SUMMEN VON QUADRATZAHLEN, SUMMEN VON KUBIKZAHLEN

D. Zagier

Die Zahlentheorie gehört neben der Geometrie zu den ältesten Gebieten der Mathematik. Ganzzahlige Lösungen der "Pythagoräischen" Gleichung $a^2 + b^2 = c^2$ wie z.B. $3^2 + 4^2 = 5^2$ oder $8^2 + 15^2 = 17^2$ wurden bereits in Babylon und in vielen anderen antiken Zivilisationen gesucht und gefunden, und ein erheblicher Teil der *Elemente* von Euklid behandelt Fragen von Primzahlen und Teilbarkeit von ganzen Zahlen. Der wohl größte Zahlentheoretiker der Antike, Diophant (ca. 250 A.D.), hat mit seinen *Arithmetika* ein Meisterwerk hinterlassen, das seiner Zeit so weit voraus war, dass es auch nach seinem Wiederauftauchen im 16. Jahrhundert für die größten Mathematiker Europas ein Rätsel und eine Inspiration darstellte. (Das Buch war seit der Verbrennung der Bibliothek in Alexandria verschollen und wurde erst im Jahr 1570 in einer arabischen Übersetzung wiederentdeckt.) Das Teilgebiet der Zahlentheorie, das sich mit der Lösbarkeit von algebraischen Gleichungen in ganzen oder gebrochenen Zahlen beschäftigt, heißt zu Diophants Ehre heute die "diophantische Analysis" oder die Theorie der "diophantischen Gleichungen". Ich möchte hier dieses Gebiet vorstellen anhand einiger älterer und neuerer Resultate zu der Frage der Darstellbarkeit einer gegebenen Zahl als Summe von Quadrat- oder Kubikzahlen.

Ich fange an mit einem der schönsten und berühmtesten Resultate aus der Zahlentheorie, nämlich der Antwort auf die Frage: welche Zahlen lassen sich als Summe von zwei Quadratzahlen darstellen? Wegen der Identität

$$(a^2 + b^2)(c^2 + d^2) \;=\; (ad - bc)^2 \;+\; (ac + bd)^2\,,$$

die besagt, dass ein Produkt zweier solcher Quadratzahlsummen ebenfalls eine solche ist, kann man sich auf Primzahlen beschränken. Die Primzahl 2 ist offenbar Summe zweier Quadratzahlen: $2 = 1 + 1 = 1^2 + 1^2$. Jede andere Primzahl ist ungerade, lässt sich also in der Form $2N + 1$ schreiben. Die Antwort auf unsere Frage, die um 1640 von Fermat gefunden wurde (aber die Diophant möglicherweise bereits wusste), lautet wie folgt:

Satz 1. (1) *Eine Primzahl der Gestalt* $2N + 1$ *mit* N **gerade** *lässt sich auf genau eine Weise als Summe zweier ganzer Quadratzahlen darstellen.* (2) *Eine Primzahl der Gestalt* $2N + 1$ *mit* N **ungerade** *hat keine Darstellung dieser Art.*

Die Aussage (2) ist sehr elementar, aber die Aussage (1) ist ein recht tiefer Satz, auch wenn man heute viele verschiedene Beweise kennt[1]. Für kleine Primzahlen

[1]Siehe z.B. D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares*, Amer. Math. Monthly **97** (1990), S. 144

können wir den Satz von Hand nachprüfen. So haben die Primzahlen 5, 13, 17, 29, 37 und 41 (mit $N = 2$, 6, 8, 14, 18 und 20) die Darstellungen 1+4, 4+9, 1+16, 4+25, 1+36 und 16+25 und keine anderen, während die Primzahlen 3, 7, 11, 19, 23 und 31 (mit $N = 1$, 3, 5, 9, 11 und 15) überhaupt nicht als Summe von zwei Quadratzahlen darstellbar sind. (Z.B. sind die Quadratzahlen bis 31 die Zahlen 1, 4, 9, 16 und 25, und man sieht sofort, dass keine zwei von ihnen sich auf 31 addieren.)

Man kann dieselbe Frage ebenfalls für gebrochene Quadratzahlen stellen. Verblüffenderweise ist auch hier die Antwort sehr einfach:

Zusatz. (1) *Eine Primzahl der Gestalt* $2N+1$ *mit* N *gerade lässt sich auf unendlich viele Weisen als Summe zweier gebrochener Quadratzahlen darstellen.* (2) *Eine Primzahl der Gestalt* $2N+1$ *mit* N *ungerade hat keiner Darstellung dieser Art.*

Zum Beispiel hat die Primzahl 5 neben der evidenten Zerlegung als $1+4 = 1^2+2^2$ ebenfalls die Darstellungen $5 = \frac{4}{25} + \frac{121}{25} = \left(\frac{2}{5}\right)^2 + \left(\frac{11}{5}\right)^2$ und $5 = \frac{4}{169} + \frac{841}{169} = \left(\frac{2}{13}\right)^2 + \left(\frac{29}{13}\right)^2$ und unendlich viele weitere, während die Primzahl 3 auch dann, wenn man Brüche zulässt, niemals in der Gestalt $a^2 + b^2$ schreibbar ist.

Ein gewisses Gegenstück zu dem obigen Satz von Fermat stellt der folgende, genau so berühmte Satz von Lagrange (1770) dar:

Satz 2. *Jede positive ganze Zahl lässt sich als Summe von höchstens vier ganzen Quadratzahlen darstellen.*

Z.B. kann man 31 als 1+1+4+25 schreiben. Mit weniger Quadratzahlen kommt man hier nicht aus, so dass man die Zahl "vier" in dem Lagrangeschen Satz nicht durch "drei" ersetzen kann. Es ist dann natürlich zu fragen, welche Zahlen mit nur drei Quadraten darstellbar sind. Dabei darf man sich auf Zahlen beschränken, die nicht durch 4 teilbar sind. (Ist nämlich $n = a^2 + b^2 + c^2$ und n durch 4 teilbar, so sind notwendigerweise a, b und c alle drei gerade und man kann die ganze Gleichung durch 4 teilen.) Hieraus ergeben sich zwei interessante Fragen:

Frage 1. Welche nicht durch 4 teilbare Zahlen lassen sich als Summe von höchstens drei Quadratzahlen schreiben?

Frage 2. Welche nicht durch 4 teilbare Zahlen lassen sich auf *genau eine Weise* als Summe von höchstens drei Quadratzahlen schreiben?

Es stellt sich heraus, dass diese Fragen viel schwieriger sind als die entsprechenden für zwei und vier Quadrate. Die erste wurde von Legendre (1798) und Gauss (1801) beantwortet. Die Antwort (die Gauss soviel Freude gemacht hat, dass er zu diesem Anlass in sein Tagebuch den berühmten Eintrag "Eureka! $n = \Delta+\Delta+\Delta$!" schrieb) ist leicht zu formulieren, obwohl ihr Beweis keineswegs elementar ist. Sie lautet:

Satz 3. *Eine nicht durch 4 teilbare natürliche Zahl* n *ist dann und nur dann als Summe von höchstens drei Quadratzahlen darstellbar, wenn der Rest von* n *nach Division durch 8 nicht gleich 7 ist.*

Die Zahlen 7, 15, 23, 31, ... sind also nicht darstellbar, während zum Beispiel die Zahlen 19 ($= 8 \times 2 + 3$) und 427 ($= 8 \times 53 + 3$) die Darstellungen $19 = 1 + 9 + 9$ bzw. $427 = 81 + 121 + 225$ besitzen. In diesen beiden Fällen ist die gegebene Darstellung die einzige, so dass wir hier auch Beispiele zu Frage 2 haben. Wenn man mit einem Computer bis etwa 10.000 oder 100.000 sucht, findet man keine weiteren solchen Zahlen und man kann vermuten, dass 427 vielleicht tatsächlich die letzte ist. Der amerikanische Mathematiker E. GROSSWALD hat entdeckt, dass dies aus einer Lösung des sogenannten *Klassenzahlproblems* von Gauss folgen würde, einer Lösung, die 1984 von B. GROSS und mir nach Vorarbeiten von D. GOLDFELD erbracht wurde. Somit haben wir die vollständige Antwort auf Frage 2:

Satz 4. *Die einzigen nicht durch 4 teilbaren Zahlen, die genau eine Darstellung als Summe von höchstens drei Quadratzahlen besitzen, sind 1, 2, 3, 5, 6, 10, 11, 13, 14, 19, 21, 22, 30, 35, 37, 42, 43, 46, 58, 67, 70, 78, 91, 93, 115, 133, 142, 163, 190, 235, 253, 403 und 427.*

Wir gehen jetzt von Quadratzahlen zu Kubikzahlen, also dritten Potenzen, über. Hier lautet das Analogon zum Lagrangeschen Satz wie folgt:

Satz 5. *Jede positive ganze Zahl lässt sich als Summe von höchstens neun ganzen Kubikzahlen darstellen.*

Dieser Satz, der 1770 von WARING als Vermutung formuliert wurde, wurde 1912 von WIEFERICH bewiesen. Man weiß übrigens, dass nur die beiden Zahlen $23 = 1+1+1+1+1+1+1+8+8$ und $239 = 1+8+8+8+8+27+27+27+125$ tatsächlich 9 Kubikzahlen brauchen und alle anderen Zahlen mit höchstens 8 auskommen; die Analoga der obigen Resultate für Quadratzahlen (also die genaue Bestimmung der Zahlen, für die man $3, 4, \ldots, 8$ Kubikzahlen braucht) sind aber nicht bekannt. Übrigens ist Satz 5 lediglich ein Spezialfall eines viel allgemeineren Ergebnisses. Waring hatte nämlich vermutet, dass jede natürliche Zahl Summe von 4 Quadraten, 9 Kubikzahlen, 19 Biquadraten (= vierte Potenzen), "und so weiter" sei, d.h., dass man bei jeder festen Potenz immer nur eine beschränkte Anzahl von Summanden braucht, um eine beliebige natürliche Zahl darzustellen. Diese Vermutung wurde 1909 in einer brillianten Arbeit von dem deutschen Mathematiker D. HILBERT bewiesen.

Zum Schluss will ich etwas über eine Frage aus demselben Themenkreis erzählen, die aber viel tiefere und schwierigere Hilfsmittel erfordert, als dies bei den bisher erwähnten Sätzen der Fall war. Diese Frage gehört zu der Theorie der sogenannten *elliptischen Kurven*, einem Teilgebiet der diophantischen Analysis, das in den letzten Jahrzehnten eine rasante Entwicklung erlebt hat und zu der Lösung von verschiedenen klassischen Problemen der Zahlentheorie geführt hat (hierunter der oben erwähnte Satz von B. Gross und mir und der sensationelle Beweis des "letzten Satzes von Fermat" von A. WILES). Am Anfang dieses Artikels hatten wir die Frage gestellt: welche Primzahlen p lassen sich als Summe von zwei Quadraten darstellen? und gesehen (Satz 1 und Zusatz), dass die Antwort auf diese Frage dieselbe ist, wenn wir bei den verwendeten Quadratzahlen nur ganze Zahlen zulassen oder auch gebrochene Summanden akzeptieren. Bei dritten Potenzen ist die Situation anders,

da—wie sich herausstellt—nur die Frage nach der Zerlegbarkeit in *gebrochene* Kubikzahlen eine interessante Antwort besitzt. Dass diese Antwort nicht leicht sein kann, sieht man anhand einfacher Beispiele. So hat bereits die kleine Primzahl 13 die nicht ganz evidente Zerlegung $13 = \frac{8}{27} + \frac{343}{27} = \left(\frac{2}{3}\right)^3 + \left(\frac{7}{3}\right)^3$ als Summe von zwei gebrochenen Kubikzahlen, während die nicht allzu große "französische" Primzahl 1789 als *einfachste* Lösung die Zerlegung

$$1789 \;=\; \left(\frac{38119538057820221}{2828707454055574}\right)^3 \;+\; \left(-\frac{24606633997841365}{2828707454055574}\right)^3$$

hat, die man mit keinem noch so leistungsstarken Computer durch direktes Ausprobieren je finden könnte. Umgekehrt gibt es auch andere Primzahlen, wie etwa 73, die gar keine Darstellung der Form $a^3 + b^3$ haben, für die man dies aber nur unter Verwendung von schwierigen Resultaten aus der modernen Zahlentheorie nachweisen kann. Schliesslich weiß man, dass (mit der bereits erwähnten Ausnahme der Primzahl 2, die die eindeutige Zerlegung als $1^3 + 1^3$ besitzt) jede Primzahl, die überhaupt als Summe zweier gebrochener Kubikzahlen darstellbar ist, dies auf unendlich viele verschiedene Weisen ist, z.B.

$$19 \;=\; \left(\frac{3}{2}\right)^3 + \left(\frac{5}{2}\right)^3 \;=\; \left(\frac{1}{3}\right)^3 + \left(\frac{8}{3}\right)^3 \;=\; \left(\frac{33}{35}\right)^3 + \left(\frac{92}{35}\right)^3 \;=\; \cdots$$

(Vergleiche den Zusatz zu Satz 1, der dieselbe Aussage für Quadratzahlen gibt.) Trotz dieser Schwierigkeiten ist die Antwort auf die Frage der Zerlegbarkeit von Primzahlen in gebrochene Kubikzahlen jetzt fast vollständig bekannt. Im letzten Teil dieses Artikels möchte ich diese Antwort vorstellen.

Bei den Quadratzahlen hing die Antwort auf die Frage der Zerlegbarkeit einer Primzahl p davon ab, ob p von der Gestalt $2N + 1$ mit N gerade oder mit N ungerade war, d.h., ob p selber die Gestalt $4k + 1$ oder $4k + 3$ hatte. Bei den Kubikzahlen stellt sich heraus, dass wir statt dessen nach dem Rest der Primzahl nach Division durch 9 (anstatt 4) unterscheiden müssen. Wenn wir also die Ausnahmeprimzahlen 2 und 3 weglassen (für die die Antwort längst bekannt ist: 2 lässt sich nur in der Form 1+1 als Summe zweier gebrochener Kubikzahlen schreiben, und 3 gar nicht), müssen wir sechs verschiedene Klassen unterscheiden:

(I)	$p = 9k+1$	($p = 19, 37, 73, 109, \ldots$)
(II)	$p = 9k+2$	($p = 11, 29, 47, 83, \ldots$)
(III)	$p = 9k+4$	($p = 13, 31, 67, 103, \ldots$)
(IV)	$p = 9k+5$	($p = 5, 23, 41, 59, \ldots$)
(V)	$p = 9k+7$	($p = 7, 43, 61, 79, \ldots$)
(VI)	$p = 9k+8$	($p = 17, 53, 71, 89, \ldots$)

Bei den Klassen (II) und (IV) ist die Antwort "nein" (d.h., diese Primzahlen sind nie als Summe zweier rationaler Kubikzahlen darstellbar), und der Beweis (Sylvester, 1856, Pepin, 1870) ist relativ elementar, da er auf der bereits von Fermat entdeckten "Methode des unendlichen Abstiegs" basiert. Bei (III) und (V) lautet die Antwort "ja" (diese Primzahlen sind also immer darstellbar); der Beweis aber, der von N. Elkies stammt und noch nicht veröffentlicht ist, benutzt bereits

wesentlich schwierigere Hilfsmittel (Theorie der sogenannten Heegner-Punkte auf Modulkurven). Im Falle (VI) ist die Antwort mit ziemlicher Sicherheit "ja". Dies ist aber noch nicht bewiesen, sondern ist nur ein Spezialfall der allgemeinen Vermutung von Birch und Swinnerton-Dyer, die ein Kriterium für die Lösbarkeit einer großen Klasse von Gleichungen dieser Art gibt—eine Vermutung, die zu den sieben berühmten Problemen gehört, für deren Lösung der amerikanische Mathematikmäzen Landon Clay vor drei Jahren Preise von jeweils einer Million Dollar ausgeschrieben hat.

Es bleibt also nur noch der Fall (I). Hier ist die Antwort auf die Frage nach der Zerlegbarkeit als $a^3 + b^3$ viel weniger klar, da sie für verschiedene Primzahlen aus dieser Klasse verschieden ausfällt: von den 27 Primzahlen der Gestalt $9k + 1$ unter 1000 sind 14 (die Primzahlen 19, 37, 127, 163, 271, 379, 397, 433, 523, 631, 829, 883, 919 und 937) als Summe von zwei Kubikzahlen darstellbar und die anderen 13 (die Primzahlen 73, 109, 181, 199, 307, 487, 541, 577, 613, 739, 757, 811 und 991) sind es nicht. Die Antwort auf die Frage, woran man die Zerlegbarkeit in zwei Kubikzahlen einer Primzahl der Klasse (I) erkennt, wurde erst vor wenigen Jahren von dem argentinischen Mathematiker F. Rodriguez Villegas und mir gefunden, und hat eine total unerwartete Gestalt. Wir definieren zunächst eine gewisse Folge von Zahlen

$$B_0 = 1\,,\ B_1 = 2\,,\ B_2 = -152\,,\ B_3 = 6848\,,\ B_4 = -8103296\,,\ \ldots$$

die durch ein elementares, wenngleich ziemlich kompliziertes Bildungsgesetz gegeben wird (s. Fig. 1). Dann gilt:

Satz 6. *Sei $p = 9k + 1$ prim. Wenn p die Zahl B_k nicht teilt, so ist p nicht als Summe zweier gebrochener Kubikzahlen darstellbar. Wenn die Vermutung von Birch und Swinnerton-Dyer stimmt, gilt auch die Umkehrung: ist B_k durch p teilbar, so hat p eine (und damit auch unendlich viele) Darstellung(en) dieser Art.*

So ist $B_2 = -152$ durch $9\times 2+1 = 19$ und $B_4 = -8103296$ durch $9\times 4+1 = 37$ teilbar, und 19 und 37 sind tatsächlich als Summen zweier Kubikzahlen darstellbar ($19 = (3/2)^3 + (5/2)^3$, $37 = (19/7)^3 + (18/7)^3$), während umgekehrt $B_8 = 532650564250569441280$ nicht durch $9\times 8 + 1 = 73$ teilbar ist und 73 nicht in der Gestalt $a^3 + b^3$ mit gebrochenen Zahlen a und b geschrieben werden kann.

Figur 1. Bildungsgesetz der Zahlen B_k . Die Zahlen in den Ovalen haben auf der k-ten nach links fallenden Diagonalen den konstanten Wert $24k$–21 (=3, 27, 51, . . .); die Zahlen in den Rechtecken haben auf der k-ten horizontalen Linie den konstanten Wert $-4k(2k-1)$ (= –4, –24, –60, . . .); die Zahlen in den Kreisen haben auf der k-ten nach rechts fallenden Diagonalen die Werte $2k, 2k$–1, . . . , 2, 1; jede fettgedruckte Zahl ist die Summe ihrer nordwestlichen, nördlichen und nordöstlichen fettgedruckten Nachbarn, jeweils mit der Zahl in dem dazwischenliegenden Kreis, Rechteck, oder Oval multipliziert; und die ganz rechts stehenden fettgedruckten Zahlen sind die B_k .