Don Zagier

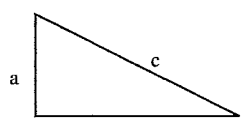
Lösungen von Gleichungen in ganzen Zahlen*

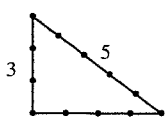
Die Frage, wie man die Lösungen in ganzen oder Bruchzahlen einer unbestimmten Gleichung ausfindig macht, ist eine der ältesten, mit denen Mathematiker sich beschäftigt haben, gehört aber gleichzeitig zu den aktuellsten Gegenständen der mathematischen Forschung. In meinem heutigen Vortrag möchte ich Ihnen über beide Aspekte etwas erzählen.

Ich beginne mit einem Beispiel, das Ihnen allen von der Schule her bekannt ist, nämlich der Gleichung

$$a^2+b^2=c^2, \tag{1}$$

welche die Beziehung zwischen den Katheten und der Hypotenuse eines rechtwinkligen Dreiecks ausdrückt (»Satz von Pythagoras«):





Uns geht es hier allerdings nicht um den geometrischen Inhalt dieser Gleichung, sondern darum, wie man ganzzahlige Lösungen findet, also Zahlentripel (a, b, c), die die Gleichung erfüllen. Da $3^2+4^2=9+16=25=5^2$ ist, hat man als einfachste Lösung das Tripel (3, 4, 5), das schon allen antiken Völkern bekannt war[1] und z.B.

* Vortrag gehalten in Schweinfurt anläßlich der Verleihung des Carus-Preises, 27. 1. 84. Viele Anregungen zu diesem Vortrag, insbesondere über Diophants Werk und dessen Interpretation vom modernen Standpunkt, habe ich dem Büchlein *Diophant und diophantische Gleichungen* (Deutscher Verlag der Wissenschaften, Berlin 1974) von I.G. Bashmakova entnommen, das ich dem interessierten Leser sehr empfehlen möchte. Eine weitere Quelle war die von derselben Autorin kommentierte Übersetzung (ins Russische) von I.N. Veselovsky (Nauka Verlag, Moskau 1974).

[1] Zur Geschichte der pythagoreischen Gleichung (1) und ihrer ganzzahligen Lösungen s. Kapitel I von B.L. van der Waerden, *Geometry and Algebra in Ancient Civilisations* (Springer-Verlag, 1983).

von den Ägyptern in Form eines in regelmäßigen Abständen geknoteten Seils der Länge $3+4+5=12$ zur Konstruktion rechter Winkel in der Landvermessung gebraucht worden sein soll; ein anderes Tripel, (8, 15, 17), wurde u.a. von Plato angegeben. Die allgemeine Lösung der Gleichung (1) steht bei Euklid (Buch X, 29) – sie wurde auch in anderen Ländern entdeckt, z.B. in Indien im 7. Jahrhundert (Brahmegupta) – und hat die Form

$$a=2pq, \quad b=p^2-q^2, \quad c=p^2+q^2, \tag{2}$$

wobei p und q beliebige positive Zahlen mit $p>q$ sind. (Eigentlich muß man auch Vielfache hiervon, also Tripel $(2hpq,\ h(p^2-q^2),\ h(p^2+q^2))$ mit irgendeinem positiven h, betrachten, aber solche proportionale Lösungen werden als im wesentlichen gleich angesehen.) Wir werden später sehen, wie man auf die Formeln (2) kommt.

Die Gleichungen (2) stellen lediglich ein Einzelergebnis dar. Die erste systematische Theorie von unbestimmten Gleichungen und ihren Lösungen wurde von dem genialen alexandrinischen Mathematiker Diophant (ca. 250 A.D.) entwickelt, zu dessen Ehre das ganze Gebiet heute die *diophantische Analysis* oder die Theorie der *diophantischen Gleichungen* heißt. Ich möchte an dieser Stelle auf Diophants Arbeit etwas näher eingehen, weil diese, wie wir sehen werden, die Keime aller späteren Entwickungen enthält.

Über Diophant selbst wissen wir sehr wenig, außer daß er, wie gesagt, in Alexandria lebte und anscheinend im Alter von 84 Jahren starb (sogar die Zeitangabe 250 A.D. könnte um bis zu 150 Jahre in beiden Richtungen falsch sein). Von seinen Werken sind die meisten verlorengegangen. Bis zum 16. Jahrhundert waren sie sogar alle verschwunden, und man wußte nur vage, was Diophant getan hatte; ein Manuskript von 6 der 13 Bücher der *Arithmetika* wurde erst 1570 von dem Astronom Johannes Müller aus Königsberg (bei Schweinfurt) dem sogenannten Regiomontanus, in Venedig entdeckt[2]. Vielleicht einmalig in der Geschichte der Wissenschaft ist die Tatsache, daß seine Schriften, als sie zu diesem Zeitpunkt – also über 1200 Jahre nach seinem Tode! – wieder auftauchten,

[2] Vor ein paar Jahren sind weitere vier Bücher aufgetaucht (s. J. Sesiano, *Books IV to VII of Diophantus' Arithmetica*, Springer-Verlag, 1982), was unter anderem eine Umnumerierung der bis dann bekannten Bücher mit sich brachte. In diesem Vortrag werden die neu entdeckten Bücher nicht berücksichtigt und die traditionelle Numerierung der Bücher verwendet.

keineswegs nur von historischem Interesse, sondern ganz im Gegenteil dem derzeitigen Wissensstand weit voraus waren und einen entscheidenden Anstoß für die Entwicklungen der nächsten ein- bis zweihundert Jahre gaben.

Diophant war der erste, der einen systematischen algebraischen Symbolismus einführte, so daß er eine Gleichung wie $3x^2-2x^2=4$ (was allerdings bei ihm so ausgesehen hätte: $K^{Y}\bar{\gamma}\pitchfork\Delta^{Y}\bar{\beta}\,\iota\,\mathring{M}\bar{\delta}$) schreiben konnte; vor ihm konnte man eine solche Formel nicht einmal in Worten ausdrücken, da man die geometrisch aufgefaßten Kubik- und Quadratzahlen wegen der Inkompatibilität der Dimensionen nicht addieren konnte und ohnehin den Begriff einer Unbekannten, mit der operiert wird, noch nicht formuliert hatte. Darüber hinaus hat Diophant das System der natürlichen (d.h. positiven ganzen) Zahlen in zwei Richtungen erweitert – zunächst, indem er negative Zahlen zuließ und die Rechenregeln für diese (etwa: Minus mal Minus gleich Plus) genau formulierte, dann durch Hinzunahme der rationalen (d.h. Bruch-)Zahlen, mit denen er genauso umging wie mit ganzen Zahlen. Um zu sehen, wie fortschrittlich dies war, muß man bedenken, daß die rationalen Zahlen noch ganz unbekannt waren (Euklid betrachtete Verhältnisse von Längen, die aber nur miteinander verglichen werden konnten und nicht etwa addiert), und daß man in Europa tausend Jahre später die negativen Zahlen noch längst nicht als vollwertig anerkannte. Es ist übrigens ein in der Geschichte der Zahlentheorie immer wieder auftretendes Phänomen, daß die Erweiterung des Zahlsystems oder der Übergang zu neuartigen Zahlen notwendig wurde, um Probleme, die die gewöhnlichen ganzen Zahlen betreffen, besser zu verstehen. Jedenfalls war die Ausdehnung der Zahlen auf positive und negative ganze und Bruchzahlen bei Diophant sehr zweckmäßig, weil man jetzt alle vier Grundrechenarten unbeschränkt ausführen konnte und auch, weil viele Problemstellungen einfacher wurden. Teilt man z.B. Gleichung (1) durch c^2 und setzt $\frac{a}{c}=x$, $\frac{b}{c}=y$, so erhält man die nunmehr in rationalen Zahlen zu lösende Gleichung

$$x^2+y^2=1, \tag{3}$$

welche nur zwei Variable enthält.

Im ersten Buch der *Arithmetika* betrachtete Diophant lineare Gleichungen (also solche, in denen die Variablen nur zur ersten

Potenz auftreten); die Methoden hier waren zum Teil schon bekannt. Für Gleichungen von höherem Grad dagegen mußten ganz neue Verfahren entwickelt werden, die wir jetzt beschreiben.

Sehen wir uns zunächst die Methode an, die Diophant für quadratische Gleichungen (Gleichungen vom Grad 2) benutzte. Als Beispiel nehmen wir die pythagoreische Gleichung in der Gestalt (3). Wir setzen in dieser Gleichung

$$y=3x+1 \tag{4}$$

und erhalten

$$\begin{aligned} x^2+(3x+1)^2&=1,\\ 10x^2+6x+1&=1,\\ 10x^2+6x&=0,\\ 10x+6&=0,\\ x=-\tfrac{3}{5},\quad y&=3x+1=-\tfrac{4}{5}, \end{aligned}$$

also (bis aufs Vorzeichen) die alte Lösung (3, 4, 5) von (1). Man sieht hier, daß die Wahl des Koeffizienten 3 in (4) völlig willkürlich war; man hätte genausogut irgendeine andere Zahl einsetzen können und würde so viele rationale Lösungen bekommen, wie man wollte. In Formeln ausgedrückt (was allerdings Diophant nicht gut konnte, weil sein Symbolismus nur eine Veränderliche auf einmal zuließ): mit dem Ansatz $y=kx+1$ anstelle von (4) erhält man

$$(k^2+1)x^2+2kx+1=1$$

und somit die allgemeine Lösung

$$x=\frac{-2k}{k^2+1},\qquad y=\frac{1-k^2}{1+k^2} \tag{5}$$

von (3), die zu (2) äquivalent ist, wenn wir $k=-\frac{q}{p}$ setzen. Daß diese Lösung den freien Parameter k enthält, impliziert, daß man unendlich viele rationale Lösungen von (3) und somit unendlich viele ganzzahlige Lösungen von (1) hat. Das Verfahren funktioniert für jede quadratische Gleichung in zwei Veränderlichen x und y: ausgehend von einer bekannten Lösung (x_0, y_0) ersetzt man zunächst x durch $x+x_0$, setzt dann $y=kx+y_0$, und erhält für jeden rationalen Wert von k eine Lösung der Gleichung. Man findet in der *Arithmetika* vielfache Anwendungen.

Wir wenden uns jetzt dem – viel subtileren – Verfahren zu, das Diophant für Gleichungen dritten Grades verwendete. Diesmal nehmen wir als Beispiel die Aufgabe 24 des IV. Buchs: man zerlege eine gegebene Zahl – etwa 6 – in zwei Teile, so daß ihr Produkt gleich einer um ihre Wurzel verminderten Kubikzahl ist, also

$$y(6-y)=x^3-x. \tag{6}$$

Hier macht Diophant in Analogie zum quadratischen Fall zunächst den Ansatz

$$x=2y-1$$

mit dem willkürlich gewählten Koeffizienten 2 und erhält

$$6y-y^2=8y^3-12y^2+4y.$$

Er bemerkt, daß die neue Gleichung sofort rational lösbar wäre, wenn die beiden Koeffizienten von y, also die Zahlen 6 und 4, gleich wären, da man dann durch y^2 teilen und die entstehende lineare Gleichung lösen könnte. Die Zahl »6« kommt von der Aufgabenstellung, die Zahl »4« dagegen ist das Doppelte des Koeffizienten »2« in dem gewählten Ansatz. Dieser Koeffizient muß also durch 3 ersetzt werden, d.h. wir setzen $x=3y-1$ und finden

$$6y-y^2=27y^3-27y^2+6y,$$
$$y=\tfrac{26}{27}, \quad x=\tfrac{17}{9},$$

die gewünschte Lösung. Diesmal ist der Parameter k im Ansatz $x=ky-1$ nicht frei, und wir erhalten nur *eine* Lösung.

Wir können Diophants Erkenntnisse so zusammenfassen:

1. Quadratische Gleichungen lassen sich durch einen bestimmten linearen Ansatz auf vielerlei Weisen lösen. Solche Gleichungen werden heute als *rational* bezeichnet.

2. Bei kubischen (und gewissen quartischen) Gleichungen liefert ein ähnlicher Ansatz manchmal spezielle Lösungen. Gleichungen dieses Typs heißen heute *elliptisch.*

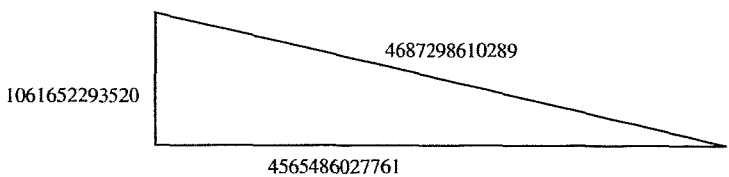
3. Gleichungen höheren Grades werden nicht betrachtet[3]. Diese nennt man heute *von höherem Geschlecht* (die Terminologie wird unten erläutert).

---

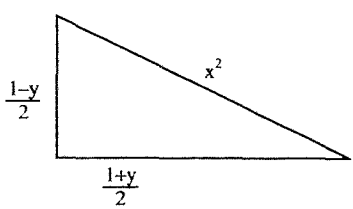
[3] Eine Ausnahme ist Aufgabe 18 des IV. Buchs, wo eine nichttriviale Lösung der Gleichung $y^2=x^6-2b^2x^3+x+b^4$ (d.h. eine mit $x\neq 0$) durch den Ansatz $y=x^3+b^2$ gefunden wird.

Von den drei Klassen haben die elliptischen die interessantesten Lösungen. Wir illustrieren dies anhand zweier historischer Beispiele.

FERMATS PROBLEM ÜBER RECHTWINKLIGE DREIECKE. In einem Brief an den Priester Mersenne stellte Fermat 1643 die folgende Aufgabe: man finde ein rechtwinkliges Dreieck mit ganzzahligen Seiten, so daß sowohl die Summe der Katheten als auch die Hypotenuse Quadrate sind. Fermat (1601–1665) war Mitbegründer der analytischen Geometrie (mit Descartes), der Wahrscheinlichkeitsrechnung (mit Pascal) und der Infinitesimalrechnung (mit Leibniz und Newton), seine größte Leistung war aber in der Zahlentheorie, wo er unmittelbar von Diophant inspiriert wurde, dessen Werk er als erster voll verstand und weiterentwickelte. Auch die genannte Frage stellte er erstmalig im Zusammenhang mit einer Aufgabe von Diophant (Nummer 22 aus Buch VI). An der von ihm gefundenen Lösung erkennt man, wie weit die Theorie in seinen Händen gekommen war:



(Fermat konnte nachweisen, daß dies die *kleinste* Lösung ist!). Die zum Problem gehörige Gleichung findet man, indem man die Seiten des Dreiecks durch die Kathetensumme teilt; diese wird dann 1 und man sucht nunmehr ein rechtwinkliges Dreieck der Gestalt



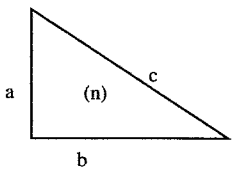
d.h. man muß die Gleichung

$$y^2 = 2x^4 - 1$$

mit x und y rational und der Nebenbedingung $-1 < y < 1$ lösen.

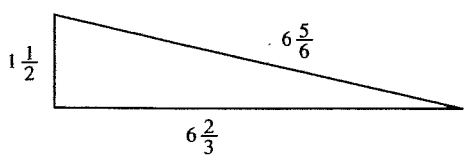
Daß eine so harmlos aussehende Gleichung eine so komplizierte Lösung haben kann, gibt einen Eindruck von der Schwierigkeit der Theorie der elliptischen Gleichungen.

KONGRUENTE ZAHLEN. Gegeben sei eine Zahl n; man soll entscheiden, ob n als Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seitenlängen vorkommen kann:



$$a^2+b^2=c^2,$$
$$\tfrac{1}{2}ab=n.$$

Eine äquivalente Aufgabe[4] ist, eine (rationale) Quadratzahl x zu finden, die sowohl um n vermindert als auch um n vermehrt eine Quadratzahl bleibt. Eine Zahl n, für die es ein Dreieck oder eine Zahl x mit den genannten Eigenschaften gibt, heißt klassisch »kongruent«. Das Problem steht bereits in einem über 1000 Jahre alten arabischen Manuskript und wurde von Leonardo Fibonacci von Pisa, einem Zeitgenossen Dantes, wieder aufgegriffen, der ihm ein ganzes Buch, das *liber quadratorum* (1225), widmete. Für $n=5$ wird die Lösung des Problems durch das Dreieck



[4] Gilt $x=s^2$, $x-n=t^2$, $x+n=u^2$, so erfüllt das Dreieck mit den Seitenlängen

$$\frac{2xn}{stu}=\frac{2ns}{tu},\quad \frac{x^2-n^2}{stu}=\frac{tu}{s},\quad \frac{x^2+n^2}{stu}$$

die gegebene Bedingung; ist umgekehrt (a, b, c) ein pythagoreisches Tripel mit $\frac{1}{2}ab=n$, so hat man die Lösung $x=\left(\frac{c}{2}\right)^2$, $x\pm n=\left(\frac{a\pm b}{2}\right)^2$ der zweiten Aufgabe.

oder durch die Zahl $x = 11\frac{97}{144}$ gelöst:

$$11\tfrac{97}{144} = (3\tfrac{15}{12})^2,$$
$$6\tfrac{97}{144} = (2\tfrac{7}{12})^2,$$
$$16\tfrac{97}{144} = (4\tfrac{1}{12})^2.$$

Wenn wir aber $n = 157$ wählen, dann sehen wir noch deutlicher als beim vorigen Beispiel, wieviel in einer elliptischen Gleichung steckt, denn die kleinste Lösung x ist in diesem Fall

$$158\,\frac{15738954790899497476048060077581662600691366163657538183350912850062498830673479750982572088 1}{31771866588716253752986042920489322122457849878951860106775096212089198787035991271029955600}!$$

Für Gleichungen von höherem Geschlecht geben wir nur ein Beispiel:

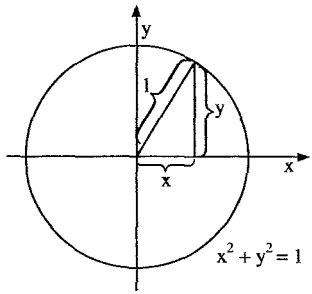
(7) $$x^n + y^n = 1 \qquad (x, y \text{ rational})$$

bzw.

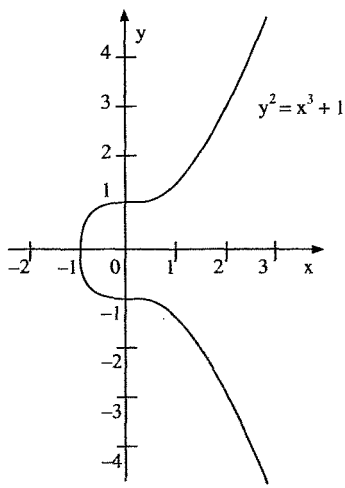
$$a^n + b^n = c^n \qquad (a, b, c \text{ ganz})$$

mit $n > 3$ (für $n = 3$ ist (7) elliptisch). Fermat hat diese Gleichung am Rande seines Exemplars von Diophant angegeben und behauptet, er habe einen wahrlich wunderbaren Beweis für ihre Unlösbarkeit (für alle $n > 2$) gefunden, der Rand sei aber zu schmal, um ihn zu fassen. Dies ist der »letzte Satz von Fermat«, bis heute ungelöst und eins der berühmtesten und wichtigsten Probleme in der mathematischen Geschichte.

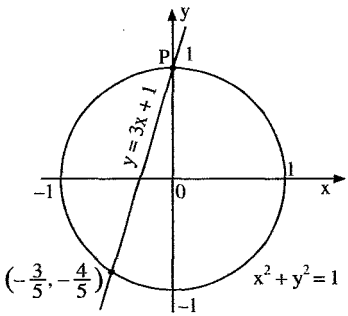
Ich möchte aber jetzt mit der Beschreibung der historischen Entwicklung fortfahren und zum schon erwähnten Thema zurückkehren, daß man oft in der Theorie der diophantischen Gleichungen durch eine Ausdehnung des benutzten Zahlsystems weiterkommt. Das erste Beispiel, der Übergang von den ganzen zu den rationalen Zahlen, haben wir schon gesehen; das zweite wäre der Übergang von den rationalen zu den *reellen* Zahlen, also Zahlen wie $\sqrt{2}$ oder π, die Streckenlängen darstellen können, aber nicht notwendigerweise Quotienten ganzer Zahlen sind. In der vorhin erwähnten analytischen Geometrie von Fermat und Descartes stellt man die Menge aller reellen Lösungen einer polynomialen Gleichung $f(x, y) = 0$ graphisch als Kurve in der Ebene dar; diese Kurve wäre im Fall der pythagoreischen Gleichung (3) ein Kreis

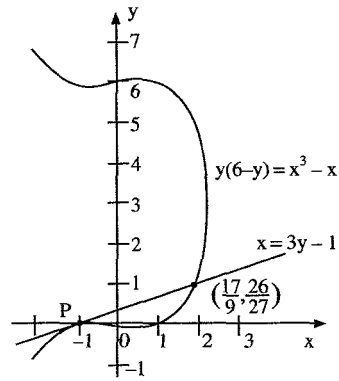


(allgemeiner, für irgendeine rationale Gleichung ein Kegelschnitt, also Ellipse, Hyperbel oder Parabel) und sähe für $y^2 = x^3 + 1$, eine typische elliptische Gleichung, so aus:



Wir werden ab jetzt Kurven und Gleichungen identifizieren, so daß wir von *rationalen Kurven, elliptischen Kurven* und *Kurven von höherem Geschlecht* sprechen und zwischen »Lösung einer Gleichung« und »Punkt auf einer Kurve« nicht unterscheiden werden. Der geometrische Standpunkt liefert neue Einsicht in den algebraischen Sachverhalt. Insbesondere können wir die vorher erläuterten Verfahren von Diophant jetzt veranschaulichen:



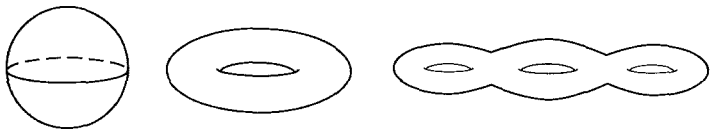


Im Fall einer rationalen Gleichung nehmen wir irgendeine bekannte Lösung und ziehen durch den entsprechenden Punkt P (hier 0, 1)) auf der Kurve eine Gerade mit willkürlich gewählter Steigung k; der zweite Schnittpunkt der Geraden mit der Kurve ist dann eine neue Lösung. Bei einer elliptischen Kurve gehen wir ebenfalls von einem bekannten Punkt P (hier $(-1, 0)$) aus und zeichnen durch diesen Punkt die *Tangent*gerade zur Kurve; diese Gerade schneidet die Kurve in einem weiteren Punkt, der eine neue rationale Lösung liefert. Allgemein kann man von zwei bekannten Lösungen ausgehen und durch die entsprechenden Punkte P und Q der Kurve eine Gerade ziehen, deren dritter Schnittpunkt mit der Kurve wieder rationale Koordinaten haben und eine neue rationale Lösung darstellen wird; die Konstruktion mit der Tangenten ist der Grenzfall $P = Q$. (Dieses allgemeine Verfahren wurde häufig von Fermat benutzt, von Diophant aber nur in dem etwas entarteten Fall, daß P oder Q ein »unendlich ferner« Punkt ist.) Übrigens war Newton anscheinend der erste, der den geometrischen Inhalt von Diophants algebraischem Verfahren im rationalen Fall erkannte[5].

Der nächste Schritt in der Kette von Erweiterungen des Zahlsystems war der Übergang zu den *komplexen* Zahlen, also Zahlen der Gestalt $x + y\sqrt{-1}$ mit x und y reell. Ohne hierauf im Detail einzugehen, können wir sagen, daß die Lösungsmenge jetzt nicht

[5] *The mathematical papers of Isaac Newton*, Band IV, ed. D.T. Whiteside, Cambridge, 1971, S. 110.

mehr eine Kurve, sondern eine geschlossene *Fläche* ist, deren Geometrie (eigentlich: Topologie) unserer Einteilung von Gleichungen in 3 Typen zugrunde liegt: diese Fläche ist nämlich eine *Sphäre* (Kugeloberfläche) im rationalen Falle, ein *Torus* (Reifen) im elliptischen Falle und sonst eine *Fläche von höherem Geschlecht*



rational elliptisch Geschlecht ≥ 2 (hier 3)

(das *Geschlecht* einer Kurve ist die Anzahl der Löcher oder Henkel, also 0 für die Sphäre, 1 für den Torus, und sonst ≥ 2). Der erste, der diophantische Gleichungen von diesem Standpunkt aus betrachtet hat, war Poincaré am Anfang dieses Jahrhunderts (die Flächen selbst waren schon 50 Jahre früher von Riemann studiert worden). Poincaré hat auch erkannt, daß die vorhin beschriebene Konstruktion einer dritten Lösung einer elliptischen Gleichung aus zwei bekannten als *Addition* aufgefaßt werden kann: mit anderen Worten, je zwei Punkten P und Q auf der Kurve mit rationalen Koordinaten kann man einen dritten Punkt $P+Q$ zuordnen[6], und die Operation $P, Q \to P+Q$ besitzt die Eigenschaften der gewöhnlichen Addition (in der Mathematik sagt man: die Menge der Punkte mit rationalen Koordinaten hat eine *Gruppenstruktur*). Er vermutete, daß jede elliptische Gleichung endlich viele Grundlösungen hat, welche bezüglich dieser Addition sämtliche anderen Lösungen erzeugen. Diese Vermutung wurde 1920 von Mordell bewiesen. Mordell hat wiederum seinerseits vermutet, daß Gleichungen von höherem Geschlecht stets nur endlich viele Lösungen haben. Das ergibt folgendes Bild. Die zunächst nur topologisch unterschiedenen

[6] Wenn die Kurve die Gestalt $y^2 = ax^3 + bx^2 + cx + d$ hat (jede elliptische Kurve kann so geschrieben werden), so ist $P+Q$ nicht der dritte Schnittpunkt der Geraden durch P und Q mit der Kurve, sondern dessen Spiegelung an der x-Achse. Das Nullelement 0 der Addition ist der unendlich ferne Punkt $y = \infty$, das Negative eines Punktes $P = (x, y)$ ist der gespiegelte Punkt $-p = (x, -y)$, und drei kollineare Punkte P, Q, R der Kurve erfüllen die Beziehung $P+Q+R=0$.

Fälle von Gleichungen, deren komplexe Lösungen eine Sphäre, einen Torus oder eine mehrhenklige Fläche bilden, verhalten sich auch vom Standpunkt ihrer rationalen Lösungen grundverschieden; für eine Sphäre gibt es stets unendlich viele Lösungen[7], die parametrisch angegeben werden; für einen Torus kann die Lösungsmenge endlich oder unendlich sein, wird aber auch im zweiten Falle von einer endlichen Teilmenge mittels eines algebraischen Verfahrens erzeugt; für eine Fläche von höherem Geschlecht sind die Lösungen schwer zu finden, haben (anscheinend) keine besondere Struktur und es soll nur endlich viele geben.

Mordells Vermutung wurde 1983 von dem jungen deutschen Mathematiker Faltings bewiesen, eine Leistung, die als eine der wichtigsten Fortschritte der letzten Jahrzehnte angesehen wird. Sein Ergebnis impliziert insbesondere, daß die Fermatsche Gleichung (7) für gegebenes $n>3$ nur endlich viele Lösungen hat (der Fall $n=3$ wurde schon von Euler erledigt).

Durch Faltings' Resultat ist die Frage nach der Struktur der Lösungen im Falle Geschlecht >1 weitgehend geklärt. Wenden wir uns wieder den elliptischen Kurven zu. Mordells Satz über die endliche Erzeugbarkeit läßt sich wie folgt präzise formulieren: Für eine elliptische Kurve kann man endlich viele Grundlösungen $P_1, \ldots, P_r$ finden, so daß überhaupt jede Lösung P geschrieben werden kann als

$$P = n_1 P_1 + \ldots + n_r P_r + Q$$

mit $n_1, \ldots, n_r$ ganze Zahlen und Q aus einem endlichen Lösungsvorrat. Die (minimal gewählte) Zahl r heißt *Rang* der elliptischen Kurve. Beispielsweise hat die Kurve

$$y^2 = x^3 - 432,$$

welche vermöge der Transformation $x = \dfrac{12c}{a+b}$, $y = 36\dfrac{a-b}{a+b}$ der Fer-

[7] Genauer gesagt: wenn es *eine* rationale Lösung gibt, gibt es unendlich viele, da man dann Diophants Methode anwenden kann. Es gibt aber auch Gleichungen, deren komplexe Lösungsmenge eine Sphäre ist, die aber überhaupt keine rationale Lösung haben (z.B. $x^2+y^2=3$, ein Kreis vom Radius $\sqrt{3}$, oder die Gleichung $x^2+y^2=-1$, die nicht einmal reelle Lösungen besitzt). Diese Möglichkeit haben wir bei der Diskussion der Arbeit Diophants nicht erwähnt, weil er nur Gleichungen betrachtete, für die er mindestens eine Lösung kannte.

matschen Gleichung $a^3+b^3=c^3$ entspricht, den Rang 0, weil sie nur die zwei Lösungen $x=12$, $y=\pm 36$ besitzt. Die Gleichung

$$y^2=2x^4+1,$$

die im Zusammenhang mit Fermats Problem über Dreiecke vorkam, hat den Rang 1. Eine Grundlösung ist der Punkt P(13,239) mit den Vielfachen $2P(\frac{1525}{1343}, \frac{2750257}{1803649})$, $3P(\frac{2165017}{2372159}, \frac{3503833734241}{5627138321281})$, ..., wobei erst 3P die Zusatzbedingung $-1<y<1$ erfüllt und das geometrische Problem löst. Ein Beispiel für eine Kurve höheren Ranges ist die Gleichung

$$y^2=4x^3-28x+25$$

mit dem Rang 3; der Leser kann ausprobieren, für wie viele kleine ganze Zahlen x die linke Seite hier ein Quadrat wird. Man kennt Beispiele von elliptischen Kurven mit Rang bis zu 14, weiß aber nicht, ob es Kurven mit beliebig hohem Rang gibt.

Es stellt sich nun die Frage, wie man den Rang einer elliptischen Kurve berechnet. Bis heute ist keine Antwort hierauf bekannt; es gibt aber eine schöne Vermutung, die ich abschließend erklären möchte. Hier ist noch einmal die entscheidende Idee der Übergang zu einem anderen Zahlbereich, der aber diesmal nicht eine Vergrößerung, sondern eine Verkleinerung des Systems der ganzen Zahlen darstellt: Man nimmt eine Primzahl p und arbeitet mit dem *endlichen* System, bestehend aus den möglichen Resten von ganzen Zahlen nach Division durch p. Diese endlich vielen Zahlen, die wir mit k^* $(0\leq k\leq p-1)$ bezeichnen werden, können genauso wie gewöhnliche Zahlen addiert und multipliziert werden (man denke an die Reste nach Division durch 10 – allerdings keine Primzahl –, die man sich als Endziffer gewöhnlicher Zahlen vorstellen kann; hier gibt es die 10 Möglichkeiten $0^*, 1^*, \ldots, 9^*$ und man hat $8^*+4^*=2^*$, $7^*\cdot 9^*=3^*$, ..., weil z.B. das Produkt zweier Zahlen mit den Endziffern 7 und 9 stets die Endziffer 3 hat). Die Idee ist jetzt, daß eine Gleichung, die viele Lösungen besitzt, also eine von hohem Rang, ebenfalls viele Lösungen in solchen Resten besitzen wird. Wir schreiben N_p für die Anzahl der Lösungen unserer Gleichung in Resten nach Division durch p. Für die früher erwähnte Gleichung $y^2=x^3+1$ und $p=7$ ist z.B. $N_p=11$. Man hat nämlich

x	0	1	2	3	4	5	6	7	8	9
x^3+1	1	2	9	28	65	126	217	344	513	730
Rest nach Division durch 7	1	2	2	0	2	0	0	1	2	2

also für die Reste

x^*	0*	1*	2*	3*	4*	5*	6*
$x^{*3}+1$	1*	2*	2*	0*	2*	0*	0*

und ähnlich

y^*	0*	1*	2*	3*	4*	5*	6*
y^{*2}	0*	1*	4*	2*	2*	4*	1*

Von den 49 möglichen Restepaaren (x^*, y^*) erfüllen also genau 11 unsere Gleichung:

$x^*=0^*$, $y^*=1^*$ oder 6^* (2 Paare),
$x^*=1^*, 2^*$ oder 4^*, $y^*=3^*$ oder 4^* (6 Paare),
$x^*=3^*, 5^*$ oder 6^*, $y^*=0^*$ (3 Paare).

Die entsprechende Rechnung für andere Primzahlen ergibt die Tabelle

p	2	3	5	7	11	13	17	19	23	29	31
N_p	2	3	5	11	11	11	17	11	23	29	35

Die Zahlen N_p können in diesem Fall durch eine schöne (und tiefliegende) Formel ausgedrückt werden:

$$N_p = \begin{cases} p, & \text{falls } p=3 \text{ oder } p \text{ die Gestalt } 3n+2 \text{ hat,} \\ p \pm 2u, & \text{falls } p \text{ die Gestalt } 3n+1 \text{ hat,} \end{cases}$$

wobei im zweiten Fall die Primzahl p als u^2+3v^2 dargestellt wurde (dies ist für Primzahlen der Gestalt $3n+1$ immer auf genau eine Weise möglich!) und das Vorzeichen so gewählt werden muß, daß N_p nicht durch 3 teilbar ist. Aus der Tabelle oder der Formel sieht man, daß N_p immer recht nahe bei p liegt; in der Tat gilt

$$p-2\sqrt{p}<N_p<p+2\sqrt{p}$$

für alle p, und zwar nicht nur in diesem Beispiel, sondern für alle elliptischen Kurven (Hasse, 1933; die Verallgemeinerung – 1974 durch den belgischen Mathematiker Deligne – dieses schon schwierigen Satzes auf Gleichungen in mehreren Variablen gilt als eine der größten intellektuellen Leistungen unseres Jahrhunderts).

Da die Zahlen N_p ungefähr gleich p sind, sind die Verhältnisse $\frac{N_p}{p}$ nahe bei 1. Wir bilden daher das Produkt

$$\frac{N_2}{2}\cdot\frac{N_3}{3}\cdot\frac{N_5}{5}\cdot\ldots\cdot\frac{N_p}{p} \tag{8}$$

(p groß) und erwarten – in Übereinstimmung mit der Idee, daß die Zahlen für Kurven von höherem Rang verhältnismäßig groß sein sollen –, daß das Produkt (8) mit wachsendem p um so schneller anwächst, je größer der Rang der Kurve ist. Dies wurde von Birch und Swinnerton-Dyer (1965) präzisiert: das Produkt (8) soll asymptotisch wie $(\log p)^g$ mit einer ganzen Zahl $g\geq 0$ anwachsen und es soll gelten [8]

$$g=r. \tag{9}$$

Sehr viel der heutigen Forschung dreht sich um Versuche, diese Vermutung zu bestätigen. Die zwei bisher stärksten Teilergebnisse:

1. 1975 zeigten J. Coates und A. Wiles, daß man für eine große Klasse von elliptischen Kurven (die z.B. die Kurve $y^2=x^3+1$ oben enthält) aus $g=0$ auch $r=0$ folgern kann, d.h. eine Gleichung, für die das Produkt (8) beschränkt bleibt, hat nur endlich viele rationale Lösungen.

---

[8] Die hier gegebene Formulierung der Vermutung von Birch und Swinnerton-Dyer ist die elementarste und zuerst gefundene. Meistens wird aber eine andere Version der Vermutung benutzt, die technischer, aber für Forschungszwecke geeigneter ist: das unendliche Produkt

$$L(s)=\prod_{p\,\mathrm{prim}}\frac{1}{1+(N_p-p)/p^s+p/p^{2s}}$$

soll eine vernünftige Funktion von s sein, die eine Nullstelle von einer wohldefinierten Ordnung g bei $s=1$ hat, und mit dieser Zahl g soll die Beziehung (9) gelten.

2. 1983 zeigten B. Gross und ich, daß man für eine noch umfassendere Klasse von elliptischen Kurven (die vermutlich sogar alle elliptischen Kurven enthält) aus $g=1$ $r\geq 1$ folgern kann, d.h. eine Gleichung, für die das Produkt (8) genau logarithmisch wächst, besitzt immer unendlich viele Lösungen.[9]

Da anscheinend die meisten elliptischen Kurven $g=0$ oder $g=1$ haben, werden in der Praxis sehr viele Fälle durch diese beiden Resultate abgedeckt. Für das theoretische Verständnis stellen sie nur einen Anfang dar; 1700 Jahre nach Diophant sind wir immer noch weit davon entfernt, die rationalen Lösungen auch sehr einfacher polynomialer Gleichungen voll zu verstehen.

[9] (Zusatz bei der Korrektur) Inzwischen gibt es neue allgemeine Ergebnisse in Richtung der Vermutung von Birch und Swinnerton-Dyer. Insbesondere konnte Kolyvagin (1988) für die unter 2. erwähnte »noch umfassendere Klasse« zeugen, daß sowohl im Falle $g=0$ wie auch im Falle $g=1$ stets $r=g$ gilt.