Pierre de Fermat

******** Nguyen

Januar 2020

Kurs	Seminarkurs Mathematik, Berühmte Mathematiker
Lehrer	******** Schmidt
Abgabetermin	2019-01-08

Inhaltsverzeichnis

Hiermit versichere ich, die vorliegende Arbeit selbstständig und nur unter Zuhilfenahme der angegeben Quellen und Hilfsmittel angefertigt zu haben. Aus den angegebenen Materialien entnommene Inhalte und Zitate sind als solche kenntlich gemacht. Ich erkläre, dass ich zu diesem Thema nicht schon einmal eine solche Arbeit angefertigt habe.

Datum	Unterschrift

1 Vorwort

In dieser Seminararbeit wird der Schwerpunkt auf Fermats Biografie, und auf seinen mathematischen Erfolgen stehen. Der Großteil seiner Arbeit lag in der Zahlentheorie, ein Gebiet welches ich selber gerne mag. Interessant an Fermat ist außerdem, dass er von Beruf her gar kein Mathematiker, sondern Jurist war und Mathematik nur als Nebenhobby gemacht hat. Der biografische Teil wird seine juristische Karriere, aber auch Fermats Charakter beschreiben. Der mathematische Teil wird relativ viele Themengebiete decken, insgesamt Kurvenanalyse, Optik, Stochastik und Zahlentheorie. Der größte Fokus wird hierbei auf der Zahlentheorie liegen. Wer sich noch nicht viel mit Mathematik beschäftigt hat wird hier auf unbekannte Begriffe und Symbole treffen, daher sind im Glossar auf Seite 18 und im Symbolverzeichnis auf Seite 19 viele dieser aufzufinden sein.

2 Biografie

In diesem Abschnitt wird das Leben von Pierre de Fermat beschrieben.

2.1 Eltern

Fermats Vater war Dominique Fermat, ein reicher Verkäufer und Hersteller. Dominique tat sein Bestes um die Familie in Reichtum aufblühen zu lassen, indem er Tauschhandel mit verschiedenen Ländern trieb. Dabei handelte er mit landwirtschaftlichen Erzeugnissen, wie z.B. Weizen, Wein, Vieh und anderen Tierprodukten. Sein Geschick und sein Ansehen haben ihn so reich werden lassen wie er geworden ist. Pierres Mutter war Claire De Long, die zweite Frau Dominiques, welche aus einer edlen Familie von Juristen kam. Durch Dominiques Ehe mit Claire De Long hatte sich die Familie außerdem die Möglichkeit bekommen, einen Platz im hohen Strafgericht von Toulouse für die beiden Söhne, Pierre und Clement, zu ergattern. Sie starb als Pierre nur sieben Jahre alt war.

2.2 Kindheit

Abbildung 1: Pierre de Fermat [1]

Eines von Pierre de Fermats Rätseln ist bereits seine Geburt. In vielen Quellen wird beschrieben, dass seine Geburt 1601 in Frankreich sei. In diesem Gedanken hat man dann auch sein 400. Jubiläum im Jahr 2001 gefeiert. Seine Geburt hat sich aber schlussendlich als 1607 herausgestellt. [2] Grund für diese Verwechslung war wahrscheinlich sein verstorbener Halbbruder, welcher ebenfalls Pierre Fermat hieß, dann 1601 geboren war und noch in der Kindheit gestorben ist. [3] Seine Karriere war von seinen Eltern bereits lange vorausgeplant, es ging ausschließlich darum sich einen Platz als parlamentarischen Berater, einem sogenannten *„Conseiller“*, in Toulouse oder Bordeaux zu erkaufen. Dafür muss man mehrere Jahre Jura studiert, einen Abschluss darin gemacht, dann noch mehrere Jahre als Anwalt, entweder in Toulouse oder Bordeaux, verbracht haben und zum Schluss eine Menge Geld aufbringen um den Platz zu erwerben. Er hat den Großteil seiner Kindheit an einer sprachenzentrierten Schule verbracht, welche er im Alter von 16 Jahren abgeschlossen hatte. Dabei hat er wichtige Sprachen wie Griechisch, Latein, Italienisch und weitere gelernt und konnte diese auch flüssig sprechen,

welche ihm in der späteren Laufzeit als Anwalt den Weg bahnen würde.

2.3 Studium

Orléans war als die Stadt bekannt, an der man am besten Zivilrecht studieren würde. Nicht nur in Frankreich, sondern in ganz Europa. Ein Abschluss von dort wurde als sehr hoch angesehen. Dort hat er dann auch an der Universität von Orléans im August 1626 seinen Abschluss gemacht, als er nur 18 Jahre alt war. Darauf folgend hat sich Fermat im Strafgericht von Bordeaux einen Platz geschaffen. Er hat in Bordeaux die vier Jahre Praxiserfahrung als Anwalt, die für die Position des *Conseillers* notwendig sind, erhalten. Eigentlich war Toulouse eine ersichtlichere Wahl gewesen, aber er hatte sich für Bordeaux für den Mathematiker-Kreis entschieden, der sich dort gebildet hatte. Er hatte nämlich damals schon Interesse an der Mathematik gefunden und ist auf die Empfehlung seines Freundes nach Bordeaux gegangen.

2.4 Aufstieg zum Conseiller

Als sein Vater Dominique Fermat im Juni 1628 gestorben ist, bekam Pierre den Großteil des Erbes und hat damit großen Reichtum erlangt. Er bekam mit dem Erbe sechs Bauernhöfe, so wie mehrere andere Grundstücke. Danach hatte er auf eine Gelegenheit gewartet, um sich einen Platz als *Conseiller* in Toulouse zu erkaufen, um dem Plan seiner Eltern nachzugehen. Diese Gelegenheit bot sich ihm, als 1630 ein Großteil der Berater einer Pest niedergefallen sind. Solch einen Platz zu erkaufen war keineswegs billig und nur mithilfe des Erbes seines Vaters möglich. Ein einfacher Bauer hatte damals 100 Livre im Jahr verdient, während man mit dem Platz als Berater leicht mehr als 45.000 Livre los wird.

Im Jahr 1631 saß er dann endlich in seinem Büro als echter *Conseiller*, durfte nun das *„de“* in seinem Namen tragen und hieß damit offiziell „Pierre de Fermat“ und nicht nur „Pierre Fermat“, ein Privileg wovon er persönlich aber nie Gebrauch gemacht hat. Um diese Zeit hat er auch seine Cousine, Louise de Long, geheiratet. Sie war zum Zeitpunkt der Hochzeit nur 15 Jahre alt. Insgesamt hatte er acht Kinder mit ihr, von denen nur fünf erwachsen geworden sind. 1637 stieg er zu einer höheren Position im Toulouser Strafgericht auf, diese Position hat er dann bis zu seinem Lebensende 1665 behalten. Mehr zu seiner Karriere als *Conseiller* lässt sich in der Dezember 2001 Ausgabe der European Mathematical Society (EMS) finden. [4]

2.5 Mathematik

Wie für viele andere Mathematiker in der Zeit war die Mathematik für ihn nur eine Nebenbeschäftigung, da es den Beruf „Mathematiker“ an sich noch nicht wirklich gab. Er hat zwar während seines Jura-Studiums in Orléans bereits Interesse an der Mathematik gefunden und sie auch aktiv verfolgt, aber weiterhin seinen Fokus auf das Anwaltsleben gelegt. Nach seinem Aufstieg als Berater hat er begonnen mit verschiedenen älteren Werken zu arbeiten, indem er sie restaurierte bzw. rekonstruierte. Oft hatte er mit anderen Mathematikern über einen Briefaustausch Kontakt, darunter René Descartes, Blaise Pascal und weitere. Auch wenn er nur ein Hobbyist war und als Amateur bezeichnet wird, wird er als der größte Amateur-Mathematiker aller Zeiten angesehen. [5, 6] Wie genau er zur Mathematik beigetragen hat, wird in Kapitel 3 behandelt.

2.6 Als Person

Er hat viele wichtige Dinge entdeckt, aber hatte selten das Verlangen diese zu veröffentlichen. Sein Sohn, Clement Samuel de Fermat, hatte nach Pierres Tod einige seiner Briefe und Randnotizen veröffentlicht. Sein Charakter findet sich auch in eben diesen Notizen wieder.

Im Briefaustausch mit anderen Mathematikern wurden sie oft von ihm aufgefordert ein bestimmtes Problem zu lösen, meist eines zu welchem er bereits eine Lösung hatte. Er bat sie also nicht einfach um Hilfe, sondern wollte nur schauen, wie schnell sie das Problem lösen konnten. Oder er hat eine Aufgabe mit dem Resultat, aber ohne den Lösungsweg präsentiert, falls er denn doch mal etwas veröffentlicht hatte. Seinen Charakter könnte man gut als leicht arrogant bezeichnen.

Auch hat er immer behauptet eine bestimmte Behauptung bewiesen zu haben,schrieb aber nie den Beweis dafür auf. Darunter gehören zum Beispiel auch der Zwei-Quadrate-Satz und Fermats großer Satz, welche beide in Kapitel 3.4 behandelt werden. Am bekanntesten wird wohl für immer folgende Behauptung bleiben, welcher als Kommentar am Buchrand in seiner Kopie von *„Arithmetica“* von Diophantus verfasst war. Dieser würde dann zu seiner berühmtesten Problemstellung werden, welche in Kapitel 3.4.4 näher behandelt wird.

> *„Ich habe einen wahrlich wunderbaren Beweis für dieses Problem entdeckt, für den dieser Buchrand zu eng ist.“*

3 Beiträge zur Mathematik

In diesem Abschnitt werden ein paar von Pierre de Fermats wichtigsten Beiträge zur Mathematik vorgestellt. Er war in vielen Teilgebieten der Mathematik aktiv.

3.1 Kurvenanalyse

1629 schon, als er nur 19 Jahre alt war und noch in Orléans studiert hatte, hatte er Interesse an der Mathematik gewonnen. Er begann verschiedene alte Bücher diesbezüglich zu lesen und auch zu rekonstruieren. Pierre de Fermat und René Descartes haben unabhängig voneinander, aber nahezu zeitgleich, die Grundbausteine für die analytische Geometrie gelegt. Die analytische Geometrie beschreibt das Lösen geometrischer Probleme mit einem kartesischem Koordinatensystem, welches allgemein ein für uns heute noch einfaches Koordinatensystem mit x- und y-Achse beschreibt. Das Konzept eines kartesischen Koordinatensystems, welches von Descartes entwickelt wurde (und auch nach ihm benannt ist) war revolutionär und daher grundlegend für die analytische Geometrie. Fermats Idee war es, verschiedene geometrische Formen bestimmten algebraischen Formeln zuzuweisen, welche das zweite bahnbrechende Konzept der analytischen Geometrie bilden.

Im Alter von 21 machte er mit seinem Werk *„Methodus ad disquirendam maximam et minimam et de tangentibus linearum curvarum“*[1] seinen ersten, aber auch einer der wichtigsten, Beiträge zur analytischen Geometrie sowie zur Differentialrechnung. Ein aus dem Lateinischen ins Englische übersetzter Artikel ist in [7] zu finden. Die Ergebnisse dieser hatte Fermat bisher nur im Briefaustausch mit anderen Mathematikern geteilt, erst 1636 ist es in Form eines Manuskripts veröffentlicht worden. Dabei hat er ein Verfahren entwickelt, mit welchem sich Maxima, Minima und Tangenten zu verschiedenen Arten von Kurven finden lassen, welches gleich zur heutigen Differentialrechnung ist. Aus seinen Ergebnissen ist er einen Schritt weiter gegangen und hat als Erstes die Fläche einer Funktion von verschiedenen Potenzfunktionen gefunden, welches der Grundansatz der Integralrechnung war. Die daraus folgende Formel wurde von Newton und Leibniz verwendet, um unabhängig voneinander den Fundamentalsatz der Analysis zu erstellen, welcher die Konzepte der Ableitung und der Integration miteinander verbindet.

[1] Methoden zur Bestimmung von Minima und Maxima und Tangenten an Kurven

3.2 Optik

Fermat war mit dem Gesetz der Brechung in der Optik, welches Descartes in 1637 in seinem Werk vorgestellt hatte, unzufrieden. Dies, zusammen mit dem gleichzeitigen Erscheinen der beiden Werke über die analytische Geometrie, entfachte eine Rivalerie zwischen den Beiden. 20 Jahre später hat Fermat das Problem neu behandelt und ist zu dem Schluss gekommen, dass Licht nicht den *kürzesten* Weg, sondern den Weg der kürzesten Zeit nimmt. Dies wird auch das „Fermatsche Prinzip“ genannt. Daraus ließ sich das Brechungsgesetz bilden, welches wir heute kennen. Dabei ist das Verhältnis der Sinusse der Eintritts- und Austrittswinkel gleich dem Verhältnis der Geschwindigkeiten, indem sich das Licht in beiden Medien bewegt, also $\frac{\sin\alpha}{\sin\beta} = \frac{c_1}{c_2}$. Das Beispiel einer Brechung hat man schon als Kind betrachten können, bei dem ein Strohhalm der ins Wasser ragt einen anderen Eintrittswinkel als Austrittswinkel besitzt. Wenn die Lichtgeschwindigkeit in einem Vakuum nun ca. $c_1 = 3 \cdot 10^8$ beträgt, aber die Lichtgeschwindigkeit im zu übergehenden Medium $c_2 = 2 \cdot 10^8$ beträgt, dann beträgt das Verhältnis von $\frac{c_1}{c_2} = \frac{3}{2}$. Da das Verhältnis der Sinusse gleich dem Verhältnis der Geschwindigkeiten sein muss, wäre beim Eintrittswinkel $\alpha = 30°$ der Austrittswinkel $\beta = 19.47°$, da $\beta = \arcsin(\sin(20°)/\frac{3}{2}) = 19.47°$, wie in Abbildung 2 zu sehen.

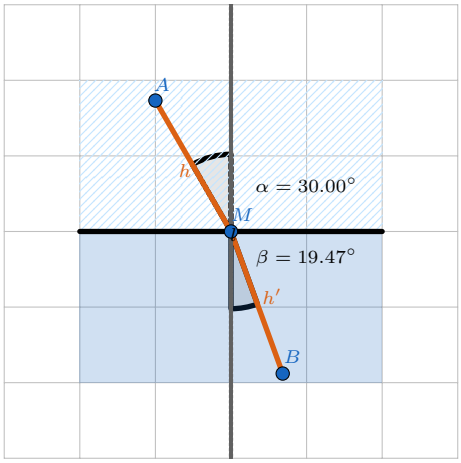

Abbildung 2: Beispiel einer Brechung

3.3 Stochastik

Blaise Pascal, ein weiterer wichtiger Mathematiker aus dieser Zeit, war ein Brieffreund von Fermat. Gemeinsam haben sie in 1654 den Grundstein für die heutige Stochastik gelegt. Pascal hatte Fermat zwei Problemstellungen anvertraut, die sich mit dem damaligen Glücksspiel befassten. Man muss bedenken, dass es damals noch kein Konzept von Stochastik gab wie es heute existiert. Damals konnte man nur grob abschätzen, dass bei einem sechs-seitigen Würfel die Chance auf eine Sechs eben $\frac{1}{6}$ beträgt. Dass die Chance auf einen Sechser-Pasch $\frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36}$ beträgt ist für uns heutzutage selbstverständlich, war damals aber eine revolutionäre Entdeckung. Eine Übersetzung des Briefaustausches zwischen Fermat und Pascal in 1654 findet sich in [8].

3.3.1 Würfelproblem

Chevalier de Méré hatte Pascal gefragt, ob es profitabel wäre, auf einen Sechser-Pasch in 24 Würfen zu wetten. Nach den damaligen Faustregeln wäre es nämlich profitabel gewesen, rein mathematisch gesehen aber nicht. Wie erwähnt ist die Chance auf einen Sechser-Pasch $\frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36}$, die Chance *keinen* Sechser-Pasch zu würfeln daher $1 - \frac{1}{36} = \frac{35}{36}$. Die Chance 24-mal hintereinander keinen Sechser-Pasch zu bekommen ist $(\frac{35}{36})^{24} = 0.5086$, also etwas mehr als die Hälfte. Da die Chance auf einen Sechser-Pasch in 24 Würfen demnach $1 - (\frac{35}{36})^{24} = 0.4914$ ist, also unter $\frac{1}{2}$ liegt, ist das Spiel also nicht profitabel. Das Konzept der Multiplikation, Potenzierung und Addition von Wahrscheinlichkeiten ist im Briefaustausch zwischen Pascal und Fermat entstanden.

3.3.2 Teilungsproblem

Das bekanntere (und auch interessantere) der beiden Probleme ist folgender:

> Zwei Spieler spielen ein Glücksspiel gegeneinander, bei dem jeder Spieler in jeder Runde die gleiche Chance zu gewinnen hat und welches auf mehrere Runden gespielt wird. Beide legen einen Wetteinsatz fest, sodass sich im Pot dann der insgesamt zweifache Wetteinsatz befindet. Es wird solange gespielt, bis einer der Spieler n-mal gewonnen hat, der Gewinner bekommt den gesamten Pot, während der Verlierer nichts bekommt (Alles oder nichts). Was aber nun, wenn das Spiel aufgrund eines Außeneinflusses beim Spielstand $a : b$ abgebrochen werden muss? Wie verteilt man dann am gerechtesten den Pot?

Zum einen könnte man vorschlagen, dass der Pot $1:1$ wieder an die Spieler zurückgegeben wird. Dann könnte aber der Spieler in Führung argumentieren, dass dieser den gesamten Pot bekommen solle, da er doch in Führung lag und sicher gewonnen hätte. Beide Lösungen sind nicht falsch, aber auch beide nicht richtig. Die Lösung, die Fermat und Pascal vorgeschlagen haben, berechnet die Gewinnwahrscheinlichkeiten der jeweiligen Spieler und teilt den Pot im Verhältnis der Wahrscheinlichkeiten auf. Fermat ist auf den Gedanken gekommen, dass es irrelevant sei, wie viele Runden man schon gewonnen hatte, sondern es einzig und allein relevant sei, wie viele Runden man zum Sieg noch braucht. Wenn ein Spieler nun noch $r = n - a$ Runden gewinnen muss und der andere Spieler $s = n - b$ Runden, dann ist das Spiel nach maximal $r + s - 1$ Runden vorbei. Beim Spielstand $3:2$ bis zu 5 Punkten braucht es also maximal $2 + 3 - 1 = 4$ Runden. Da jeder Spieler die gleiche Chance zu gewinnen hat, gibt es 2^{r+s-1} Möglichkeiten, wie sich das Spiel entwickeln könnte. Fermat konnte also alle Möglichkeiten tabellarisch notieren, zählen bei welchen welcher Spieler gewinnen würde und damit die Proportionen der Gewinnchancen nutzen um den Pot zu verteilen.

Pascal hatte den Ansatz noch verbessert, da je größer $r + s - 1$, desto exponentiell schwerer wird es die gesamte Tabelle zu schreiben. Mit dem pascalschen Dreieck, welches er damals entwickelt hatte, sowie einer Summenformel, ist er auf folgende Formel gekommen, wobei $\binom{r+s-1}{k}$ den Binomialkoeffizienten darstellt:

$$\sum_{k=0}^{r-1} \binom{r+s-1}{k} : \sum_{k=0}^{s-1} \binom{r+s-1}{k}$$

Beim Beispiel von $3:2$ bis 5 Punkten wäre das also ein Verhältnis von $11:5$ bzw. $0.6875:0.3125$.

3.4 Zahlentheorie

Auch wenn Fermat wichtige Beiträge zur Analysis und zur Stochastik geleistet hat, finden sich seine größten und bekanntesten Werke im Gebiet der Zahlentheorie. Dies war Fermats Lieblingsgebiet. Dabei spielt das Buch *„Arithmetica“* von Diophantus eine wichtige Rolle, da es viele Ideen von Fermat im Gebiet der Zahlentheorie entfacht hat. Oft hat er Notizen oder neue Ideen an den Rand seiner Kopie von Arithmetica geschrieben. Die Bekanntesten seiner Ideen werden folgend vorgestellt. Wenn nicht anders beschrieben, dann sind alle Variablen grundsätzlich eine ganze Zahl ($\mathbb{Z}$).

Um die Kapitel 3.4.1 und 3.4.2 besser zu verstehen, muss das Konzept der Kongruenz in der Zahlentheorie erklärt werden. Für die Kongruenz wird das Symbol $\equiv$ verwendet. Grundlegend wird die Schreibweise „$a \equiv b \pmod{m}$“ benutzt (sprich „a und b kongruent modulo m“), welche beschreibt, dass der Rest von $\frac{a}{m}$ und $\frac{b}{m}$ gleich ist. Als Beispiel kann lässt sich „$9 \equiv 17 \pmod{8}$“ nehmen, da $9 : 8 = 1$ Rest 1 und $17 : 8 = 2$ Rest 1. Im Endeffekt ist es aber nichts anderes als $(a \bmod m) = (b \bmod m)$.

3.4.1 Zwei-Quadrate-Satz

Fermat hat folgendes behauptet:

> Eine ungerade Primzahl kann als eine Summe von zwei Quadraten $p = x^2 + y^2$ dargestellt werden, wobei x und y natürlich sind, wenn, und nur wenn $p \equiv 1 \pmod{4}$.

Zur Einfachheit halber lässt sich die Bedingung „$p \equiv 1 \pmod{4}$“ auch als „Wenn p als $4n + 1$ darstellbar ist“ umformulieren. Schauen wir uns ein paar Beispiele an.

- 17 ist prim und kann als $4 \cdot 4 + 1$ dargestellt werden, daher ist der Zwei-Quadrate-Satz anwendbar: $17 = 4^2 + 1^2 = 16 + 1$
- 29 ist prim und ist $4 \cdot 7 + 1$: $29 = 5^2 + 2^2 = 25 + 4$
- 37 ist prim und ist $4 \cdot 8 + 1$: $37 = 6^6 + 1^2 = 36 + 1$
- 7 ist prim, kann aber nicht als $4n + 1$ dargestellt werden, daher ist 7 auch nicht als eine Summe von zwei Quadraten darstellbar.

Fermat hatte behauptet, den Zwei-Quadrate-Satz mit der Methode des unendlichen Abstiegs bewiesen zu haben. Eine Erklärung der Methode ist im Glossar zu finden. Er hat aber,wie man es von ihm gewohnt war, keinen Beweis niedergeschrieben. Der erste Beweis kam von Leonhard Euler 1747, nachdem er mehrere Jahre damit verbracht hatte einen Beweis zu finden. Dieser hatte ebenfalls den unendlichen Abstieg genutzt. Mittlerweile existieren verschiedene Beweise, die auf verschiedenen Konzepten basieren, darunter ein Beweis welcher gaußsche Zahlen nutzt [9], oder auch ein Beweis in einem einzigen Satz. [10]

3.4.2 Faktorisierungsmethode

Die Faktorisierungsmethode von Fermat findet die Faktoren einer natürlichen ungeraden Zahl n, die aus mindestens zwei Primzahlen zusammengesetzt ist.

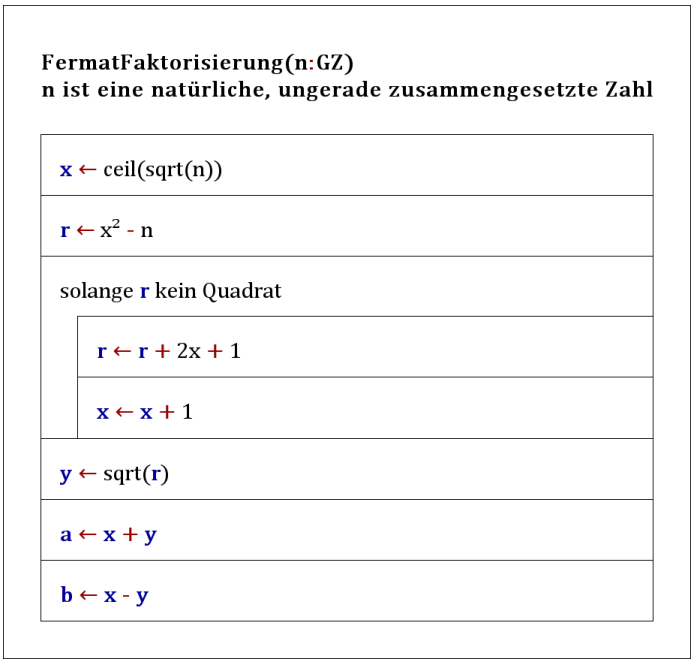

Abbildung 3: Algorithmus von Fermats Faktorisierungsmethode in einem Struktogramm

Wenn die Faktorisierung von n nun $n = a \cdot b$ ist, dann ist der Algorithmus für die Faktorisierungsmethode wie in Abbildung 3 beschrieben. Dabei ist folgender Fakt grundlegend für die Faktorisierung:

Hypothese. *Jede ungerade Zahl kann als eine Differenz von zwei Quadraten dargestellt werden.*

Beweis. Wenn man nun annimmt, dass sich eine ungerade Zahl n auch als

$$n = x^2 - y^2 \tag{1}$$

schreiben lässt, ist es möglich mit der dritten binomischen Formel die Gleichung zu

$$n = (x + y)(x - y) \tag{2}$$

umzuschreiben. Nun setzt man eine Variable a und b gleich der beiden Faktoren aus (2), sodass $a = x + y$ und $b = x - y$. Wenn man nun auf x und y auflöst, dann bekommt man $x = \frac{a+b}{2}$ und $y = \frac{a-b}{2}$. Eingesetzt in (1) ergibt es

$$
\begin{aligned}
n &= \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 \\
&= \frac{a^2 + 2ab + b^2 - a^2 + 2ab - b^2}{4} \\
&= \frac{4ab}{4} = ab
\end{aligned}
$$

Somit kann jede ungerade Zahl kann als eine Differenz von zwei Quadraten dargestellt werden.

□

Dies wird nun genutzt, es wird solange eine Zahl y gesucht, bis diese eine Quadratzahl ist. Da jede ungerade Zahl als Differenz von zwei Quadraten dargestellt werden kann und eine dann bereits gefunden wurde, lässt sich die andere leicht durch Subtraktion finden. Nun hat man zwei Faktoren a und b von n gefunden. Da n ungerade ist, müssen die beiden Faktoren auch ungerade sein, da n sonst gerade wäre. Wenn a oder b noch keine Primzahlen sind, dann kann man die gleiche Methode nutzen, um für jeweils a oder b die Faktoren zu finden. So hat Fermat bereits 1643 eine Primfaktorzerlegung von der Zahl 2.027.651.281 durchgeführt. Auch dieser Beweis wurde von Fermat mit ins Grab genommen.

3.4.3 Kleiner Satz

Fermats kleiner Satz ist der zweitbekannteste von Fermats Werken, nach dem großen Satz, er wird „klein“ genannt, um ihn nicht mit dem Großen zu verwechseln. Dieser wurde 1640 in einem Brief von Fermat zu Bernard Frénicle de Bessy vorgestellt. Fermat hat den Satz als folgende Aussage vorgestellt:

> Wenn p prim und $a \nmid p$ (a nicht durch p teilbar), dann gilt
>
> $$a^{p-1} \equiv 1 \pmod{p} \tag{3}$$

Dies kann man auch als

> Wenn p prim und a ganzzahlig, dann gilt
>
> $$a^p \equiv a \pmod{p} \tag{4}$$
>
> sodass $a^p - a$ ein Mehrfaches von p sein muss.

formulieren, auch wenn die Anfangsbedingungen offener aussehen. Dies ist möglich, da die Formel 3 voraussetzt, dass $a \nmid p$. Daher muss es auch eine Zahl b geben, sodass $ab \equiv 1 \pmod{p}$, da a ansonsten keinen Teiler hätte. Wenn also nun $a^p \equiv a \pmod{p}$ und beide Seiten mit b multipliziert werden, lässt sich auf beiden Seiten ein a herauskürzen und es kommt $a^{p-1} \equiv 1 \pmod{p}$ heraus, welches somit äquivalent zu Formel 4 ist. Ein paar Beispiele:

- Wenn $a = 2$ und $p = 5$, dann $2^5 = 32 = 2 \cdot 16$. Damit lässt sich 2^5 als ein Mehrfaches von 2 darstellen.
- Wenn $a = 5$ und $p = 13$, dann $5^{13} = 1220703125 = 5 \cdot 244140625$.
- $a = 35$ und $p = 19$: $35^{19} = 21741667147394453048706054687 5$
  $= 35 \cdot 621190489925555801391601562 5$

Mittlerweile gibt es einige Methoden um den Satz zu beweisen. Anders als der Beweis des großen Satzes von Fermat, passt der des kleinen Satzes leicht auf die Rückseite einer Postkarte. Da alle aber für den durchschnittlichen Leser etwas schwerer zu verstehen sind, werde ich darauf verzichten einen zu umfassen. Ein Beweis mit dem binomischen Lehrsatz lässt sich in [11] finden. Der Beweis von Fermat selber ist, wie man es sich schon denken kann, nirgendwo zu finden.

Auf dem kleinen Satz aufbauend ist der Satz von Euler, welcher eine Verallgemeinerung des kleinen Satzes darstellt, wobei p nicht prim sein muss. Der kleine Satz wird heutzutage als Basis für den fermatschen Primzahltest und in der heutigen Kryptografie als Basis der RSA-Verschlüsselung genutzt.

3.4.4 Großer Satz

Der große Satz von Fermat, auch „Fermats letzter Satz“ oder „Fermatsche Vermutung“ genannt, ist sein bekanntestes Problem. Der Name „Fermats letzter Satz“ kommt nicht daher, dass es wortwörtlich der letzte Satz war den er aufgestellt hatte, sondern weil es der Satz von Fermat war, der als letztes bewiesen wurde. Den großen Satz bzw. die Problemstellung, sowie den Beweis, hat er selbst nie veröffentlicht. Erst fünf Jahre nach seinem Tod hat einer seiner Söhne die zahlreichen Randnotizen in Fermats Kopie von Diophantus „Arithmetica“ gefunden und veröffentlicht. Aufgestellt in ca. 1637 findet sich folgende Notiz am Rande:

> *„Es ist unmöglich eine Zahl dritter Potenz in zwei Zahlen dritter Potenzen, oder eine Zahl vierter Potenz in zwei Zahlen vierter Potenzen, oder allgemein, jede Potenz höher als 2 in die zwei gleichen*

zu zerlegen. Ich habe einen wahrlich wunderbaren Beweis für dieses Problem entdeckt, für den dieser Buchrand zu eng ist.“

Allgemein formuliert bedeutet das:

Die Gleichung $x^n + y^n = z^n$ mit $n, x, y, z \in \mathbb{N}$ hat für $n > 2$ keine ganzzahlige Lösung.

Dass es für $n = 2$ unendlich viele Lösungen gibt, wussten schon die Griechen. Man muss nur das Stichwort „Satz des Pythagoras“ sagen und es sollte einem direkt die Zahlengruppe $3, 4, 5$ einfallen, welche für $n = 2$ die gültige Lösung $3^2 + 4^2 = 5^2$ bildet. Zwar hat Fermat nicht den gesamten Satz bewiesen, dafür aber den Fall $n = 4$ mit seiner eigen entwickelten Methode des unendlichen Abstiegs, dessen Beschreibung im Glossar zu finden ist.

Einfach zu verstehen wie er war, haben viele Mathematiker versucht den großen Satz von Fermat zu beweisen, jedoch sind alle am Versuch gescheitert. Über mehrere Jahrhunderte blieb die Lösung ein Mysterium. Erst 350 Jahre später hat Andrew Wiles 1995 einen kompletten Beweis des großen Satz von Fermat veröffentlicht. Dieser war schon seit seiner Kindheit, als er zehn Jahre alt war, von der Einfachheit des großen Satzes fasziniert und hat sich seitdem vorgenommen, diesen als Erstes zu beweisen. Da er aber schnell gemerkt hatte, dass es mit seinem mathematischen Wissen zu dieser Zeit nichts werden könne, hat er, erst nachdem er 33 geworden war, die Suche fortgesetzt. Nach mehr als 6 Jahren geheimgehaltener und akribischer Forschung hatte er 1993 den Beweis vorgetragen, mit dem Titel „Modular Forms, Elliptic Curves and Galois Representations.“. Dieser hatte sich nicht anmerken lassen, dass es sich hierbei um den Beweis Fermats großen Satz handelt. Erst am Ende des dritten und letzten Vortrags hat er nebenbei angemerkt, dass er nun den Satz bewiesen hatte. [12] Im August wurde aber ein Fehler im Beweis entdeckt, den Wiles erst in September 1994 korrigieren konnte und Mai 1995 dann neu veröffentlicht hat. Für den Beweis hat er viele Preise und Auszeichnungen erhalten und er gilt als eines der wichtigsten Fortschritte der modernen Mathematik.

Den großen Satz hier zu beweisen würden den kompletten Rahmen der Arbeit sprengen. Wer einen Blick in Wiles 109 Seiten langen Beweis werfen möchte, findet diesen in [13]. Der Beweis behandelt den Modularitätssatz (früher auch „Taniyama-Shimura-Vermutung“ genannt) und elliptische Kurven. Wiles beweist den schwierigsten Teil davon, welches gleichzeitig den großen Satz impliziert. Der vollständige Beweis des Modularitätssatzes ist 2001 gefunden worden. Ein Buch, welches den großen Satz und damit auch den Modularitätssatz weiter im Detail behandelt findet sich hier [14].

Der Beweis des großen Satzes wurde erst nach 6 Jahren Forschungen mit mathematischen Mitteln des 20. Jahrhunderts gefunden, daher ist man sich heutzutage einig, dass Fermat zwar behauptet hat einen Beweis gefunden zu haben, aber doch nie einen hatte oder dass sein Beweis fehlerhaft war.

Glossar

Algebra Themengebiet der Mathematik, welches die Eigenschaften von Rechenoperation umfasst und mit Unbekannten in Gleichungen arbeitet. 8

Analysis Themengebiet der Mathematik, welches die Untersuchung von Funktionen beschreibt und die Methoden der Differentialrechnung und Integralrechnung, basierend auf der Infinitesimalrechnung. 8

analytische Geometrie Themengebiet der Mathematik, welches die Geometrie innerhalb eines Koordinatensystems umfasst. 8, 9

Binomialkoeffizient Anzahl der k-elementigen Teilmengen einer n-elementigen Menge, geschrieben als $\binom{n}{k}$ sprich „n über k“. 11

Brechung Auch Refraktion genannt, beschreibt die Veränderung der Richtung des Lichts bei einem Übergang in ein anderes Medium, in welchem es sich mit anderer Geschwindigkeit bewegt. 9

Differentialrechnung Teil des mathematischen Themengebiets Analysis, welches sich mit der Berechnung lokaler Veränderungen von Funktionen beschäftigt (Ableitung, Minima, Maxima etc.), basierend auf der Infinitesimalrechnung. 8, 18

Faktor Bestandteile einer Multiplikation. 13

Infinitesimalrechnung Methode, um eine Funktion auf unendlich kleinen (infinitesimalen) Schritten zu beschreiben, Grundbaustein der Differentialrechnung und Integralrechnung. 18

Integralrechnung Teil des mathematischen Themengebiets Analysis, welches sich mit der Berechnung von Volumen oder Flächen von Funktionen beschäftigt, basierend auf der Infinitesimalrechnung. 8, 18

Kongruenz Die Beziehung zwischen zwei Zahlen, dessen Modulo mit demselben Divisors identisch ist. 12

Methode des unendlichen Abstiegs Eine von Fermat entwickelte Methode, welche einen Beweis durch Widerspruch beschreibt, bei dem ein kleinstes Element in einer Zahlenmenge vorhanden sein muss, dem aber nicht so ist, oder umgekehrt, dass es kein kleinstes Element geben soll, aber eines existiert. Ähnlich zu einem Beweis durch Induktion. 12, 16

Modulo Der Rest einer Division zweier Zahlen. 18

Natürliche Zahl Alle Zahlen, mit deren Hilfe beliebige Objekte gezählt werden können ($\mathbb{N} = \{1, 2, 3, 4, \dots\}$). 12, 13

Optik Themengebiet der Physik, welches die Lehre des Lichts darstellt. 9

Pascalsches Dreieck Form der grafischen Darstellung der Binomialkoeffizienten in einem Dreieck, bei dem jeder Eintrag die Summe der zwei darüberstehenden Einträge ist. 11

Primzahl Eine natürliche Zahl, die ausschließlich durch 1 und sich selbst geteilt werden kann. 12–15

Quadratzahl Eine Zahl, die durch die Multiplikation einer ganzen Zahl mit sich selbst entsteht. 12–14

Stochastik Themengebiet der Mathematik, welches die Wahrscheinlichkeitsrechnung, sowie die Mathematische Statistik zusammenfasst. 10

Zahlentheorie Themengebiet der Mathematik, welches sich mit Eigenschaften ganzer Zahlen beschäftigt. 11, 12

Symbolverzeichnis

$\binom{n}{k}$ Binomialkoeffizient, sprich „n über k“

$\equiv$ Kongruenz, Beispiel „$a \equiv b \pmod{m}$“, sprich „a und b sind kongruent modulo m“, bei der Division durch m besitzen a und b den gleichen Rest

$\in$ Element einer Menge, Beispiel „$n \in \{2, 4, 5\}$“, sprich „n ist ein Element von $\{2, 4, 5\}$“

$\sum$ Summe, griechischer Buchstabe Sigma, Beispiel $\sum_{n=1}^{10} n^2$ quadriert alle Zahlen von 1 bis 10 und addiert diese ($1^2 + 2^2 + \ldots + 10^2 = 385$)

$a \mid b$ Ganzzahlige Teilbarkeit, sprich „a ist durch b teilbar“

$a \nmid b$ Verneinung von $a \mid b$

c Lichtgeschwindigkeit, ca. $3 \cdot 10^8 \frac{m}{s}$

Literatur

[1] unbek. *Pierre de Fermat.* (letzter Zugriff: 2020-01-06). URL: https://commons.wikimedia.org/wiki/File:Pierre_de_Fermat.jpg.

[2] Friedrich Katscher. *When Was Pierre de Fermat Born?* (letzter Zugriff: 2020-01-06). 2016. URL: https://www.maa.org/press/periodicals/convergence/when-was-pierre-de-fermat-born.

[3] Famous Scientists. *Pierre de Fermat.* (letzter Zugriff: 2020-01-06). 2014. URL: https://www.famousscientists.org/pierre-de-fermat/.

[4] Friedrich Katscher. „EMS Newsletter December 2001". In: (2001). (letzter Zugriff: 2020-01-06), S. 12–16. URL: http://www.emis.de/newsletter/newsletter42.pdf.

[5] L. Mlodinow. *Wenn Gott würfelt: oder Wie der Zufall unser Leben bestimmt.* Rowohlt E-Book, 2011. ISBN: 9783644009516. URL: https://books.google.de/books?id=fcuKAgAAQBAJ.

[6] Carl B. Boyer. *Pierre de Fermat.* (letzter Zugriff: 2020-01-06). 2019. URL: https://www.britannica.com/biography/Pierre-de-Fermat.

[7] Pierre de Fermat. „Method for the Study of Maxima and Minima". In: (1629). (letzter Zugriff: 2020-01-06). URL: https://science.larouchepac.com/fermat/fermat-maxmin.pdf.

[8] Blaise Pascal Pierre de Fermat. „Fermat and Pascal on probability". In: (1654-1660). (letzter Zugriff: 2020-01-06). URL: https://www.york.ac.uk/depts/maths/histstat/pascal.pdf.

[9] George Robert Woodbury. „The representation of a number by two or four squares". In: (2012). (letzter Zugriff: 2020-01-06), S. 2–4. URL: https://math.uchicago.edu/~may/REU2012/REUPapers/Woodbury.pdf.

[10] D. Zagier. „A One-Sentence Proof That Every Prime p congruent to 1 modulo 4 Is a Sum of Two Squares". In: (unbek.). (letzter Zugriff: 2020-01-06, Jahr wird auf 2002 geschätzt). URL: https://web.archive.org/web/20120205194801/http://www.math.unh.edu/~dvf/532/Zagier.

[11] Eric W. Weissstein. *Fermat's Little Theorem.* (letzter Zugriff: 2020-01-06). URL: http://mathworld.wolfram.com/FermatsLittleTheorem.html.

[12] Gina Kolata. *At Last, Shout of 'Eureka!' In Age-Old Math Mystery.* (letzter Zugriff: 2020-01-06). Juni 1993. URL: https://www.nytimes.com/1993/06/24/us/at-last-shout-of-eureka-in-age-old-math-mystery.html.

[13] Andrew John Wiles. „Modular elliptic curves and Fermat's Last Theorem“. In: (1995). (letzter Zugriff: 2020-01-06). URL: http://scienzamedia.uniroma2.it/~eal/Wiles-Fermat.pdf.

[14] Henri Darmon, Fred Diamond und Richard Taylor. „Fermat's Last Theorem“. In: (1995). URL: https://www.intlpress.com/site/pub/files/_fulltext/journals/cdm/1995/1995/0001/CDM-1995-1995-0001-a001.pdf.