(a^2 + 3b^2) \\ &\geq 3|n^3| \\ &> |n^3|, \end{aligned}$$

weil $u^2 - 9v^2 = l^3m^3 \neq 0$ und $b \neq 0$, weil b ungerade ist. Dies ist ein Widerspruch zur Minimalität von $|z|$.

2.Fall: $ggT(2a, a^2 + 3b^2) = 3$
Wir setzten $a := 3c$. Daher gilt c ist gerade und $4 \mid c$ (wegen $8 \mid 2a$), während $3 \nmid b$ (weil a, b teilerfremd sind). Demnach ist

$$\begin{aligned} -z^3 &= x^3 + y^3 \\ &= (a + b)^3 + (a - b)^3 \\ &= (3c + b)^3 + (3c - b)^3 \end{aligned}$$

$$
\begin{aligned}
&= 27c^3 + 27c^2b + 9cb^2 + b^3 + 27c^3 - 27c^2b + 9cb^2 - b^3 \\
&= 54c^3 + 18cb^2 \\
&= 18c(3c^2 + b^2),
\end{aligned}
$$

wobei $ggT(18c, 3c^2 + b^2) = 1$: Da c gerade und b ungerade ist, gilt folglich $3c^2 + b^2$ ist ungerade. Ferner gilt $3 \nmid 3c^2 + b^2$ und $ggT(b, c) = 1$.
Nach der eindeutigen Primfaktorzerlegung ganzer Zahlen sind $18c$ und $3c^2+b^2$ dritte Potenzen:

$$
\begin{aligned}
18c &= r^3, \\
3c^2 + b^2 &= s^3,
\end{aligned}
$$

wobei s ungerade ist und $3 \mid r$ gilt. Nach 2.2 gibt es $u, v \in \mathbb{Z}$ mit

$$
\begin{aligned}
s &= u^2 + 3v^2, \\
b &= u(u^2 - 9v^2), \\
c &= 3v(u^2 - v^2).
\end{aligned}
$$

Dann ist u ungerade und v gerade (da b ungerade ist), $v \neq 0$ (da $c \neq 0$), $ggT(u, v) = 1$. Also sind $2v$, $u + v$ und $u - v$ paarweise teilerfremd. Aus $r^3 = 18c = 54v(u + v)(u - v)$ leiten wir ab, dass $(\frac{r}{3})^3 = 2v(u + v)(u - v)$ und $2v$, $u + v$ und $u - v$ dritte Potenzen sind:

$$
\begin{aligned}
2v &= -n^3, \\
u + v &= l^3, \\
u - v &= -m^3.
\end{aligned}
$$

Folglich ist $l^3 + m^3 + n^3 = 0$ mit l, m, n von Null verschieden und n gerade. Nun zeigen wir noch, dass $|z| > |n|$. In der Tat gilt

$$
\begin{aligned}
|z|^3 &= 18|c|(3c^2 + b^2) \\
&= 54|v(u^2 - v^2)|(3c^2 + b^2) \\
&= 27|n|^3|(u^2 - v^2)|(3c^2 + b^2) \\
&> |n|^3,
\end{aligned}
$$

weil $u^2 - v^2 = -l^3m^3 \neq 0$, $|3c^2 + b^2| \geq 1$. Erneut ist dies ein Widerspruch zur Minimalität von $|z|$.

Im Folgenden wollen wir nun noch Lemma 2.2 beweisen. Zu diesem Zweck verwenden wir Argumente, die bereits Fermat bekannt waren, in Verbindung mit der Untersuchung von ganzen Zahlen der Form $u^2 + v^2$. Sei S die Menge

der ganzen Zahlen der Form a^2+3b^2 $(a,b \in \mathbb{Z})$. S ist bezüglich der Multiplikation abgeschlossen, da

$$\begin{aligned}(*)(a^2+3b^2)(c^2+3d^2) &= a^2c^2+3a^2d^2+3b^2c^2+9b^2d^2\\ &= (a^2c^2 \pm 6abcd+9b^2d^2) \mp 6abcd+3(a^2d^2+b^2c^2)\\ &= (ac \pm 3bd)^2+3(a^2d^2 \mp 2abcd+b^2c^2)\\ &= (ac \pm 3bd)^2+3(ad \mp bc)^2.\end{aligned}$$

2.3 Lemma: Sei p eine Primzahl ≥ 5, dann sind folgende Aussagen äquivalent:

(a) $p \equiv 1 \bmod 3$.

(b) Es gibt ein $w \in \mathbb{N}$ mit $-3 \equiv w^2 \bmod p$.

Beweis:
(a) $\Rightarrow$ (b)
Nach Voraussetzung gibt es ein $n \in \mathbb{N}$ mit $p-1=3n$. Wegen $p \geq 5$ ist $2 \leq n < p-1$. Die Kongruenz $x^n \equiv 1 \bmod p$ hat nach (Kap.II,5.5) in $\mathbb{Z}/\mathrm{p}\mathbb{Z}$ genau n Lösungen. Also existiert ein $y \in \mathbb{N}$, $y \not\equiv 0 \bmod p$ mit $y^n \not\equiv 1 \bmod p$. Nach dem kleinen Satz von Fermat (Kap.II,5.3) gilt:

$$y^{p-1} \equiv 1 \bmod p.$$

Setze $x=y^n$, dann gilt: $x \not\equiv 1 \bmod p$ und $x^3=(y^n)^3=y^{3n}=y^{p-1} \equiv 1 \bmod p$, d.h. $p \mid x^3-1=(x-1)(x^2+x+1)$, aber $p \nmid x-1$. Also gilt $p \mid x^2+x+1$. Setze nun $w=2x+1$:

$$\begin{aligned}w^2+3 &= (2x+1)^2+3\\ &= 4x^2+4x+4\\ &= 4(x^2+x+1)\\ &\equiv 0 \bmod p,\end{aligned}$$

d.h. $-3 \equiv w^2 \bmod p$.

(b) $\Rightarrow$ (a)
Wegen $ggT(2,p)=1$ gibt es $x, y \in \mathbb{Z}$ mit $w-1=2x+py$ (Kap.II, 2.4 (b)). Es folgt also $w \equiv (2x+1) \bmod p$, und daher gilt außerdem $4(x^2+x+1)=(2x+1)^2+3=w^2+3 \equiv 0 \bmod p$. Wegen $p \neq 2$ ist $x^2+x+1 \equiv 0 \bmod p$. Angenommen es gilt $x^2 \equiv 1 \bmod p$, dann gilt ferner $x^2-1 \equiv 0 \bmod p$ und damit ist auch $(x+1)(x-1) \equiv 0 \bmod p$. Daher muss entweder $(x+1) \equiv 0 \bmod p$ oder $(x-1) \equiv 0 \bmod p$ gelten.

(i) $x+1 \equiv 0 \bmod p$, d.h. $x \equiv -1 \bmod p$.

(ii) $x-1 \equiv 0 \bmod p$, d.h. $x \equiv 1 \bmod p$.

(i) einsetzen ergibt $x^2+x+1 \equiv 1 \bmod p$, ferner gilt auch noch $x^2+x+1 \equiv 0 \bmod p$ und daher muss $p = 1$ gelten. Dies ist aber ein Widerspruch zur Voraussetzung $p \geq 5$.
(ii) einsetzen ergibt $x^2+x+1 \equiv 3 \bmod p$, da auch noch $x^2+x+1 \equiv 0 \bmod p$ gilt, muss $p = 3$ gelten. Dies ist aber ebenfalls ein Widerspruch zu $p \geq 5$. Daher ist die Annahme falsch und es gilt:

$$(**) \quad x^2 \not\equiv 1 \bmod p, \text{ und damit auch } x \not\equiv 1 \bmod p.$$

Dividiert man $p-1$ durch 3 mit Rest, so erhält man:

$$p-1 = 3q+r \text{ mit } q \geq 0, 0 \leq r < 3.$$

Ferner ist $x^3-1 = (x-1)(x^2+x+1) \equiv 0 \bmod p$ und $x^3 \equiv 1 \bmod p$. Daraus folgt $1 \equiv x^{p-1} \equiv x^{3q+r} \equiv (x^3)^q x^r \equiv x^r \bmod p$. Nach $(**)$ ist $r = 0$ und daher gilt $3 \mid p-1$, d.h. $p \equiv 1 \bmod 3$.

2.4 Lemma: Wenn k eine von Null verschiedene ganze Zahl ist, p eine Primzahl mit $p = c^2+3d^2 \in S$ und $pk = a^2+3b^2 \in S$, dann gilt $p \mid ac \pm 3bd$ und $p \mid ad \mp bc$ (mit entsprechenden Vorzeichen) und

$$k = \left(\frac{ac \pm 3bd}{p}\right)^2 + 3\left(\frac{ad \mp bc}{p}\right)^2 \in S.$$

Beweis: Wir haben

$$\begin{aligned} k &= \frac{pk}{p} \\ &= \frac{a^2+3b^2}{c^2+3d^2} \\ &= \frac{(a^2+3b^2)(c^2+3d^2)}{(c^2+3d^2)^2} \\ &= \left(\frac{ac \pm 3bd}{c^2+3d^2}\right)^2 + 3\left(\frac{ad \mp bc}{c^2+3d^2}\right)^2 \end{aligned}$$

nach $(*)$. Aber

$$\begin{aligned} (ac+3bd)(ac-3bd) &= a^2c^2 - 9b^2d^2 \\ &= a^2c^2 + 3a^2d^2 - 3a^2d^2 - 9b^2d^2 \end{aligned}$$

$$
\begin{aligned}
&= a^2(c^2+3d^2) - 3(a^2+3b^2)d^2 \\
&= a^2c^2 + a^2 3d^2 - 3pkd^2 \\
&= a^2c^2 + 3a^2d^2 - 3(c^2+3d^2)kd^2 \\
&= a^2c^2 + 3a^2d^2 - 3kc^2d^2 - 9kd^4 \\
&= (a^2 - 3kd^2)(c^2+3d^2).
\end{aligned}
$$

Da $c^2+3d^2 = p$ eine Primzahl ist, gilt $p \mid ac+3bd$ oder $p \mid ac-3bd$. Im ersten Fall ist $\frac{ac+3bd}{p} \in \mathbb{Z}$, folglich ist auch $3\left(\frac{ad-bc}{p}\right)^2 = k - \left(\frac{ac+3bd}{p}\right)^2 \in \mathbb{Z}$. Demnach ist auch $\frac{ad-bc}{p} \in \mathbb{Z}$ und $k = \left(\frac{ac+3bd}{p}\right)^2 + 3\left(\frac{ad-bc}{p}\right)^2 \in S$. Im Fall $p \mid ac-3bd$ schließt man analog.

2.5 Lemma: Wenn p eine Primzahl ist, dann ist $p \in S$ genau dann, wenn $p = 3$ oder $p \equiv 1 \bmod 3$.

Beweis: Wenn $p = a^2+3b^2$, $p \neq 3$ und $b \neq 0$, so gilt $p \equiv a^2 \bmod 3$ und $3 \nmid a$, demnach gilt $p \equiv a^2 \equiv 1 \bmod 3$.
Offensichtlich gilt $3 \in S$.
Sei also $p \equiv 1 \bmod 3$. Nach dem Lemma 2.3 existiert ein $t \in \mathbb{N}$, so dass $0 < t < \frac{p}{2}$ und $-3 \equiv t^2 \bmod p$. Dann ist $mp = t^2+3 < (\frac{p}{2})^2 + 3 < p^2$ also $0 < m < p$. Wir zeigen nun, dass für jedes $t \geq 1$ höchstens eine Primzahl $p \neq 2$ und $p \neq 3$ existiert, so dass gilt $p \mid t^2+3$, aber $p \nmid u^2+3$ für jedes u mit $1 \leq u < t$.
Wir nehmen an, dass verschiedene Primzahlen p und p' wie oben beschrieben existieren, wobei $p < p'$. Nach der vorherigen Bemerkung gilt dann $0 < t < \frac{p}{2}$ und $t^2+3 = pm$ mit $0 < m < p$. Wenn $p' \mid t^2+3$, dann gilt ferner $p' \mid m$, so dass $p' \leq m < p$ gilt, was ein Widerspruch zu $p < p'$ ist.
Nun können wir die Behauptung beweisen.
Angenommen es existiert eine Primzahl p, $p \equiv 1 \bmod 3$, so dass $p \notin S$. Wir nehmen das kleinstmögliche p, das diese Bedingung erfüllt. Sei $t \geq 1$ die kleinstmögliche ganze Zahl, so dass $p \mid t^2+3$ gilt, also gilt $0 < t < \frac{p}{2}$ und $t^2+3 = mp$ mit $0 < m < p$. Wenn p' irgendeine Primzahl ist, die m teilt, also $m = p'm'$, dann gilt $p' \leq m < p$ und somit gilt $p' \in S$. Wegen $p'(pm') = pm = t^2+3 \in S$ folgt nach dem Lemma 2.4, dass $pm' \in S$. Wenn $m' = 1$, dann ist $p \in S$, was wir zeigen wollten. Wenn p'' eine Primzahl ist, die m' teilt, also $m' = p''m''$ gilt, dann ist $p'' \leq m' < p$ und folglich gilt $p'' \in S$, und demnach $p''(pm'') = pm' \in S$ und nach dem Lemma 2.4 ist $pm'' \in S$, mit $m'' < m'$. Wenn wir dieses Argument immer wiederholen, dann gelangen wir schließlich zu dem Schluß, dass $p \in S$.

2.6 Lemma: Sei $m = u^2 + 3v^2$, mit $u, v \neq 0$ und $ggT(u, v) = 1$. Wenn p eine ungerade Primzahl ist und $p \mid m$ gilt, dann ist $p \in S$.

Beweis: Wegen $p \mid m$ gilt $m \equiv 0 \bmod p$ und somit gilt auch $u^2 \equiv -3v^2 \bmod p$. Da $3 \in S$ gilt, nehmen wir an, dass $p \neq 3$. Ferner gilt wegen $p \mid m$ auch noch $p \nmid v$, denn sonst würde auch $p \mid u$ gelten und dies wäre ein Widerspruch zur Voraussetzung ($ggT(u, v) = 1$). Da $p \nmid v$ gilt, folgt nach Kapitel II, 5.4, dass $a^{p-1} \equiv 1 \bmod p$. Setzen wir nun $v' := v^{p-2}$, dann gilt $vv' \equiv 1 \bmod p$. Daher ist $(uv')^2 \equiv u^2 v'^2 \equiv -3v^2 v'^2 \equiv -3(vv')^2 \equiv -3 \bmod p$. Nach dem Lemma 2.2 ist dann auch $p \equiv 1 \bmod 3$ und nach dem Lemma 2.5 folgt schließlich $p \in S$.

Wir vervollständigen die bisherigen Lemmas, wie folgt:

2.7 Lemma: Wenn p eine Primzahl und $p \in S$, dann ist die Darstellung von p in der Form $p = a^2 + 3b^2$ (mit $a \geq 0$, $b \geq 0$) eindeutig.

Beweis: Wir verwenden das Lemma 2.4 mit $k = 1$. Somit ist $p = a^2 + 3b^2 = c^2 + 3d^2$ (wobei $a, c \geq 0, b > 0, d > 0$). Folglich gilt

$$1 = \left(\frac{ac \pm 3bd}{p}\right)^2 + 3\left(\frac{ad \mp bc}{p}\right)^2,$$

also gilt $p = ac \pm 3bd$ und $ad = \pm bc$. Deshalb gilt

$$\begin{aligned} pd &= acd \pm 3bd^2 \\ &= \pm bc^2 \pm 3bd^2 \\ &= \pm b(c^2 + 3d^2) \\ &= \pm bp. \end{aligned}$$

Folglich gilt $d = \pm b$, daher gilt $b = d$ und daraus folgt $a = c$.

2.8 Lemma: Sei $m = u^2 + 3v^2 \geq 3$ und $ggT(u, v) = 1$. Wenn m ungerade ist und $m = \prod_{i=1}^{n} p_i^{e_i}$ (wobei $p_1, ..., p_n$ Primzahlen sind und $e_i \geq 1$), dann existieren ganze Zahlen a_i und b_i ($i = 1, ..., n$), so dass $p_i = a_i^2 + 3b_i^2$ und

$$u + v\sqrt{-3} = \prod_{i=1}^{n} (a_i + b_i\sqrt{-3})^{e_i}.$$

Beweis durch Induktion nach m: Für $m = 3$ ist $u = 0$ und $v = 1$. Daher setzt man $a_1 = 0$ und $b_1 = 1$.

Sei also $m > 3$, so gilt $m = u^2 + 3v^2$, mit $u \neq 0$ und $v \neq 0$, $ggT(u, v) = 1$. Sei p eine Primzahl, die m teilt, also gilt $m = pk$. Nach dem Lemma 3.6 ist $p \in S$ und hat daher die Form $p = a^2 + 3b^2$. Demnach erfüllt jedes $p \in S$ das Lemma 2.8. Nach dem Lemma 2.4 gilt ferner $k = c^2 + 3d^2$, wobei $c = \frac{(ua \pm 3vb)}{p}$ und $d = \frac{(ub \mp va)}{p}$ (mit entsprechenden Vorzeichen). Wir wissen außerdem $(a \pm b\sqrt{-3})(c \mp d\sqrt{-3}) = (ac + 3bd) \pm (bc - ad)\sqrt{-3}$, wobei

$$\begin{aligned}
ac + 3bd &= \frac{a(ua \pm 3vb)}{p} + \frac{3b(ub \mp va)}{p} \\
&= \frac{1}{p}(ua^2 \pm 3vab + 3ub^2 \mp 3vab) \\
&= u \cdot \frac{1}{p}(a^2 + 3b^2) \\
&= u, \\
\pm(bc - ad) &= \pm\left(\frac{b(ua \pm 3vb)}{p} - \frac{a(ub \mp va)}{p}\right) \\
&= \pm\frac{1}{p}(uab \pm 3vb^2 - uab \pm va^2) \\
&= v \cdot \frac{1}{p}(3b^2 + a^2) \\
&= v,
\end{aligned}$$

so dass $(a \pm b\sqrt{-3})(c \mp d\sqrt{-3}) = u + v\sqrt{-3}$.
Wenn $k = 1$ gilt, ist $m = p$ und da für Primzahlen das Lemma 2.8 gilt ist nichts weiter zu zeigen. Im Fall $k \neq 1$ ist $3 \leq k < m$ und $k = c^2 + 3d^2$. Ferner gilt $ggT(c, d) = 1$, da $u = ac + 3bd$ und $v = \pm(bc - ad)$ teilerfremd sind. Nach der Induktion ist das Resultat für k wahr, folglich lässt sich $c \mp d\sqrt{-3}$ in der angegebenen Form ausdrücken. Da $(a \pm b\sqrt{-3})(c \mp d\sqrt{-3}) = u + v\sqrt{-3}$ gilt das Ergebnis auch für m.

2.9 Lemma: Sei E die Menge aller Tripel (u, v, s), so dass s ungerade ist, $ggT(u, v) = 1$ und $s^3 = u^2 + 3v^2$. Sei F die Menge aller Paare (t, w), wobei $ggT(t, w) = 1$, $3 \nmid t$ und $t \not\equiv w \bmod 2$. Dann hat die Abbildung $\phi : F \to \mathbb{Z}^3$, gegeben durch $\phi(t, w) = (u, v, s)$ mit

$$\begin{aligned}
u &= t(t^2 - 9w^2), \\
v &= 3w(t^2 - w^2), \\
s &= t^2 + 3w^2,
\end{aligned}$$

das Bild E.

Beweis: Es gilt

$$\begin{aligned} u^2+3v^2 &= [t(t^2-9w^2)]^2+3[3w(t^2-w^2)]^2 \\ &= t^6-18t^4w^2+81t^2w^4+27t^4w^2-54t^2w^4+27w^6 \\ &= t^6+9t^4w^2+27t^2w^4+27w^6 \\ &= (t^2+3w^2)^3 \\ &= s^3. \end{aligned}$$

Weil t, w nicht beide gerade bzw. ungerade sein können, ist s ungerade.
Als nächstes wollen wir zeigen, dass $ggT(u,v)=1$ gilt. Angenommen $ggT(t^2-9w^2, t^2-w^2) \neq 1$, dann gibt es eine Primzahl p mit $p \mid t^2-9w^2$ und $p \mid t^2-w^2$, dann gilt auch $p \mid 9t^2-9w^2$ und folglich auch $p \mid 8t^2$. Daher muss $p=2$ gelten (da $p \nmid t$ wegen $ggT(t,w)=1$). Dies kann aber nicht sein, da nach Voraussetzung t und w verschiedene Parität haben. Also gilt $ggT(t^2-9w^2, t^2-w^2)=1$.
Nun zeigen wir noch, dass $ggT(u,v)=1$. Sei p eine Primzahl von der Primfaktorzerlegung von u. Dann gilt $p \mid u$ und daher gilt ferner $p \mid t$ oder $p \mid t^2-9w^2$.

(i) $p \mid t$ und daher gilt $p \neq 3$, $p \nmid w$ und $p \nmid (t^2-w^2)$. Deshalb gilt $p \nmid v$.

(ii) $p \nmid t$, daher gilt $p \mid t^2-9w^2$ und $p \nmid 3w$ und daraus folgt wegen $ggT(t^2-9w^2, t^2-w^2)=1$, dass $p \nmid t^2-w^2$. Wegen $p \nmid 3w$ und $p \nmid t^2-w^2$ gilt folglich $p \nmid v$.

Also ist $ggT(u,v)=1$. Dies zeigt, dass $\phi(t,w)=(u,v,s) \in E$, d.h. Bild $\phi \subseteq E$.
Nun zeigen wir die entgegengesetzte Inklusion. Gegeben ist ein Tripel $(u,v,s) \in E$. Sei $s^3=\prod_{i=1}^{n} p_i^{e_i}$ die Zerlegung von s^3 in ein Produkt von Primzahlen ($p_1,...,p_n$ verschieden, $e_i \geq 1$), also gilt $e_i=3e_i'$ für jedes i. Nach dem Lemma 2.8 existieren a_i, b_i mit $i=1,..,n$, so dass $p_i=a_i^2+3b_i^2$ und

$$u+v\sqrt{-3}=\prod_{i=1}^{n}(a_i+b_i\sqrt{-3})^{e_i}.$$

Sei t, $w \in \mathbb{Z}$ definiert durch die Beziehung

$$\prod_{i=1}^{n}(a_i+b_i\sqrt{-3})^{e_i'}=t+w\sqrt{-3},$$

also ist $u+v\sqrt{-3}=(t+w\sqrt{-3})^3$. Berechnen wir explizit die dritte Potenz auf der rechten Seite der Gleichung, so erhalten wir

$$\begin{aligned} (t+w\sqrt{-3})^3 &= t^3+3t^2w\sqrt{-3}-9tw^2-3\sqrt{-3}w^3 \\ &= t^3-9tw^2+(3t^2w-3w^3)\sqrt{-3} \end{aligned}$$

und daraus folgt, dass $u = t(t^2 - 9w^2)$ und $v = 3w(t^2 - w^2)$. Wir verwenden noch die folgende Regel für die Konjugation komplexer Zahlen (Kap.II, 7.2(c)). Sind $x, y \in \mathbb{R}$ und $z = x + iy \in \mathbb{C}$, so heißt $\overline{z} := x - iy$ die zu z konjugierte komplexe Zahl. Es gilt

$$\overline{zw} = \overline{z} \cdot \overline{w} \text{ für alle } z, w \in \mathbb{C}, \text{ also auch } \overline{z}^n = \overline{z^n}.$$

Es folgt

$$\begin{aligned}
s^3 &= u^2 + 3v^2 \\
&= (u + v\sqrt{-3})(u - v\sqrt{-3}) \\
&= (u + i\sqrt{3}v)\overline{(u + i\sqrt{3}v)} \\
&= (t + i\sqrt{3}w)^3\overline{(t + i\sqrt{3}w)^3} \\
&= (t + i\sqrt{3}w)^3 \left[\overline{(t + i\sqrt{3}w)}\right]^3 \\
&= \left[(t + w\sqrt{-3})(t - w\sqrt{-3})\right]^3 \\
&= \left[t^2 + 3w^2\right]^3
\end{aligned}$$

und somit gilt $s = t^2 + 3w^2$. Daraus ergibt sich, dass t und w nicht die gleiche Parität haben, $ggT(t, w) = 1$ und $\phi(t, w) = (u, v, s)$ gilt.
Insbesondere gilt nach 2.9: Ist s ungerade und $s^3 = u^2 + 3v^2$ mit $ggT(u, v) = 1$, dann schreibt sich s in der Form $s = t^2 + 3w^2$ mit $u = t(t^2 - 9w^2)$ und $v = 3w(t^2 - w^2)$. Damit ist auch 2.2 bewiesen.
Nun haben wir alle Schritte des Beweises von Euler von 2.1 im einzelnen genauer betrachtet und bewiesen.

§3 Der Fall $n = 4$

Fermat beschäftigte sich mit dem Problem, ob die Fläche eines Pythagoras-Dreiecks das Quadrat einer ganzen Zahl ist. Dies führte dazu, dass er die Gleichung

$$X^4 - Y^4 = Z^2$$

betrachtete. Schließlich konnte er zeigen:

3.1 Satz: Die Gleichung

$$X^4 - Y^4 = Z^2$$

hat keine positive ganzzahlige Lösung.

3.2 Lemma: Seien s, t teilerfremde positive ganze Zahlen, wobei $s > t$. Dann gilt $ggT(s+t, s-t) = 1$, falls s und t verschiedene Parität haben und $ggT(s+t, s-t) = 2$, falls s und t ungerade sind. Im zweiten Fall ist dann also $ggT(\frac{s+t}{2}, \frac{s-t}{2}) = 1$.

Beweis von 3.2: Ist $d := ggT(s+t, s-t)$, so gilt $d \mid s+t$ und $d \mid s-t$, also gilt auch $d \mid 2s = (s+t)+(s-t)$ und $d \mid 2t = (s+t)-(s-t)$. Es folgt $d \mid ggT(2s, 2t) = 2 \cdot ggT(s,t) = 2 \cdot 1 = 2$ und daher gilt $d = 1$ oder $d = 2$.
Sind s und t beide ungerade, so sind $s+t$ und $s-t$ beide gerade und folglich ist $d = 2$.
Haben aber s und t verschiedene Parität, so sind $s+t$ und $s-t$ beide ungerade, also $2 \neq d = ggT(s+t, s-t)$. Daraus folgt schließlich $d = 1$.

Beweis des Satzes: Angenommen die Behauptung sei falsch und (x, y, z) ist ein Tripel aus positiven ganzen Zahlen, mit minimalem x, so dass $x^4 - y^4 = z^2$. Wenn eine Primzahl p sowohl x als auch y teilt, dann gilt $p^4 \mid z^2$, und damit gilt auch $p^2 \mid z$. Sei $x = px'$, $y = py'$ und $z = p^2 z'$, dann gilt $x'^4 - y'^4 = z'^2$ mit $0 < x' < x$, und dies ist ein Widerspruch zur Minimalität von x. Daher muss $ggT(x, y) = 1$ gelten.
Wir wissen $z^2 = x^4 - y^4 = (x^2 + y^2)(x^2 - y^2)$. Da $ggT(x, y) = 1$ und somit auch $ggT(x^2, y^2) = 1$, ist nach 3.2 der $ggT(x^2 + y^2, x^2 - y^2)$ entweder 1 oder 2. Wir betrachten daher zwei Fälle:

1. Fall: $ggT(x^2 + y^2, x^2 - y^2) = 1$
Da das Produkt von $x^2 + y^2$ und $x^2 - y^2$ ein Quadrat ist, ist auch $x^2 + y^2$ und $x^2 - y^2$ jeweils ein Quadrat. Genauer: Es existieren positive ganze Zahlen s, t mit $ggT(s, t) = 1$, so dass

$$x^2 + y^2 = s^2,$$

$$x^2 - y^2 = t^2.$$

Wegen $2x^2 = s^2 + t^2$ muss entweder sowohl s als auch t gerade sein oder beide müssen ungerade sein. Ferner dürfen wegen $ggT(s,t) = 1$ nicht beide gerade sein. Also gilt, dass sowohl s als auch t ungerade sein muss.
Es existieren positive ganze Zahlen u, v, so dass

$$u = \frac{(s+t)}{2},$$

$$v = \frac{(s-t)}{2},$$

wobei nach 3.2 $ggT(u,v) = 1$, weil s und t ungerade sind.
Es gilt $uv = \frac{(s^2-t^2)}{4} = \frac{2y^2}{4} = \frac{y^2}{2}$, daher gilt $y^2 = 2uv$. Da $ggT(u,v) = 1$, existieren positive ganze Zahlen l, m mit

$$\begin{array}{rcl} u &=& 2l^2 \\ v &=& m^2 \end{array} \qquad \text{oder} \qquad \begin{array}{rcl} u &=& l^2 \\ v &=& 2m^2. \end{array}$$

1. Möglichkeit: u ist gerade, $ggT(u,v,x) = 1$ und

$$u^2 + v^2 = \frac{(s+t)^2 + (s-t)^2}{4} = \frac{s^2 + t^2}{2} = x^2.$$

Nach 1.3 folgt, dass positive ganze Zahlen a, b existieren mit $0 < b < a$ und $ggT(a,b) = 1$, so dass

$$\begin{array}{rcrcl} 2l^2 &=& u &=& 2ab, \\ m^2 &=& v &=& a^2 - b^2, \\ && x &=& a^2 + b^2, \end{array}$$

folglich gilt $l^2 = ab$. Daher existieren positive ganze Zahlen c, d mit $ggT(c,d) = 1$, so dass

$$\begin{array}{rcl} a &=& c^2, \\ b &=& d^2. \end{array}$$

Daraus folgt $m^2 = c^4 - d^4$. Das Tripel (c, d, m) aus positiven ganzen Zahlen wäre somit eine Lösung der Gleichung $X^4 - Y^4 = Z^2$. Ferner würde auch noch, wie leicht zu erkennen ist, $0 < c \leq a < x$ gelten. Dies ist aber ein Widerspruch zur Minimalität von x.

2. Möglichkeit: v gerade, $ggT(u,v,x)=1$ und

$$u^2+v^2=\frac{(s+t)^2+(s-t)^2}{4}=\frac{s^2+t^2}{2}=x^2.$$

Nach 1.3 existieren wieder positive ganze Zahlen a,b mit $0<a<b$ und $ggT(a,b)=1$, so dass

$$\begin{array}{rcccl} 2m^2 & = & v & = & 2ab, \\ l^2 & = & u & = & a^2-b^2, \\ & & x & = & a^2+b^2. \end{array}$$

Es gilt also $m^2=ab$. Folglich existieren positive ganze Zahlen c,d mit $ggT(c,d)=1$, so dass

$$\begin{array}{rcl} a & = & c^2, \\ b & = & d^2. \end{array}$$

Also gilt $l^2=c^4-d^4$. Damit wäre das Tripel (c,d,l) aus positiven ganzen Zahlen eine Lösung der Gleichung $X^4-Y^4=Z^2$ und ferner würde
$0<c\leq a<x$ gelten. Dies ist aber ein Widerspruch zur Minimalität von x.

2. Fall: $ggT(x^2+y^2,x^2-y^2)=2$
Jetzt sind x,y ungerade und z gerade. Nach 1.3 existieren positive ganze Zahlen a,b mit $0<b<a$ und $ggT(a,b)=1$, so dass

$$\begin{array}{rcl} x^2 & = & a^2+b^2, \\ y^2 & = & a^2-b^2, \\ z & = & 2ab. \end{array}$$

Daher gilt $x^2y^2=a^4-b^4$. Damit wäre das Tripel (a,b,xy) eine Lösung von 3.1. Wegen $0<a<x$ ist dies aber ein Widerspruch zur Minimalität von x. Damit wäre 3.1 bewiesen.

3.3 Korollar: Die Fläche eines Pythagoras-Dreiecks ist nicht das Quadrat einer ganzen Zahl.

Beweis: Sind a,b,c die Seiten eines Pythagoras-Dreiecks, wobei c die Hypothenuse ist, so gilt $c^2=a^2+b^2$. Angenommen die Fläche ist das Quadrat einer ganzen Zahl s, dann gilt: $\frac{ab}{2}=s^2$. Ferner würde gelten

$$\begin{array}{rcl} (a+b)^2 & = & c^2+4s^2, \\ (a-b)^2 & = & c^2-4s^2. \end{array}$$

Folglich gilt dann auch

$$(a^2 - b^2)^2 = (a^2 + b^2)^2 - 4a^2b^2 = c^4 - 16s^4 = c^4 - (2s)^4.$$

Ferner ist $a^2 \neq b^2$, da sonst $c^2 = 2a^2$ und $\sqrt{2} = \frac{c}{a}$ eine rationale Zahl wäre. Daher würde die Gleichung $X^4 - Y^4 = Z^2$ eine nicht triviale Lösung von ganzen Zahlen besitzen, dies ist aber ein Widerspruch zu 3.1.

3.4 Satz: Die Gleichung

$$X^4 + Y^4 = Z^4$$

hat keine positive ganzzahlige Lösung.

Beweis: Angenommen x, y, z sind positive ganze Zahlen, mit $x^4 + y^4 = z^4$, dann gilt auch $z^4 - y^4 = (x^2)^2$, dies ist aber ein Widerspruch zu 3.1.

Schluss

Wiles' Beweis des letzten Fermatsatzes beruht auf der Bestätigung der Taniyama - Shimura - Vermutung aus den fünfziger Jahren. In seiner Argumentation gebraucht er eine Reihe mathematischer Verfahren, die erst in den letzten zehn Jahren entwickelt wurden, zum Teil auch von ihm selbst. Bei seinem Beweis handelt es sich um ein Meisterstück der modernen Mathematik. Fermat schrieb, sein Beweis passe nicht auf den Rand seiner Ausgabe der *Arithmetica* von Diophantos. Diese Aussage trifft sicherlich auch auf Wiles' Beweis zu. Doch kann man andererseits auch mit großer Sicherheit davon ausgehen, dass die Beweise von Wiles und Fermat nicht identisch waren, da Fermat sicher nicht schon vor allen anderen die Modulformen, die Taniyama-Shimura-Vermutung usw. erfunden hat.
Zur Erklärung dieser Tatsache gibt es unter den Mathematikern zwei Meinungen. Die Skeptiker glauben, dass Fermats letzter Satz durch eine seltene Schwäche des Genies entstanden sei und dass ihm wohl bei der Beweisführung ein kleiner Fehler unterlaufen sei. Die Optimisten hingegen glauben daran, dass Fermat einen echten Beweis gefunden haben könnte, der auf den Verfahren des siebzehnten Jahrhunderts beruht und der ein so ausgeklügeltes Argument gebraucht, dass es allen anderen entgangen sei. Diese Frage wird wohl immer unbeantwortet bleiben.[37]

Eine weitere interessante Tatsache ist, „dass Wiles' Lösung einer der letzten heroischen Beweise sein könnte und dass man sich in Zukunft auf rohe Gewalt statt auf elegante Argumentation verlegen wird, um Resultate zu erzielen."[38]
Obwohl Wiles für seinen Beweis viele moderne zahlentheoretische Verfahren einsetzte, verwendete er, wie vor ihm schon Pythagoras und Euler, nur seinen Verstand, Stift und Papier.
Das Problem, das der englische Mathematiker Francis Guthrie im Oktober 1852 in die Welt setzt, war das erste Zeichen für die Veränderung in der Beweisführung. Als er eine Karte der britischen Grafschaften mit Farben

[37] vgl. [4], S.337 f.
[38] Singh 2003, S.326

bemalte, stellte er sich die Frage, wieviele Farben man mindestens benötige, um jede beliebige Karte so zu bemalen, dass keine zwei aneinandergrenzenden Gebiete gleichfarbig sind. Die Frage erschien ihm anfangs trivial, doch er konnte sie nicht lösen. Und es sollte auch einige Zeit vergehen, bis dieses Problem gelöst werden konnte.[39]
Die Geschichte des Problems verlief ähnlich, wie die des Fermatproblems: Die Vermutung konnte zwar für immer kompliziertere Karten bewiesen werden, doch so lange der allgemeine Beweis noch ausstand, konnte jederzeit jemand die Vermutung von Guthrie widerlegen.
Im Juni 1976 wurde Guthries Vierfarbenproblem von Haken und Appel endlich gelöst. Das Bemerkenswerte daran war, dass es sich um den ersten mathematischen Beweis handelte, bei dem ein Computer mehr geleistet hatte, als nur die Rechnung zu beschleunigen. Er hatte soviel zum Ergebnis beigetragen, dass der Beweis ohne ihn nicht möglich gewesen wäre. Es handelte sich dabei zwar um eine gewaltige Leistung, doch machte sich unter den Mathematikern Unbehagen breit, da der Beweis im herkömmlichen Sinne nicht zu überprüfen war.[40]
Man kann also davon ausgehen, dass es einen derartigen Beweis, wie Andrew Wiles ihn führte, in der modernen Mathematik kaum mehr geben wird.

Zum Abschluss möchte ich mich noch recht herzlich bei Herrn Prof. Dr. Rolf Waldi für die gute Zusammenarbeit und freundliche Unterstützung bedanken.

[39] vgl. [4], S.326
[40] vgl. [4], S.333

Literaturverzeichnis

[1] Hardy, Godfrey/ Wright, Edward: Einführung in die Zahlentheorie, Oldenburg, München 1958

[2] Ischebeck, Friedrich: Einladung zur Zahlentheorie, Wissenschaftsverlag, Mannheim 1992

[3] Ribenboim, Paulo: Fermat's Last Theorem for Amateurs, Springer Verlag, New York 1999

[4] Singh, Simon: Fermats letzter Satz. Die abenteuerliche Geschichte eines mathematischen Rätsels, dtv, München 1997

[5] Waldi, Rolf: Elemente der Zahlentheorie und Aufbau des Zahlensystems, Vorlesungsmitschrift, Regensburg SS 2003, http://www.uni-regensburg.de/Fakultaeten/nat_ Fak_ I/Mat4/waldi/vorles-03.html

[6] http://fermats.workjoke.com

[7] http://www.zruser.uni-heidelberg.de/ ci3/fermat.pdf

Abbildungsverzeichnis

Regensburg, den 16.12.2004

Eidesstattliche Erklärung

Ich versichere, dass ich diese Hausarbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benützt habe.

Nina Ramsauer