Elliptische Kurven: Fortschritte und Anwendungen

Don Zagier

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str.26
D-5300 Bonn 3
Federal Republic of Germany

and

Department of Mathematics
University of Maryland
College Park, MD 20742
U S A

MPI/89 - 23

Elliptische Kurven: Fortschritte und Anwendungen

Don Zagier

Max-Planck-Institut für Mathematik, 5300 Bonn, BRD

und University of Maryland, College Park, MD 20742, USA

§1. Elliptische Kurven

Ich fange an mit einer Definition, die zunächst weder einleuchtend noch besonders vielversprechend aussieht: Eine *elliptische Kurve* ist eine Kurve, die durch eine Gleichung

$$y^2 = x^3 + ax + b \qquad (a,\ b \text{ Konstanten},\ 4a^3 + 27b^2 \neq 0) \tag{1}$$

in der Ebene gegeben werden kann.

Wegen ihrer Tiefe und der Vielfalt ihrer Zusammenhänge mit anderen Gebieten gehört die Theorie der elliptischen Kurven zu den schönsten in der Mathematik. Sie erscheint in der *Funktionentheorie* in der Gestalt der Theorie der elliptischen Funktionen, deren Entwicklung durch **Gauß, Abel** und **Jacobi** zu den Höhepunkten der Mathematik des 19ten Jahrhunderts gehört. Die elliptischen Funktionen sind die doppelt-periodischen Funktionen, die man findet, wenn man elliptische Integrale (die Funktionen, die die Bogenlänge auf Ellipsen messen—daher der Name) umkehrt; für beliebige $a,b \in \mathbb{C}$ läßt sich die Kurve (1) durch solche Funktionen parametrisieren, d.h. es gibt Perioden $\omega_1,\omega_2 \in \mathbb{C}$ und komplexwertige Funktionen $X(z)$, $Y(z)$ auf $\mathbb{C}/\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, die identisch die Gleichung $Y(z)^2 = X(z)^3 + aX(z) + b$ erfüllen. In der *algebraischen Geometrie* sind die elliptischen Kurven gleichwohl die einfachsten interessanten Kurven (d.h. Kurven von positivem Geschlecht) und die einfachsten Beispiele von abelschen Varietäten (Varietäten mit einer abelschen Gruppenstruktur, die durch polynomiale Funktionen gegeben wird) und dienen somit als ideale Einführung in die allgemeine

Theorie. Insbesondere liefern sie schöne Anwendungen des Satzes von Riemann-Roch, der Theorie der Zetafunktionen von Varietäten über endlichen Körpern und des Begriffs einer formalen Gruppe. Der für den heutigen Vortrag wichtige Aspekt von elliptischen Kurven ist aber ihr Auftreten in der *Zahlentheorie*. Vor allem werden wir uns für die rationalen Lösungen der Gleichung (1) interessieren unter der Annahme, daß die Koeffizienten a und b in (1) rationale oder ganze Zahlen sind. Diese harmlos klingende Frage führt zu unerwartet tiefen Erkenntnissen in der Zahlentheorie. Ich will heute einen Überblick über diesen Aspekt der Theorie geben und erzählen, welche Fragen uns gegenwärtig am meisten beschäftigen, welche Fortschritte in letzter Zeit erzielt worden sind und welche Anwendungen inner- und außerhalb der Zahlentheorie daraus entstanden sind. Um die modernen Entwicklungen voll genießen zu können, muß man aber etwas über die Vorgeschichte der elliptischen Kurven wissen, die ich jetzt kurz schildern möchte. Dazu fange ich ganz früh an, mit **Diophant**, einem der größten (und meiner Meinung nach sehr unterschätzten) Mathematiker der Antike.

Die Methode von Diophant. Diophant, der in Alexandria vermutlich im dritten Jahrhundert lebte, war der erste Mathematiker, der systematisch mit negativen und rationalen Zahlen arbeitete, der erste, der Produkte von Zahlen als reine Zahlen betrachtete (statt—wie seine Vorgänger—als Flächeninhalte oder Volumina) und daher mit Potenzen größer als der dritten arbeiten konnte, und der erste, der einen kompletten algebraischen Symbolismus einführte und somit Gleichungen wie etwa $3x^3-2x^2=4$ (was bei ihm so ausgesehen hätte: $\bar{\gamma}K^{\nu}\Uparrow\bar{\beta}\Delta^{\nu}\iota\tilde{\delta}\dot{M}$) schreiben konnte. Seine aus dreizehn Büchern bestehende *Arithmetika* ging nach der Vernichtung der alexandrinischen Bibliothek verloren; erst im Jahr 1570 entdeckte der Astronom und Mathematiker **Johannes Müller ("Regiomontanus")** sechs der Bücher in Venedig in einer arabischen Übersetzung. Diophant war seiner Zeit so weit voraus gewesen, daß es auch dann noch 50 Jahre dauerte, bis der erste europäische Mathematiker, und zwar Pierre de Fermat, sein Werk voll verstehen konnte.

Diophant hatte eine systematische Methode, um quadratische Gleichungen in zwei Veränderlichen zu lösen und kubische anzugreifen. Bei quadratischen ist seine Methode ganz leicht: man fängt mit einer schon bekannten Lösung an, schreibt die Gleichung einer beliebigen Geraden durch diesen Punkt auf und erhält damit eine quadratische Gleichung in einer Veränderlichen, von der man eine rationale Lösung schon kennt; die zweite Lösung ist dann ebenfalls rational. Um z.B. die Lösungen von $x^2+y^2=1$ zu finden, fängt man mit der Lösung $(x,y)=(0,1)$ an, schreibt die Gleichung einer durch diesen Punkt gehenden Geraden als $y=1-tx$ (t rational) auf und rechnet dann:

$$x^2+(1-tx)^2=1, \qquad x^2-2tx+t^2x^2=0, \qquad x=\frac{2t}{1+t^2}, \qquad y=1-tx=\frac{1-t^2}{1+t^2}.$$

Somit erhält man die allgemeine ganzzahlige Lösung $a=2pqr$, $b=(p^2-q^2)r$, $c=(p^2+q^2)r$ $(p,q,r\in\mathbb{Z})$ der pythagoräischen Gleichung $a^2+b^2=c^2$ (setze $x=\frac{a}{c}$, $y=\frac{b}{c}$, $t=\frac{q}{p}$), die allerdings langevor Diophant bekannt war und insbesondere schon bei **Euklid** steht.

Bei kubischen Gleichungen versagt Diophants Methode zunächst, weil die Gerade *zwei* weitere Schnittpunkte mit der Kurve besitzt, aber Diophant entdeckte, daß man bei passender Wahl der Steigung der Geraden nur *eine* weitere Lösung, und zwar eine rationale, findet. Als Beispiel betrachten wir die Gleichung $y^2=x^3-3x+1$. Wie vorher setzen wir die Gleichung $y=1-tx$ der allgemeinen Geraden durch die bekannte Lösung $(x,y)=(0,1)$ ein und erhalten eine polynomiale Gleichung in x, deren konstantes Glied wegfällt:

$$(1-tx)^2=x^3-3x+1, \qquad x^3-t^2x^2+(2t-3)x=0.$$

Da diesmal aber die Gleichung kubisch statt quadratisch ist, haben wir auch nach Kürzung eines Faktors x immer noch eine quadratische Gleichung, deren Lösungen nicht rational zu sein brauchen. Wählen wir aber speziell $t=3/2$, so fällt auch das lineare Glied unserer kubischen Gleichung weg und wir können einen Faktor x^2 kürzen, um eine lineare Gleichung zu erhalten, die sofort gelöst werden kann:

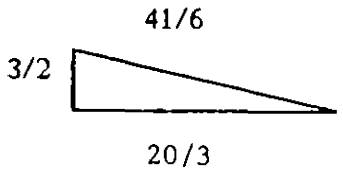
$$y=1-\frac{3}{2}x, \qquad x^3-\frac{9}{4}x^2=0, \qquad x=\frac{9}{4}, \qquad y=1-\frac{3}{2}\cdot\frac{9}{4}=-\frac{19}{8}.$$

Der geometrische Inhalt der Methode ist klar: während wir im Falle eines Kegelschnittes durch einen gegebenen Punkt eine *beliebige* Gerade ziehen und genau einen weiteren Schnittpunkt erhalten konnten, müssen wir im kubischen Falle die *Tangente* wählen, damit nicht zwei, sondern nur ein weiterer Schnittpunkt entsteht. Die geometrische Interpretation, die sehr wichtig ist—wir werden in Zukunft gar nicht zwischen den *Lösungen* der Gleichung (1) und den *Punkten* auf der von ihr beschriebenen Kurve E unterscheiden—stand natürlich Diophant noch nicht zur Verfügung. Sie wurde erst von **Isaac Newton** bemerkt.

Fermat und die Methode des unendlichen Abstiegs. Diophants Methode wurde von **Fermat** zu seiner berühmten Methode der "descente infinie" oder "unendlicher Abstieg" weiterentwickelt. Diese Methode sieht wie folgt aus. Die Diophantische Konstruktion assoziiert zu jeder Lösung $P=(x,y)$ von (1) eine zweite Lösung $P'=(x',y')$ (=dritter Schnittpunkt der Tangenten durch P mit der Kurve), die im allgemeinen kompliziertere Koordinaten hat, d.h., die Zähler und Nenner von x' und y' sind meistens viel größer als

die von x und y. Unter geeigneten Umständen kann man zeigen, daß jede Lösung von (1) auf diese Weise entsteht, d.h. sie hat die Gestalt P' für eine i.a. viel einfachere Lösung P. Wiederholt man dieses Verfahren, so kommt man zu immer kleineren Lösungen von (1) und somit zu einem Widerspruch, falls (1) keine ganz kleinen Lösungen hat, und zu einer Beschreibung aller Lösungen, falls es eine kleine Lösung gibt. Die Methode hat also sowohl negative wie auch positive Anwendungen. Z.B. hat Fermat selbst sie benutzt, um zu zeigen, daß die Gleichungen $x^4+y^4=z^2$ und $x^4+y^2=z^4$ (also erst recht die Gleichung $x^4+y^4=z^4$) keine Lösungen in positiven ganzen Zahlen besitzen, aber auch, um das einfachste ganzzahlige pythagoräische Dreieck zu finden, wovon sowohl die Hypotenuse wie auch die Summe der Katheten Quadrate sind (Brief von Fermat an Mersenne, 1643; die Lösung lautet 1061652293520, 4565486027761, 4687298610289).

Wir illustrieren Fermats Methode anhand eines sehr klassischen Problems, das über 1000 Jahre alt ist (es taucht in einem vor 972 datierten anonymen arabischen Manuskript auf) und dem Leonardo Pisano ("Fibonacci") ein ganzes Buch, sein *liber quadratorum*, widmete: das Problem der sogenannten kongruenten Zahlen. Die Aufgabe besteht darin, eine gegebene Zahl n als Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seiten darzustellen oder (äquivalenterweise: Übungsaufgabe!) drei rationale Quadrate in arithmetischer Progression mit gemeinsamer Differenz n zu finden. Falls das Dreieck bzw. die Quadrate existieren, heißt n "kongruent". Für $n=5$ lautet die bereits in den erwähnten Büchern gegebene Lösung

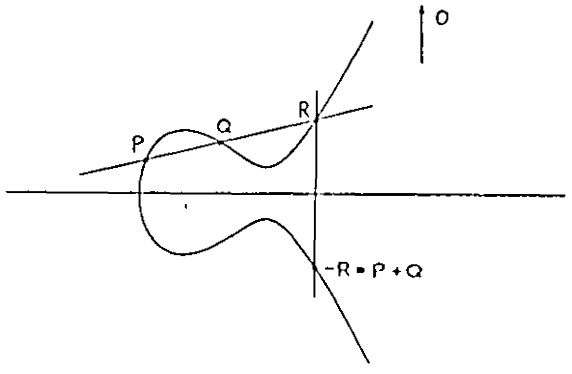


bzw. $6\frac{97}{144}=\left(2\frac{7}{12}\right)^2$, $11\frac{97}{144}=\left(3\frac{6}{12}\right)^2$, $16\frac{97}{144}=\left(4\frac{1}{12}\right)^2$

Um das Problem anzugehen, betrachten wir die durch die Gleichung $y^2=x(x+n)(x-n)$ gegebene elliptische Kurve. Ist $P=(x,y)$ eine beliebige nichttriviale Lösung (d.h. $y\neq 0$) dieser Gleichung, so hat der durch Diophants Tangentenmethode konstruierte Punkt $P'=(x',y')$ die Eigenschaft, daß nicht nur das Produkt $x'(x'+n)(x'-n)$ $(=y'^2)$, sondern alle drei Faktoren $x', x'+n, x'-n$ Quadratzahlen sind, d.h., n ist kongruent. Für die Ausgangslösung P brauchen x und $x\pm n$ nicht Quadrate zu sein, aber sie sind bis auf quadratische Faktoren sehr eingeschränkt. Ist z.B. n prim und $\equiv 5 \pmod 8$, so zeigt man leicht, daß jede von diesen drei Zahlen eine der Gestalten $\pm\square$, $\pm 2\cdot\square$, $\pm n\cdot\square$ oder $\pm 2n\cdot\square$ ($\square$=rationale Quadratzahl) haben muß. Dies führt zur Unterscheidung endlich vieler Fälle, die einzeln untersucht werden. Ist z.B. $x=-A^2$, $x+n=B^2$, $x-n=-C^2$ (und man kann in unserem Falle n prim, $n\equiv 5 \pmod 8$ leicht zeigen, daß es, wenn überhaupt, stets eine solche Lösung gibt), so müssen wir das Gleichungssystem

$C^2-B^2=2A^2$, $C^2-A^2=n$ lösen. Die erste Gleichung läßt sich nach Diophants Methode sofort lösen: es muß gelten $A=2RS/M$, $B=(R^2-2S^2)/M$, $C=(R^2+2S^2)/M$ für passende ganze Zahlen R, S, M. Damit ist das Problem auf die Lösbarkeit von $M^2n=R^4+4S^4$ reduziert worden. Für $n=5$ ist jetzt die Lösung $M=R=S=1$ ($\Leftrightarrow$ $x=-4$, $y=6$, $x'=6\frac{97}{144}$) evident. Für andere Primzalen n muß man unter Umständen den Abstieg ein- oder mehrmals wiederholen, wobei man als ersten Schritt die Diophantische Methode auf die quadratische Gleichung $n=U^2+4V^2$ anwendet und eine Lösung mit $UV=\square$ ($\Rightarrow$ $U=R^2/M$, $V=S^2/M$) zu finden versucht. Für $n=157$ etwa führt diese Methode nach einigen Schritten zu einer Lösung. Diese ist, wie Fermat vielleicht gesagt haben würde, ganz wunderbar, aber die Seite ist leider zu schmal, um sie zu enthalten: die drei rationalen Quadratzahlen haben im Zähler und Nenner jeweils fast 100 Dezimalziffern.

Gruppenstruktur. Satz von Mordell. Was Diophant und Fermat entdeckt hatten, war die erste Andeutung des Additionsgesetzes auf elliptischen Kurven: Statt der Tangenten durch *einen* Punkt P kann man die Sehne durch *zwei* Punkte P, Q betrachten, die einen dritten Schnittpunkt mit der Kurve besitzt. Schreibt man diese als $-(P+Q)$, so ist "+", wie es sich herausstellt, eine kommutative, assoziative binäre Operation auf der Menge der Lösungen, die (unter Hinzunahme des unendlichen fernen Punkts O als Nullelement) damit zu einer *abelschen Gruppe* wird. Es ist die Existenz dieser Zusatzstruktur, die für den Reichtum der Theorie der elliptischen Kurven verantwortlich ist.



Gruppengesetz auf $E(\mathbb{Q})$
Addition: $P+Q+R=0 \Leftrightarrow P,Q,R$ kollinear
Inverses: $P=(x,y) \Rightarrow -P=(x,-y)$
Nullelement: O = Punkt im Unendlichen

Natürlich kam diese Formulierung in der Sprache der Gruppentheorie erst viel später, und zwar mit **Poincaré**, um 1900. Poincaré hat vermutet, daß die Gruppe der rationalen Lösungen einer elliptischen Kurve mit rationalen Koeffizienten stets *endlich erzeugt* sei, d.h. daß man sämtliche Lösungen der Gleichung aus endlich vielen durch wiederholte Anwendung der Sehnenkonstruktion erhalten könne. Seine Vermutung wurde 1922 von dem englischen Mathematiker **L.J. Mordell** bewiesen. Mordells Satz wurde 1940 von **A. Weil** verallgemeinert, indem er beliebige algebraische Zahlkörper (statt $\mathbb{Q}$) und beliebige abelsche Varietäten (statt nur elliptische Kurven) zuließ. Die Gruppe der rationalen Punkte auf einer elliptischen Kurve E (einschließlich des Punktes O) wird die

Mordell-Weil-Gruppe genannt und mit $E(\mathbb{Q})$ bezeichnet. Unsere Hauptfragen betreffen die Struktur dieser Gruppe.

Struktur der Mordell-Weil-Gruppe. Nach dem Struktursatz für endlich erzeugte abelsche Gruppen hat die Mordell-Weil-Gruppe die Gestalt

$$E(\mathbb{Q}) \simeq \mathbb{Z}\oplus\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}\oplus T \tag{2}$$
$$r$$

für eine bestimmte Zahl $r\geq 0$ (der *Rang* von E) und eine endliche abelsche Gruppe T (die *Torsionsgruppe* von E). Die Zahl r, die die wichtigste diophantische Invariante der Kurve E ist, hat eine schöne Interpretation, die ohne die Gruppenstruktur auf $E(\mathbb{Q})$ erklärt werden kann: bezeichnet $N(B)$ die Anzahl der Lösungen von Gleichung (1), für die der Zähler und Nenner von x kleiner oder gleich einer positiven Zahl B sind, so gilt

$$N(B)+1 \sim C(\log B)^{r/2} \qquad (B\to\infty) \tag{3}$$

mit einer bestimmten, nur von der Kurve E abhängigen reellen Konstanten C. (Die Zahl "+1" auf der linken Seite von (3) wird gebraucht, weil man beim Zählen der rationalen Lösungen auch den Punkt im Unendlichen mitzählen muß.) Der Beweis von (3) ist ein Korollar des Beweises des Mordellschen Satzes.

In Anbetracht der Formel (2) können wir die Frage nach der Struktur von $E(\mathbb{Q})$ wie folgt präzisieren:

i) Wie bestimmt man die Torsionsgruppe T einer gegebenen elliptischen Kurve?

ii) Was sind die Möglichkeiten für T? Wie häufig kommen sie jeweils vor?

iii) Wie bestimmt man den Rang r einer gegebenen elliptischen Kurve?

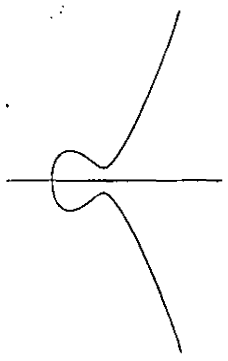
iv) Was sind die Möglichkeiten für r? Wie häufig kommen sie jeweils vor?

Die Antwort zur ersten Frage ist ein elementarer Satz, die zur zweiten Frage ein sehr schwieriger Satz, die zur dritten Frage nur eine Vermutung, und die zur vierten Frage noch unbekannt. Genauer:

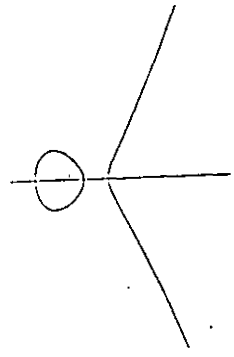
Zu i): Seien o.B.d.A. die Zahlen a, b in (1) ganz (da wir sie durch $x\mapsto k^2x$, $y\mapsto k^3y$ durch k^4a, k^6b ersetzen können). Dann gilt der relativ elementare Satz von **Nagell-Lutz:** Jeder Torsionspunkt $P\neq 0$ in $E(\mathbb{Q})$ hat ganze Koordinaten und eine y-Koordinate, die entweder gleich 0 oder ein Teiler von $4a^3+27b^2$ ist. (Natürlich ist $y=0$ mit $P=-P$ oder $2P=O$ äquivalent, da $-(x,y)=(x,-y)$.) Damit hat man für eine gegebene Kurve E nur endlich viele Kandidaten für Torsionspunkte und kann sie alle durchprobieren.

Zu ii): Die Gruppe $E(\mathbb{Q})$ ist eine Untergruppe von $E(\mathbb{R})$, der Gruppe der *reellen* Lösungen von (1) (zusammen mit dem unendlich fernen Punkt O). Diese Gruppe ist

isomorph zur Kreislinie $S^1=\mathbb{R}/\mathbb{Z}$ oder zum Produkt $S^1\times\mathbb{Z}/2\mathbb{Z}$, je nachdem, ob $4a^3+27b^2$ positiv oder negativ ist.



$4a^3+27b^2>0$



$4a^3+27b^2<0$

Somit muß der Torsionsanteil T von $E(\mathbb{Q})$ entweder zyklisch oder das Produkt einer zyklischen Gruppe mit $\mathbb{Z}/2\mathbb{Z}$ sein. Da die 2-Torsion von $E(\mathbb{Q})$ gerade die Menge der Punkte $(x,0)$ mit $x\in\mathbb{Q}$, $x^3+ax+b=0$, ist, haben wir den Strukturssatz:

x^3+ax+b über $\mathbb{Q}$ irreduzibel $\Rightarrow T\simeq\mathbb{Z}/n\mathbb{Z}$, n ungerade,
$x^3+ax+b=$(linear)$\times$(quadratisch) über $\mathbb{Q}\Rightarrow T\simeq\mathbb{Z}/n\mathbb{Z}$, n gerade,
x^3+ax+b zerfällt in lineare Faktoren über $\mathbb{Q}\Rightarrow T\simeq\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, n gerade.

So weit ist alles elementar. Alles andere als elementar ist der 1977 von B. Mazur bewiesene Satz, daß der Wert von n in den drei Fällen durch 9 bzw. 12 bzw. 8 beschränkt ist. Hiernach gibt es genau 15 Möglichkeiten für die Torsionsgruppe T. Alle kommen für unendlich viele Kurven E vor. Dabei ist allerdings $|T|=1$ der generische Fall, und die anderen Möglichkeiten treten nur für spezielle Werte von b^2/a^3 auf, z.B. kann $|T|$ nur gerade sein, wenn b^2/a^3 die Gestalt $c(c+1)^2$ mit $c\in\mathbb{Q}$ hat (nämlich $c=x^2/a$, $x\in\mathbb{Q}$, $x^3+ax+b=0$). Mazurs Satz beruht auf einer sehr tiefliegenden Analyse von Modulkurven vom Standpunkt der arithmetischen algebraischen Geometrie.

Zu iii): Eine obere Abschätzung für den Rang einer gegebenen elliptischen Kurve E wird durch die Fermatsche Methode des unendlichen Abstiegs geliefert. Z.B. hat die Kurve $y^2=x^3-n^2x$, die wir im Zusammenhang mit dem Problem der kongruenten Zahlen betrachteten, den Rang 0, falls n eine Primzahl $\equiv 3$ (mod 8) ist, Rang ≤ 1, falls n prim und $n\equiv 5$ oder 7 (mod 8), und Rang ≤ 2, falls n prim und $n\equiv 1$ (mod 8). Eine untere Abschätzung kann natürlich dadurch geschehen, daß man eine bestimmte Anzahl von linear unabhängigen Lösungen hinschreibt. Z.B. hat die Kurve $y^2=x^3-25x$ Rang mindestens 1 (also tatsächlich gleich 1), weil $(-4,6)$ eine Lösung unendlicher Ordnung ist. Häufig gibt es aber eine Kluft zwischen der oberen und der unteren Abschätzung—entweder, weil Fermats Methode zu grob ist (z.B. ist im Falle $n\equiv 1$ (mod

8) oben der wahre Wert des Ranges häufig 0 statt 2) oder, weil die Lösungen außerhalb des Suchbereichs liegen (etwa die fast 100-stellige kleinste Lösung für $n=157$). Eine einigermaßen befriedigende Antwort auf die Frage, wie man den Rang bestimmt, wird erst durch die Birch-Swinnerton-Dyer-Vermutung gegeben, die wir gleich besprechen wollen.

Zu iv): Hier ist, wie bereits gesagt, nichts bekannt. Der Weltrekord für den größten bekannten Rang stand 1948 bei 4, 1974 bei 6, und ist jetzt 14 (**Mestre**, 1984), nachdem **Néron** 1954 abstrakt (d.h., ohne Beispiele anzugeben) bewiesen hatte, daß es unendlich viele elliptische Kurven mit Rang ≥ 11 geben muß. Es wird allgemein vermutet, daß es elliptische Kurven mit beliebig hohem Rang gibt. Kurven von hohem Rang sind aber nicht leicht zu finden: Mestres Beispiel hat (in der Schreibweise (1)) die Koeffizienten $a=-35971713708112$, $b=85086213848298394000$.

Über die Frage, wie die verschiedenen Werte von r verteilt sind, ist ebenfalls nichts bekannt. Immerhin liefert die Vermutung von Birch und Swinnerton-Dyer eine Vorhersage für die Parität von r (siehe unten), die ungefähr gleich häufig gerade und ungerade ausfällt. Bis vor kurzer Zeit glaubten die meisten Spezialisten, daß für fast alle Kurven der Rang den minimalen Wert annimmt, der nach dieser Einschränkung der Parität zulässig ist, d.h., r ist fast immer gleich 0, wenn er gerade sein muß, und gleich 1, wenn er ungerade sein muß. Aber numerische Rechnungen für die Familie der elliptischen Kurven $x^3+y^3=m$ ($m\leq 70000$, m kubenfrei), die vor kurzem ausgeführt worden sind, ergaben für $r=0$, $r=1$, $r\geq 2$ die Dichten 38,3%, 48,9% und 12,8% anstelle der erwarteten Werte 50%, 50% und 0%. Die Situation hier ist also zur Zeit unklar.

Die Vermutung von Birch und Swinnerton-Dyer. L-Reihen. Modulare elliptische Kurven. Die entscheidende Idee zu der Frage, wie man den Rang einer elliptischen Kurve finden kann, ist in einer Vermutung enthalten, die Anfang der 60er Jahre von **B. Birch** und **H.P.S. Swinnerton-Dyer** aufgestellt wurde. Diese Idee ist, daß eine Gleichung mit besonders vielen rationalen Lösungen (d.h. eine Kurve mit besonders hohem Rang) auch besonders viele Lösungen in dem Körper der ganzen Zahlen modulo einer Primzahl p haben soll—mindestens "im Durchschnitt", wenn p variiert. Um dies quantitativ zu formulieren, definiert man für jede Primzahl p

$$N(p) = \text{Anzahl der Paare } (x,y) \pmod p \text{ mit } y^2\equiv x^3+ax+b.$$

Man würde naiv erwarten, daß $N(p)$ ungefähr gleich p ist, weil es p^2 Paare (x,y) (mod p) gibt und für jedes Paar die Wahrscheinlichkeit, daß die Kongruenz gilt, gleich $1/p$ beträgt, oder weil es p Werte für x gibt modulo p gibt und für jedes x mit $x^3+ax+b\not\equiv 0$ die Anzahl der Quadratwurzeln von x^3+ax+b mit gleicher Wahrscheinlichkeit gleich 0 oder 2 ist. Diese naive Erwartung wird bestätigt durch den von H.

Hasse 1933 bewiesenen Satz

$$p - 2\sqrt{p} < N(p) < p + 2\sqrt{p} \tag{4}$$

("Riemannsche Vermutung für elliptische Kurven"). Die Vermutung von Birch und Swinnerton-Dyer ("BSD-Vermutung") besagt nun in der einfachsten Formulierung, daß man die asymptotische Formel

$$\prod_{p<x} \frac{N(p)+1}{p} \sim C_1 (\log x)^r \qquad (x \to \infty) \tag{5}$$

hat, wobei C_1 eine positive reelle Zahl ist, die nur von der elliptischen Kurve abhängt, und r den Rang der Kurve bezeichnet. (Man nimmt hier $N(p)+1$ statt $N(p)$ aus demselben Grund wie in (3).) Daß dieselbe Zahl r in den asymptotischen Formeln (3) und (5) vorkommt, stellt eine wunderbare und tiefliegende Beziehung zwischen den Lösungen von (1) in den Körpern $\mathbb{Q}$ und $\mathbb{Z}/p\mathbb{Z}$ dar.

Allerdings ist die Formel (5) wegen der sehr langsamen Divergenz des Produktes sowohl für theoretische wie auch für numerische Überlegungen etwas ungeeignet. Eine viel bessere Formulierung der BSD-Vermutung, die ebenfalls von Birch und Swinnerton-Dyer angegeben wurde, involviert die *L-Reihe* von E. Diese ist eine Funktion einer komplexen Variablen s, die für s genügend groß durch die Formel

$$L(s) \approx \prod_p \frac{1}{1 + \left(N(p) - p\right) p^{-s} + p^{1-2s}} \tag{6}$$

definiert wird, wobei das Produkt über alle Primzahlen p läuft und das Zeichen "$\approx$" bedeutet, daß die Definition des Faktors für p geändert werden muß, falls p die Diskriminante $4a^3+27b^2$ teilt (die genaue Definition in diesem Falle spielt für uns keine Rolle). Wegen (4) konvergiert dieses Produkt, falls s (oder der Realteil von s) größer als 3/2 ist. Die präzisere Formulierung der BSD-Vermutung besagt, daß die Funktion $L(s)$ in s analytisch fortsetzbar ist und eine Nullstelle genau $r$ter Ordnung im Punkt $s=1$ besitzt. (Man sieht, daß dies eine Art Präzisierung von (5) ist, weil bei $s=1$ das unendliche Produkt in (6) formal zu $\prod \frac{p}{N(p)+1}$ wird.) Ferner soll der Anfang der Taylor-Entwicklung von $L(s)$ bei $s=1$ durch die Formel

$$L(s) \sim C_0 (s-1)^r \quad (s \to 1), \qquad C_0 = \pi^{-r} \Gamma(\tfrac{r}{2}+1)^2 C^{-2} \Omega\, |Ш| \tag{7}$$

gegeben werden, wobei C die Konstante in (3) bezeichnet, Ω ein einfaches Vielfaches des elliptischen Integrals $\int_\alpha^\infty (x^3+ax+b)^{-1/2}\,dx$ (α = größte reelle Wurzel von $x^3+ax+b=0$), und $|Ш|$ die Ordnung der sogenannten *Tate-Schafarewitsch-Gruppe* Ш von E, einer

bestimmten abelschen Gruppe, die mit der Lösbarkeit in rationalen Zahlen von gewissen mit (1) verwandten diophantischen Gleichungen zu tun hat (die genaue Definition von Ш werden wir nicht geben). Die Vermutung (7) ist besonders kühn, weil man im allgemeinen nicht nur nicht weiß, ob die Funktion $L(s)$ in der Nähe von $s=1$ erklärt ist, sondern auch nicht, ob die Gruppe Ш überhaupt endlich ist!

Die Gestalt der Euler-Faktoren in (6) ist zunächst keineswegs einleuchtend. Daß man genau diese Definition der L-Funktion nehmen muß, liegt daran, daß es eine sehr große Klasse von elliptischen Kurven gibt, für die man weiß, daß $L(s)$ gute analytische Eigenschaften hat. Das sind die sogenannten *modularen elliptischen Kurven*. Eine elliptische Kurve E heißt *modular*, wenn sie durch *Modulfunktionen* parametrisiert werden kann, d.h., es gibt eine Zahl N und zwei Funktionen $\xi(\tau)$ und $\eta(\tau)$ ($\tau\in\mathbb{C}$, $\Im(\tau)>0$) mit den folgenden Eigenschaften:

(a) $\xi(\tau)$ und $\eta(\tau)$ sind invariant unter $\tau\mapsto\frac{A\tau+B}{NC\tau+D}$ $(A,B,C,D\in\mathbb{Z},\ AD-NBC=1)$;

(b) $\xi(\tau)$ und $\eta(\tau)$ haben Fourier-Entwicklungen in $e^{2\pi i\tau}$ mit Koeffizienten in $\mathbb{Q}$;

(c) Es gilt $\eta(\tau)^2=\xi(\tau)^3+a\,\xi(\tau)+b$ identisch in τ.

Unter diesen Voraussetzungen weiß man, daß die zwei folgenden Behauptungen gelten:

(d) Ist $L(s)=\sum_{n=1}^{\infty}a_n n^{-s}$, so ist die assoziierte Funktion $f(\tau)=\sum_{n=1}^{\infty}a_n e^{2\pi i n\tau}$ eine *Modulform der Stufe* N: es gilt $f\left(\frac{A\tau+B}{NC\tau+D}\right)=(NC\tau+D)^2 f(\tau)$ für $A,B,C,D\in\mathbb{Z}$, $AD-NBC=1$.

(e) Die Funktion $L(s)$ ist eine ganze Funktion von s und erfüllt die Funktionalgleichung $(2\pi)^{-s}N^{s/2}\Gamma(s)L(s)=\pm(2\pi)^{s-2}N^{1-s/2}\Gamma(2-s)L(2\text{-}s)$. Dabei läßt sich das Vorzeichen explizit bestimmen, was zusammen mit der Formel (7) eine explizite Vermutung über die Parität des Ranges liefert (r soll gerade oder ungerade sein, je nachdem, ob ein Plus- oder Minuszeichen in der Funktionalgleichung vorkommt).

Es wird allgemein vermutet, daß *jede* elliptische Kurve über $\mathbb{Q}$ in der Tat modular ist. Diese tiefe und aufregende Vermutung, die auch außerhalb der Theorie der elliptischen Kurven sehr wichtige Konsequenzen haben würde (siehe "Anwendungen"), heißt meistens die Taniyama-Weil-Vermutung, weil Taniyama 1955 die Frage aufgeworfen hat, ob die L-Funktionen von elliptischen Kurven mit den L-Reihen von Modulformen zusammenhängen, und Weil 1967 bewiesen hat, daß elliptische Kurven über $\mathbb{Q}$, deren assoziierte L-Funktionen Funktionalgleichungen wie in (e) besitzen (was nach den schon damals existierenden Vermutungen über Zetafunktionen von algebraischen Varietäten immer zu erwarten gewesen wäre), tatsächlich modular sind. In der Literatur findet man häufig die Terminologie "Weil-Kurve" statt "modulare elliptische Kurve".

§2. Fortschritte

Im letzten Abschnitt haben wir einen Teil der historischen Entwicklung der Theorie der elliptischen Kurven beschrieben und dabei auch über einige wichtige Sätze berichtet, die in neuerer Zeit bewiesen worden sind (z.B. Hasses Satz über die Anzahl der Punkte modulo einer Primzahl und Mazurs Satz über die möglichen Torsionsuntergruppen einer elliptischen Kurve über $\mathbb{Q}$). Wir wollen jetzt systematischer über neuere Ergebnisse berichten, wobei wir uns nur auf solche konzentrieren werden, die mit der Vermutung von Birch und Swinnerton-Dyer zusammenhängen. Natürlich hat es viele wichtige und schöne Resultate gegeben, die andere Aspekte der Theorie betreffen, etwa den Satz von Silverman (1986), wonach—grob formuliert—die Anzahl der ganzzahligen Lösungen von (1) durch $C^{(r+1)(s+1)}$ (r = Rang der elliptischen Kurve, s = Anzahl der Primfaktoren von $4a^3+27b^2$, C eine effektiv bestimmbare universelle Konstante) abgeschätzt werden kann (daß diese Anzahl endlich ist, wurde schon 1929 von **C.L. Siegel** bewiesen), oder der Satz von **Elkies** (1987), wonach eine beliebige elliptische Kurve E unendlich viele supersinguläre Primzahlen p (das sind solche mit $N(p)=p$) besitzt. Aus naheliegenden Gründen müssen wir uns aber auf nur einen Teil der Theorie beschränken.

Um einige der Ergebnisse zu formulieren, müssen wir noch eine wichtige Klasse von elliptischen Kurven einführen. Das sind die sog. Kurven mit *komplexer Multiplikation* oder (nach den englischen Anfangsbuchstaben) *CM-Kurven*. Eine elliptische Kurve E hat genau dann komplexe Multiplikation, wenn sie eine nichttriviale algebraische Abbildung in sich selbst zuläßt, die die Gruppenstruktur erhält. Zum Beispiel ist

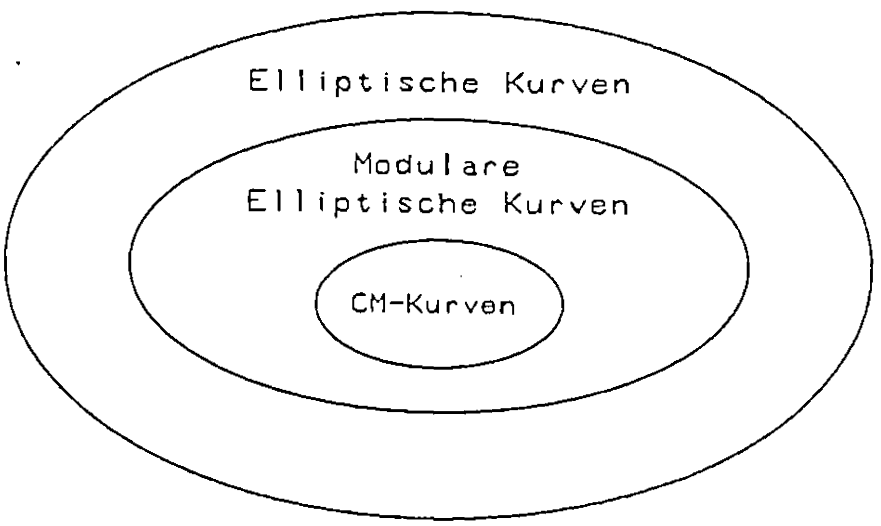
$$y^2=x^3-35x+98=(x+7)(x-\alpha)(x-\bar{\alpha}) \qquad \left[\alpha=\frac{7+i\sqrt{7}}{2}\right]$$

eine CM-Kurve, weil mit (x,y) auch

$$\left[x'=\frac{(x+7)(x-\bar{\alpha})}{\lambda^2(x-\alpha)}+\bar{\alpha},\quad y'=\frac{y(x+i\sqrt{7})(x-7-2i\sqrt{7})}{\lambda^3(x-\alpha)^2}\right] \qquad \left[\lambda=\frac{-1+i\sqrt{7}}{2}\right]$$

eine Lösung ist und die Abbildung $(x,y)\mapsto(x',y')$ ein Gruppenhomomorphismus ist. Die Kurven mit komplexer Multiplikation sind relativ selten: man weiß, daß die Gleichung (1) (mit $a,b\in\mathbb{Q}$) genau dann eine CM-Kurve definiert, wenn entweder a oder b gleich Null ist oder die rationale Zahl a^3/b^2 einen von 11 speziellen Werten annimmt, wovon der einfachste $-\frac{125}{28}$ und der komplizierteste $-\frac{37933248432640000}{5627087890963}$ ist. Eine Besonderheit von CM-Kurven, deren Entdeckung im Prinzip auf Gauß zurückgeht, ist, daß die Anzahl $N(p)$

der Lösungen modulo einer Primzahl p durch eine einfache Formel gegeben werden kann, z.B. ist diese Anzahl für die Kurve $y^2=x^3-35x+98$ gleich $p\pm 2M$, falls p eine Darstellung als M^2+7N^2 zuläßt, und gleich p sonst. Nach Arbeiten von **Max Deuring** weiß man, daß jede CM-Kurve auch modular ist. Die bisher eingeführten Klassen von elliptischen Kurven lassen sich also durch das Venn-Diagramm



veranschaulichen, wobei die kleinste Teilmenge klein und die mittlere Teilmenge vermutlich gleich der gesamten Menge ist.

Wir bezeichnen den Rang einer elliptischen Kurve E mit r und, falls E modular ist, die Ordnung der L-Reihe von E bei $s=1$ (die manchmal "analytischer Rang von E" genannt wird, weil sie nach der BSD-Vermutung mit r übereinstimmen soll) mit r'. Die Sätze, die wir nennen wollen, lauten nun wie folgt:

Coates-Wiles (1977): Ist E eine CM-Kurve mit $r'=0$, so ist auch $r=0$.
Der Satz besagt also, daß die Mordell-Weil-Gruppe einer CM-Kurve endlich ist, falls $L(1)$ nicht verschwindet. Der sehr raffinierte Beweis läuft nicht über die komplexe L-Reihe, sondern über ein p-adisches Analogon $L_p(s)$, dessen Wert bei $s=1$ mit dem entsprechenden Wert der komplexen L-Funktion zusammenhängt.

Greenberg (1983): Ist E eine CM-Kurve mit r' ungerade, so ist entweder $r\geq 1$ oder Ш, die Tate-Schafarewitsch-Gruppe von E, ist unendlich.
Zu diesem Satz können wir, da wir Ш nicht genau definiert haben, nur bemerken, daß der Beweis wieder p-adische L-Funktionen benutzt.

Gross-Zagier (1983): Ist E eine modulare elliptische Kurve mit $r'=1$, so ist $r\geq 1$.
Mit anderen Worten, man hat hier im Gegensatz zu dem Satz von Coates und Wiles ein Kriterium dafür, daß die Mordell-Weil-Gruppe *unendlich* ist: das ist bestimmt der Fall,

wenn $L(1)=0$ und $L'(1)\neq 0$. Der Beweis beruht auf der Theorie der *Heegner-Punkte*. Das sind gewisse rationale Punkte auf E, die man konstruieren kann, wenn E modular ist und die L-Reihe im Punkt $s=1$ verschwindet. Diese Punkte erhält man auf die folgende Weise. Setzt man in der modularen Parametrisierung $\tau \mapsto P(\tau)=(\xi(\tau),\eta(\tau))$ einen imaginär-quadratischen Wert τ_0 ein, so hat der Punkt $P(\tau_0)\in E$ algebraische Koordinaten, und die Summe P_0 von allen zu $P(\tau_0)$ konjugierten Punkten gehört zu $E(\mathbb{Q})$. In der Arbeit von Gross-Zagier wurde gezeigt, daß die *Höhe* von P_0 (das ist ein bestimmtes Maß für die Größe der Zähler und Nenner der Koordinaten von P_0) proportional zu $L'(1)$ ist. Insbesondere ist (für eine geeignete Wahl von τ_0) P_0 ein Element unendlicher Ordnung von $E(\mathbb{Q})$, falls $L'(1)\neq 0$, womit man die oben angegebene Version des Satzes erhält.

Rubin (1987): Ist E eine CM-Kurve mit $r'=0$, so ist Ш endlich.
Mit anderen Worten, unter denselben Voraussetzungen wie im Satz von Coates-Wiles (CM-Kurve, $L(1)\neq 0$) läßt sich beweisen, daß die Tate-Schafarewitsch-Gruppe von E endlich ist; außerdem liefert Rubins Beweis einen Teil der Behauptung über die Ordnung $|Ш|$ in der BSD-Vermutung. Da wir die Definition von Ш nicht gegeben haben, können wir schwerlich eine Vorstellung von der Rubinschen Beweisidee geben, außer zu sagen, daß Ш eine Art Analogon der Klassengruppe eines algebraischen Zahlkörpers ist und daß Rubins Beweis durch eine neue Methode von F. Thaine zur Abschätzung solcher Klassengruppen inspiriert wurde. Bevor dieser Satz bewiesen wurde, gab es keine einzige elliptische Kurve, für die die Endlichkeit der Tate-Schafarewitsch-Gruppe nachgewiesen worden war!

Kolyvagin (1988): Ist E eine modulare elliptische Kurve mit $r'=0$, so sind $E(\mathbb{Q})$ und Ш endlich (und die BSD-Formel für $L(1)$ ist fast wahr).
Mit anderen Worten, die sehr einschränkende Annahme der komplexen Multiplikation in den Sätzen von Coates-Wiles und Rubin läßt sich durch die viel schwächere Annahme der Modularität ersetzen. Eigentlich hat Kolyvagin den Satz nicht ganz wie oben formuliert bewiesen, sondern er benötigte zusätzlich noch eine gewisse analytische Voraussetzung (nämlich, daß es unter den Kurven, die man erhält, indem man die linke Seite von (1) mit einer rationalen Zahl $d\neq 0$ multipliziert, mindestens eine mit analytischem Rang $r'=1$ gibt). Es war aber sehr stark anzunehmen, daß diese zusätzliche Bedingung für jede modulare elliptische Kurve erfüllt ist, und diese Annahme ist gerade von Bump-Friedberg-Hoffstein und unabhängig von K. und R. Murty auf analytische Weise bewiesen worden. Kolyvagins genialer Beweis beruht auf kohomologischen Methoden und ist in einem gewissen Sinne erstaunlich einfach.

§3. Anwendungen

Wir werden in diesem letzten Abschnitt einige Anwendungen der Theorie der elliptischen Kurven auf klassische Probleme der diophantischen Analysis beschreiben. Natürlich bestehen auch andere Arten von Anwendungen. Insbesondere hat die Theorie der elliptischen Kurven über endlichen Körpern (speziell: die Abschätzung (4) und die Tatsache, daß die Gruppe der Lösungen modulo einer Primzahl p immer entweder zyklisch oder das Produkt zweier zyklischer Gruppen ist) in den letzten Jahren mehrere Anwendungen in der algorithmischen Zahlentheorie gefunden, z.B. die deterministische Bestimmung der Darstellung einer Primzahl $p \equiv 1 \pmod 4$ als Summe zweier Quadratzahlen in polynomialer Zeit (Schoof, 1980), ein nicht-deterministischer, aber häufig sehr schneller Algorithmus zur Faktorisierung großer Zahlen (Lenstra, 1986) und verschiedene hiermit verwandte Algorithmen zur Nachprüfung oder zur "Zertifikation" von großen Primzahlen (Goldwasser-Kilian, 1986, Pomerance, 1987). In einer völlig anderen Richtung liefert die Theorie der ganzzahligen Punkte auf elliptischen Kurven die Aussage, daß 24 die einzige Zahl $n>1$ ist, für die $1^2+\cdots+n^2$ ein Quadrat ist; diese Eigenschaft von 24 hängt nach Conway-Sloane mit der Existenz des 24-dimensionalen Leechschen Gitters und somit mit der Erscheinung der Zahl 26 in der Stringtheorie ("no-ghost theorem") und vielleicht mit der Dimension des Universums zusammen. Wie gesagt wollen wir uns aber lieber auf rein diophantische Fragen beschränken!

Anwendung 1: Die Fermatsche Tripelgleichung.

Eine hübsche Anwendung des Mazurschen Satzes über Torsionspunkte auf elliptischen Kurven ist eine Aussage über die sogenannte Fermatsche Tripelgleichung

$$1+Ax=\square,\quad 1+Bx=\square,\quad 1+Cx=\square \qquad (\square = \textit{rationale Quadratzahlen}),$$

wobei A,B,C gegebene, voneinander und von Null verschiedene rationale Zahlen bezeichnen:

Theorem. Die Tripelgleichung hat stets unendlich viele rationale Lösungen, außer wenn A, B, C (eventuell nach Vertauschung) *einer der folgenden vier algebraischen Gleichungen genügen:*

$$(i)\quad \sqrt{\frac{A}{C}}+\sqrt{\frac{B}{C}}=1, \qquad (ii)\quad \frac{A}{C}+\frac{B}{C}=1,$$

$$(iii)\quad \sqrt{\frac{C-A}{C}}+\sqrt{\frac{C-B}{C}}=1, \qquad (iv)\quad \left(1+\sqrt{\frac{C-B}{A}}\right)\left(1+\sqrt{\frac{C-A}{B}}\right)=2.$$

(Bemerkung. Die Umkehrung des Satzes gilt nicht: auch wenn A,B,C einer der vier

Gleichungen (*i*)-(*iv*) genügen, kann es vorkommen, daß die Tripelgleichung unendlich viele Lösungen besitzt; so z.B. bei $(A,B,C) = (5,16,21)$ oder $(9,25,64)$.)

Um das Theorem zu erhalten, betrachtet man die durch $y^2 = (Ax+1)(Bx+1)(Cx+1)$ gegebene elliptische Kurve E und den rationale Punkt $P = (0,1)$ auf E. Man verifiziert direkt, daß dann jeder Punkt der Gestalt $P+2Q$ ($Q \in E(\mathbb{Q})$ beliebig) eine x-Koordinate hat, die die Fermatsche Tripelgleichung erfüllt. Insbesondere bekommt man unendliche viele Lösungen, falls P unendliche Ordnung hat, nämlich die x-Koordinaten von $3P$, $5P$, $7P$, ... Da $E(\mathbb{Q})$ aber mindestens die drei 2-Torsionspunkte $(-\frac{1}{A},0)$, $(-\frac{1}{B},0)$, $(-\frac{1}{C},0)$ besitzt, kann nach dem Mazurschen Satz die Ordnung eines weiteren Torsionspunkts auf E nur 3, 4, 6 oder 8 sein. Diese vier Fälle entsprechen genau den vier im Satz angegebenen speziellen Gestalten des Ausgangtripels (A,B,C). Übrigens hatte schon Fermat die generische Lösung $3P$ entdeckt und bemerkt, daß diese nicht mehr existiert, wenn $A+B=C$.

Anwendung 2: Teillösung des Sylvesterschen Problems.

Eine alte und naheliegende Aufgabe der diophantischen Analyse besteht darin, zu entscheiden, ob eine gegebene Zahl n als Summe zweier Kubikzahlen dargestellt werden kann. Dieses Problem ist deswegen schwierig, weil man keine a priori Abschätzung für die Größe der dabei auftretenden Zähler und Nenner hat: z.B. ist $n=13$ ganz einfach als $\frac{343}{27}+\frac{8}{27}$ darstellbar, während die Darstellung von $n=382$ Zahlen von fast 50 Dezimalstellen involviert. Im 19ten Jahrhundert hat **J.J. Sylvester** vermutet, daß n stets darstellbar ist, falls n prim und $n \equiv 4 \pmod 9$. Diese Behauptung, die aus der Birch-Swinnerton-Dyer-Vermutung folgen würde, ist noch unbewiesen, aber **Ph. Satgé** konnte 1986 einen ganz ähnlichen Satz beweisen:

Theorem. Falls $n/2$ *prim und* $n \equiv 4 \pmod 9$, *so ist* n *als* x^3+y^3 $(x,y \in \mathbb{Q})$ *darstellbar.*

Zum Beispiel ist $22 = \left(\frac{17299}{9954}\right)^3 + \left(\frac{25469}{9954}\right)^3$. Der Beweis des Theorems beruht auf der Theorie der Modulformen und der Heegner-Punkte: man weiß, daß die elliptische Kurve $X^3+Y^3=2p$ eine Parametrisierung durch Modulformen $X=\xi(\tau)$, $Y=\eta(\tau)$ zuläßt und daß für geeignete quadratische Irrationalitäten τ die Werte dieser Modulformen Zahlen in einem bestimmten algebraischen Zahlkörper ("Ringklassenkörper vom Führer p zu $\mathbb{Q}(\sqrt{-3})$") sind; Satgé konnte beweisen, daß man eine nichttriviale rationale Lösung erhält, indem man diese algebraischen Lösungen im Sinne des Additionsgesetzes der Kurve aufsummiert.

Anwendung 3: Bedingte Lösung des Problems der kongruenten Zahlen.

Wenn die Vermutung von Birch und Swinnerton-Dyer wahr ist, haben wir die folgende elementare und überraschende Antwort auf die Frage, wann eine vorgegebene Zahl n kongruent ist. Sei n positiv und quadratfrei (o.B.d.A., da mit n auch $\pm k^2 n$ für jedes $k \in \mathbb{Q}$ kongruent ist). Ist n ungerade, so definieren wir $A_+(n)$ (bzw. $A_-(n)$) als die Anzahl der Tripel $(x,y,z) \in \mathbb{Z}^3$ mit $x^2+2y^2+8z^2=n$ und z gerade (bzw. ungerade). Ist n gerade, so definieren wir $A_\pm(n)$ genauso, aber mit $2x^2+2y^2+16z^2$ statt $x^2+2y^2+8z^2$. Dann gilt:

Theorem (unter Annahme der BSD-Vermutung). Die Zahl n *ist genau dann kongruent, wenn* $A_+(n) = A_-(n)$.

Hierbei ist die Richtung "⇒" eine Konsequenz des Satzes von Coates und Wiles; die BSD-Vermutung braucht man nur für die Umkehrung. Diese schöne Anwendung der Theorie der elliptischen Kurven wurde von J. Tunnell 1985 bemerkt. Sie geht wie folgt. Wir haben oben schon gesehen, daß die Zahl n genau dann kongruent ist, wenn die elliptische Kurve $E_n : y^2 = x^3 - n^2 x$ eine nichttriviale Lösung hat. Nach der BSD-Vermutung ist dies genau dann der Fall, wenn $L(E_n,1)=0$, wobei die Richtung "$L(E_n,1) \neq 0 \Rightarrow n$ nicht kongruent" schon aus dem Satz von Coates-Wiles folgt, da E_n eine CM-Kurve ist. Ein Satz von **Waldspurger** (1984) liefert aber für jede modulare elliptische Kurve E eine Formel für $L(E,1)$ als im wesentlichen das Quadrat eines Fourier-Koeffizienten einer bestimmten Modulform. In unserem Falle ist dieser Koeffizient gleich $A_+(n) - A_-(n)$, und die Behauptung folgt.

Auch ohne Vermutung kann man häufig entscheiden, ob eine Zahl kongruent ist. Ist $A_+(n) \neq A_-(n)$, so ist nach dem oben gesagten n nicht kongruent. Ist dagegen $A_+(n) = A_-(n)$ (also $L(E_n,1)=0$), aber die Ableitung $L'(E_n,1) \neq 0$—was man ja numerisch nachprüfen kann—so ist n nach dem Satz von Gross-Zagier kongruent. Für die übrigen n findet man in der Praxis einen Punkt auf E_n mit verhältnismäßig kleinen Koordinaten, da nach der BSD-Vermutung der Rang von E_n in diesen Fällen mindestens 2 ist. Auf diese Weise hat man die Kongruenz oder Nichtkongruenz von allen Zahlen bis 2000 in relativ kurzer Rechenzeit bestimmen können, während früher jede einzelne Zahl n eine schwierige Aufgabe darstellte.

Anwendung 4: Lösung des Klassenzahlproblems von Gauß.

In den *Disquisitiones Arithmeticae* von Gauß wird jeder negativen Zahl d eine Zahl $h(d)$, die Klassenzahl von d, zugeordnet. Diese Zahl mißt die Abweichung von eindeutiger Primzahlzerlegung in dem imaginärquadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$. Sie läßt sich auch elementar interpretieren, indem man sagt, daß die Dichte der Primzahlen, die durch eine quadratische Form der Diskriminante d darstellbar sind, $\frac{1}{2h(d)}$ beträgt. Gauß

stellte die berühmte Vermutung auf, daß die Klassenzahl zusammen mit $|d|$ nach Unendlich strebt, eine Behauptung, die 1934 von **Heilbronn** (nach Vorarbeiten von **Deuring** und **Mordell**) bewiesen wurde. Der Beweis war aber *ineffektiv*: das heißt, er gab nicht einmal im Prinzip die Möglichkeit, die Liste aller Zahlen d mit einem gegebenen Wert der Klassenzahl $h(d)$ zu bestimmen. Die Spezialfälle $h(d)=1 \Rightarrow |d| \leq 163$, $h(d)=2 \Rightarrow |d| \leq 427$ wurden durch Arbeiten von **Heegner** (1952), **Baker** (1969) und **Stark** (1969) bewiesen, aber der allgemeine Fall blieb offen. Im Jahre 1975 bewies **D. Goldfeld** durch ein ingeniöses analytisches Argument eine effektive untere Abschätzung für $h(d)$, die mit $|d|$ nach Unendlich strebt. Er brauchte aber hierfür die Existenz einer elliptischen Kurve, deren L-Reihe bei $s=1$ eine Nullstelle mindestens dritter Ordnung hat (und noch eine weitere Eigenschaft besitzt). Erst 1983 konnte man mit Hilfe des Satzes von Gross-Zagier beweisen, daß etwa die elliptische Kurve $-139y^2=x^3+10x^2-20x+8$ die erforderlichen Eigenschaften besitzt: einerseits ist diese Kurve modular und hat einen ungeraden analytischen Rang r', andererseits verschwindet der Heegner-Punkt, der nach dem Satz unendliche Ordnung haben müßte, wenn r' gleich 1 wäre; also ist $r' \geq 3$. Somit haben die elliptischen Kurven den letzten Schritt zur Lösung eines klassischen zahlentheoretischen Problems beitragen können.

Der Spezialfall "$h(d)=4 \Rightarrow |d| \leq 1555$" hat übrigens eine schöne Anwendung, die von **E. Grosswald** bemerkt wurde:

Theorem. Die einzigen Zahlen, die eine eindeutige Darstellung als Summe dreier Quadratzahlen zulassen, 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 *und die Produkte von diesen Zahlen mit Potenzen von* 4.

Die Beziehung zwischen den beiden Fragestellungen rührt von dem Satz von **Gauß-Hermite** her, welcher die Anzahl der Darstellungen einer beliebigen natürlichen Zahl in Termen von Klassenzahlen ausdrückt.

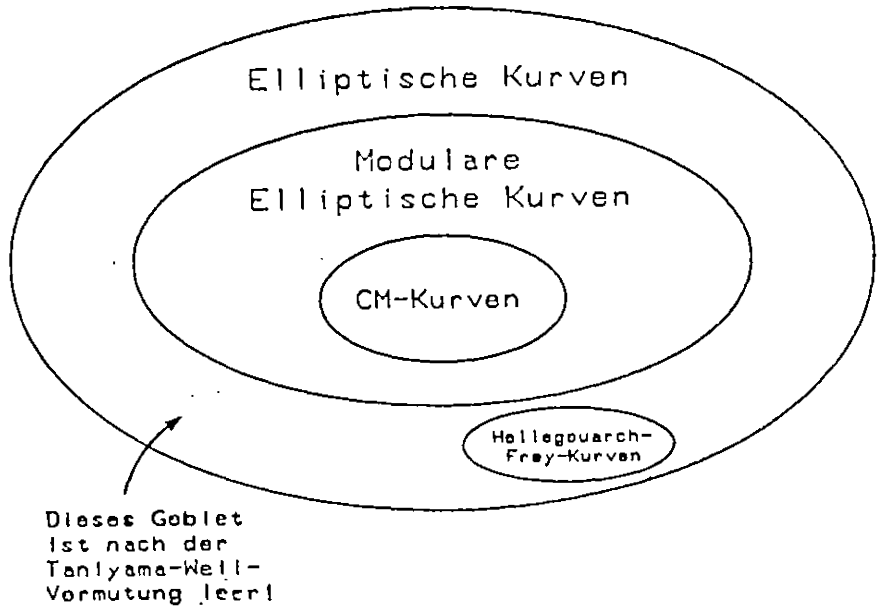
Anwendung 5: Bedingter Beweis des großen Theorems von Fermat.

Wie wir gesehen haben, ist die Taniyama-Weil-Vermutung, daß jede elliptische Kurve über $\mathbb{Q}$ modular ist, eine Aussage, die auf einigermaßen überzeugender theoretischer und numerischer Evidenz basiert. 1986 bewies **K. Ribet**:

Theorem. Gilt die Vermutung von Taniyama-Weil, so gilt auch der "letzte Satz von Fermat": es gibt keine natürlichen Zahlen A, B, C *und* $n>2$ *mit* $A^n+B^n=C^n$.

Um dieses überraschende Resultat zu erhalten, nimmt man an, es gäbe solche Zahlen, und betrachtet die spezielle elliptische Kurve $E_F: y^2=x(x-A^n)(x-C^n)$, die für einen anderen Zweck von **Y. Hellegouarch** und in diesem Zusammenhang von **G. Frey** eingeführt wurde. Ribet konnte einen Teil einer Vermutung von **J-P. Serre** beweisen,

wonach jede modulare elliptische Kurve eine bestimmte Eigenschaft haben muß, die die Kurve E_F nachweislich nicht besitzt. Somit wäre die Kurve E_F ein Gegenbeispiel zu der Vermutung von Taniyama und Weil. Wir können die Situation mit Hilfe unseres Venn-Diagramms auf folgende Weise veranschaulichen:



Literatur

Für den Leser, der näheres zu den hier angeschnittenen Themen erfahren möchte, gebe ich einige Hinweise auf die Literatur. Außerdem werden die Arbeiten angegeben, deren Ergebnisse im Text vorkommen, auch wenn ihr Niveau weit über das dieser Einführung hinausgeht.

Zu §1: Die Lehrbücher von J. Silverman (*The Arithmetic of Elliptic Curves*, Graduate Texts in Math. 106, Springer, 1985), D. Husemöller (*Elliptic Curves*, Graduate Texts in Math. 111, Springer, 1987) und J. Chahal (*Topics in Number Theory*, Univ. Series in Math., Plenum, 1988) sind alle drei als allgemeine Einführung in die Theorie der elliptischen Kurven sehr zu empfehlen. Über die Beiträge von Diophant kann man in dem schönen Büchlein *Diophant und diophantische Gleichungen* von I.G. Bashmakova (DVW, 1974) oder in B.L. van der Waerden, *Geometry and Algebra in Ancient Civilizations* (Springer,1983) lesen. Zu der Geschichte spezieller diophantischer Gleichungen vor 1920 siehe Band II von L.E. Dickson, *History of the Theory of Numbers* (Stechert, 1934, und Chelsea, 1952); z.B. enthält Dickson viel

Auskunft über die Werke von Fermat und Diophant und einen ganzen Abschnitt über das Problem der kongruenten Zahlen.

Mazurs Satz über die möglichen Torsionsgruppen von Mordell-Weil-Gruppen über $\mathbb{Q}$ wird in seinen (sehr schwierigen) Arbeiten "Modular curves and the Eisenstein ideal," IHES Publ. Math. 47 (1977), 33-186, und "Rational points on modular curves," *Modular Functions of One Variable V*, Lecture Notes in Math. **601** (1977), 107-148, bewiesen. Ein Beispiel einer elliptischen Kurve mit Rang (mindestens, und nach der BSD-Vermutung genau) 14 wird in J.-F. Mestre, "Formules explicites et minorations de conducteurs de variétés algébriques," Compositio Mathematica 58 (1986), 209–232, vorgestellt. Die Rechnungen zum Rang der Kurven $x^3+y^3=m$ befinden sich in D. Zagier and G. Kramarz, "Numerical investigations related to the L-series of certain elliptic curves," J. Ind. Math. Soc. 52 (1987), 1-19.

Zu §2: Die—durchgehend schwierigen—Originalarbeiten zu diesem Abschnitt sind wie folgt: J. Silverman, "A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves," J. Reine Angew. Math. 378 (1987), 60–100; N. Elkies, "The existence of infinitely many supersingular primes for any elliptic curve over $\mathbb{Q}$," Invent. Math. 89 (1987), 561–567; J. Coates and A. Wiles, "On the conjecture of Birch and Swinnerton-Dyer," Invent. Math. 39 (1977), 223–251; R. Greenberg, "On the Birch and Swinnerton-Dyer conjecture," Invent. Math. 72 (1983), 241–265; B. Gross and D. Zagier, "Heegner points and derivatives of L-series," Invent. Math. 84 (1986), 225–320; K. Rubin, "Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication," Invent. Math. 89 (1987), 527–560; В.А. Колывагин, Конечность $E(\mathbb{Q})$ и Ш$(E,\mathbb{Q})$ для подкласса кривых Вейля, Изв. Акад. Наук СССР 52 (1988), 522-540. Ein Überblick über einige dieser Ergebnisse, und speziell über die Sätze von Rubin und Kolyvagin, wird von L. Washington in "Number fields and elliptic curves" (erscheint in den Proceedings des NATO Advanced Study Institute, Banff 1988) gegeben. Eine Exposition des Satzes von Kolyvagin gibt K. Rubin in "The work of Kolyvagin on the arithmetic of elliptic curves" (erscheint in *Arithmetic of Complex Manifolds, Erlangen, May* 1988, Springer Lecture Notes in Math.).

Zu §3: Die Anwendung der Theorie der elliptischen Kurven über endlichen Körpern auf die Darstellung einer Primzahl als Summe zweier Quadrate ist in R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," Math. Comp. 44 (1985), 483–494, enthalten. Für die Anwendungen auf Primalitätstests und Faktorisierungsalgorithmen siehe den Übersichtsartikel von H. Lenstra, "Elliptic curves and number-theoretic algorithms," Proc. ICM Berkeley 1986, 99–120.

Zur Fermatschen Tripelgleichung siehe J. Leech, "Four integers whose twelve quotients sum to squares," Can. J. Math. 38 (1986), 1261-1280. Leech macht auch die

Bemerkung, daß es außer in Ausahmefällen immer unendlich viele Lösungen der Fermatschen Tripelgleichung gibt, begründet dies aber unzureichend und ohne den Fall (tv) zu erwähnen.

Der Satz von Ph. Satgé über die Darstellbarkeit von $2p$ als Summe zweier Kubikzahlen ist enthalten in seiner Arbeit "Un analogue du calcul de Heegner," Invent. Math. 87 (1987), 425–439.

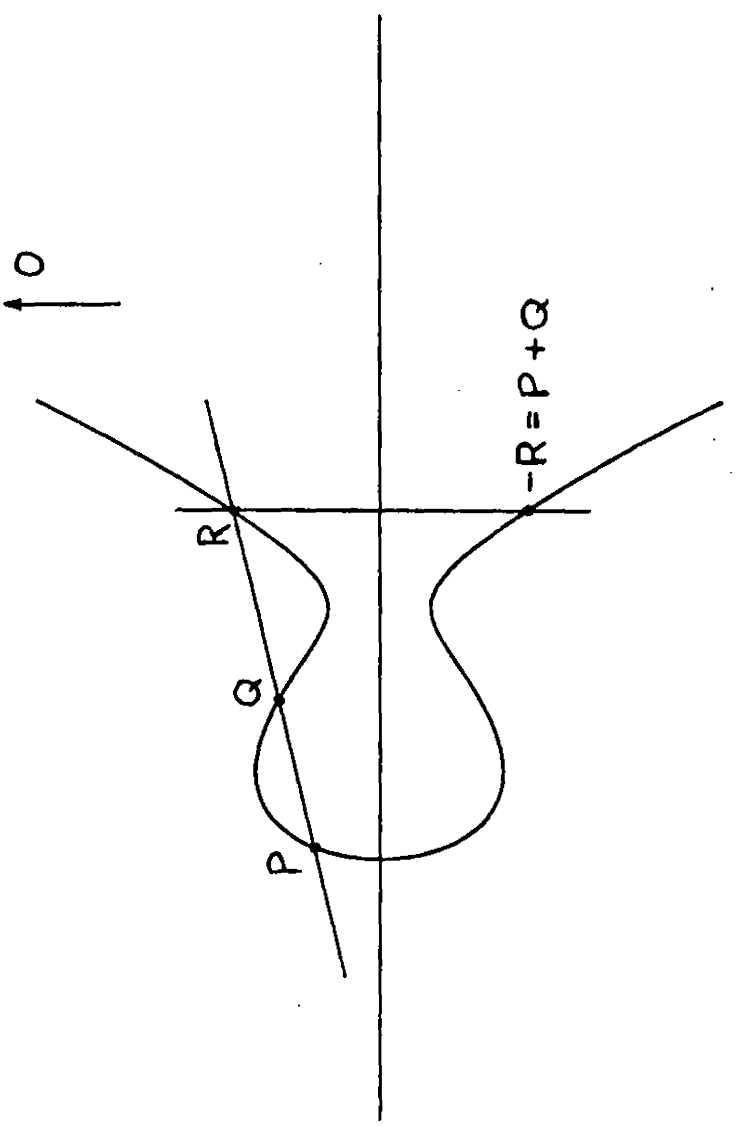
Der Satz von J-L. Waldspurger über Werte von $L(1)$ wird in seiner Arbeit "Sur les coefficients de Fourier des formes modulaires de poids demi-entier," J. Math. Pures Appl. 60 (1981), 375–484 bewiesen. Die Arbeit von J. Tunnell, in der er diesen Satz auf das Problem der kongruenten Zahlen anwendet, ist "A classical Diophantine problem and modular forms of weight 3/2," Invent. Math. 72 (1983), 323–334. Eine Einführung in die Theorie der elliptischen Kurven und Modulformen, die diese Anwendung als Endziel setzt, ist das Buch *Introduction to Elliptic Curves and Modular Forms* von N. Koblitz, Graduate Texts 97, Springer, 1984. Die im Text erwähnten numerischen Rechnungen bis $n=2000$ sind in G. Kramarz, "All congruent numbers less than 2000," Math. Ann. 273 (1986), 337–340 enthalten.

Die ursprüngliche Arbeit von D. Goldfeld zum Klassenzahlproblem ist "The class numbers of quadratic fields and the conjectures of Birch and Swinnerton-Dyer," Ann. Scuola Norm. Sup. Pisa 3 (1976), 623-663. Eine Exposition seiner Methode und der Anwendung des Gross-Zagierschen Satzes gibt J. Oesterlé in "Nombres de classes des corps quadratiques imaginaires," Sém. Bourbaki 1983–1984, Exposé 631, Astérisque 121–122 (1985), 309-323, oder (weniger detailliert und weniger technisch) D. Zagier, "L-series of elliptic curves, the Birch-Swinnerton-Dyer conjecture, and the class number problem of Gauss," Notices A.M.S. 31 (1984), 739–743. Die Bemerkung, daß man mit der Bestimmung aller Diskriminanten mit Klassenzahlen 1, 2 oder 4 auch die Liste aller eindeutig als Summe dreier Quadratzahlen darstellbaren Zahlen kennt, steht bei P.T. Bateman und E.Grosswald, "Positive integers expressible as a sum of three squares in essentially only one way," J. Number Theory 19 (1984) 301-308 und in Grosswalds schönem Buch *Representations of Integers as Sums of Squares* (Springer, 1987). Der Nachweis, daß -1555 die letzte Diskriminante mit der Klassenzahl 4 ist, wurde in der Doktorarbeit "Class Number 4" von S. Arno (Stanford, 1986) erbracht.

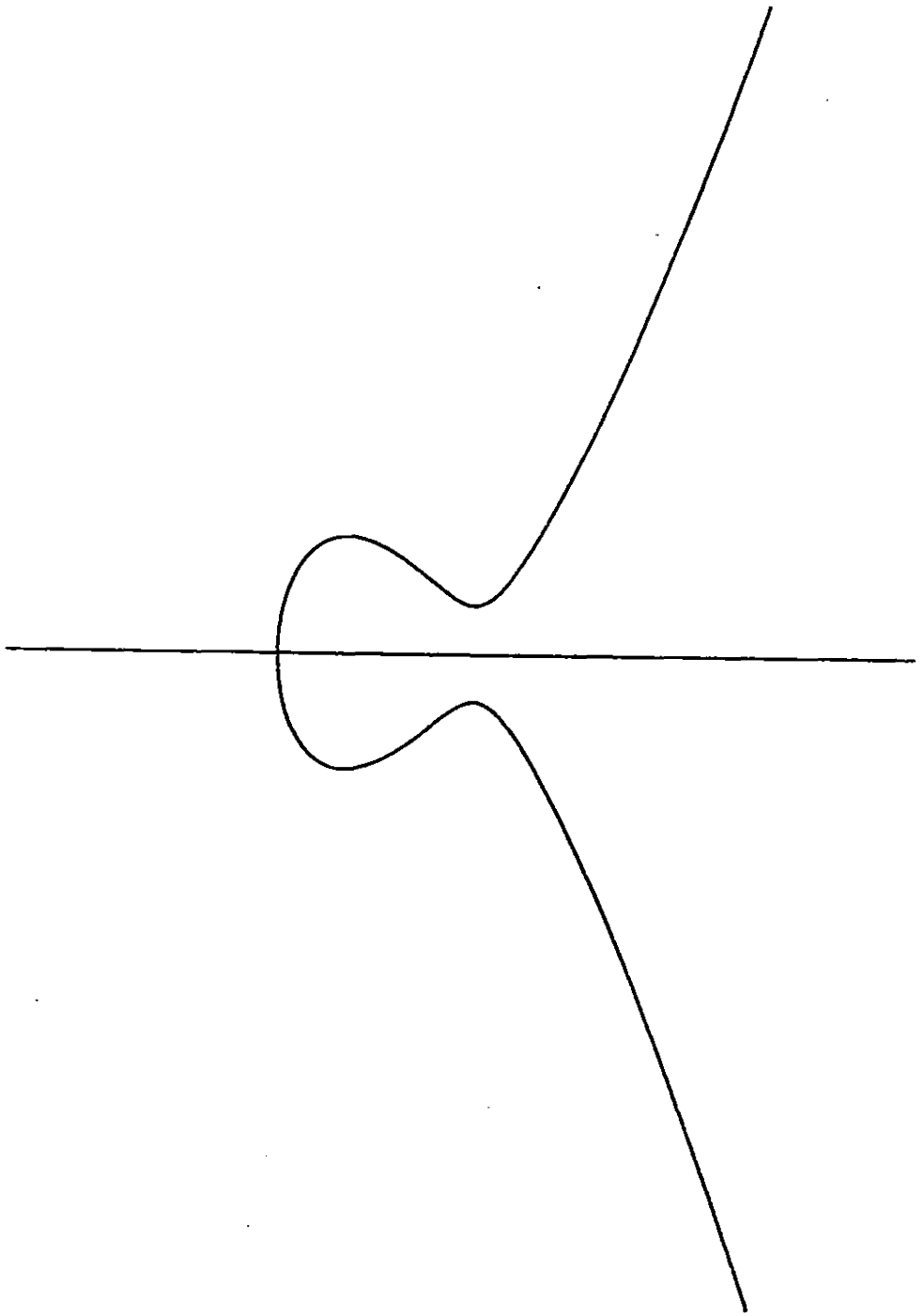
Für die Eigenschaften der Hellegouarch-Frey Kurven und ihre Anwendung auf den letzten Satz von Fermat siehe G. Frey, "Links between stable elliptic curves and certain diophantine equations," Ann. Univ. Saraviensis 1 (1986), 1-40. Der im Text zitierte Satz von Ribet wird in seiner (schweren) Arbeit "On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms" (Preprint, Berkeley, 1988) bewiesen.

S. 4

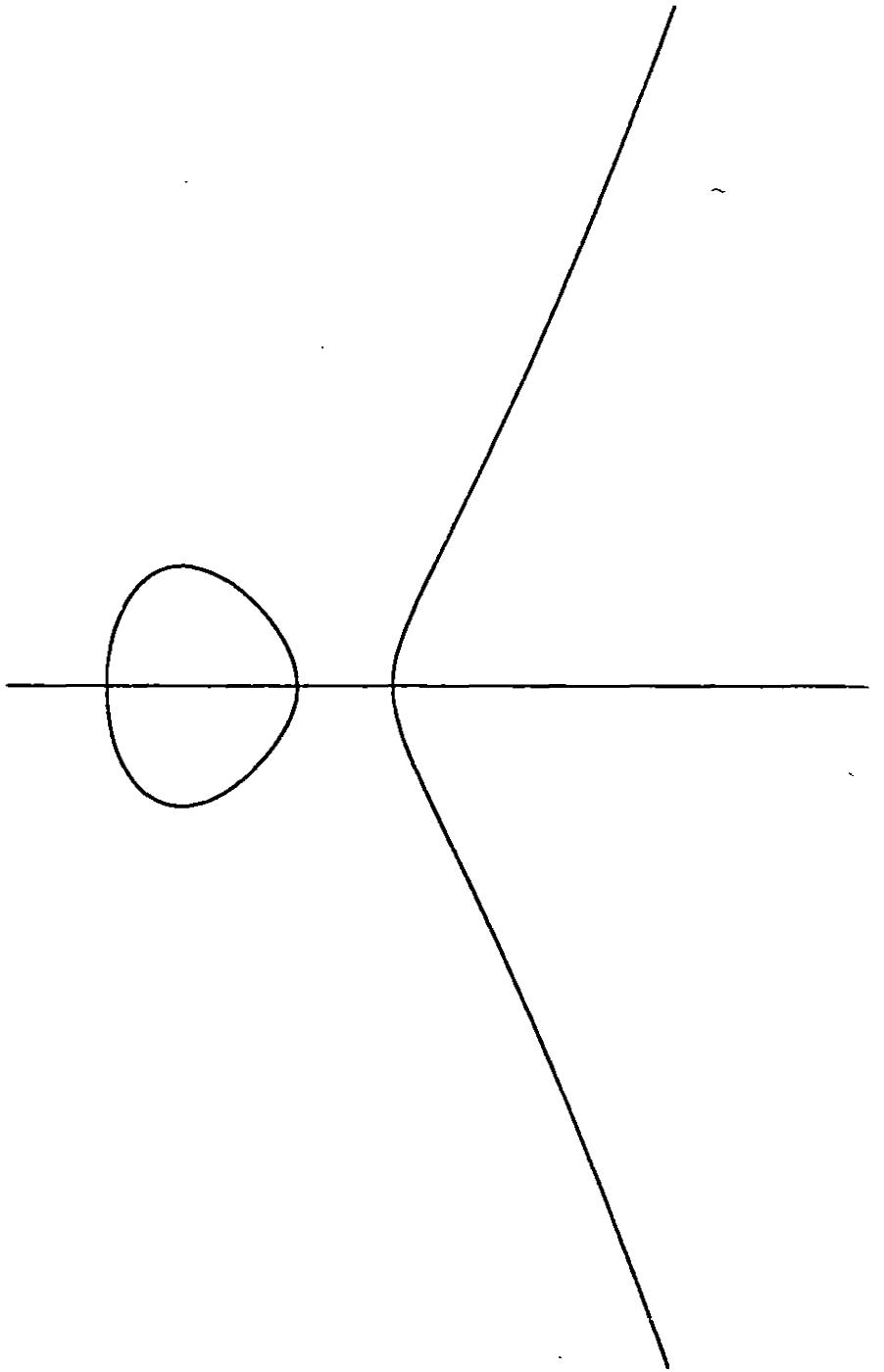
S.5

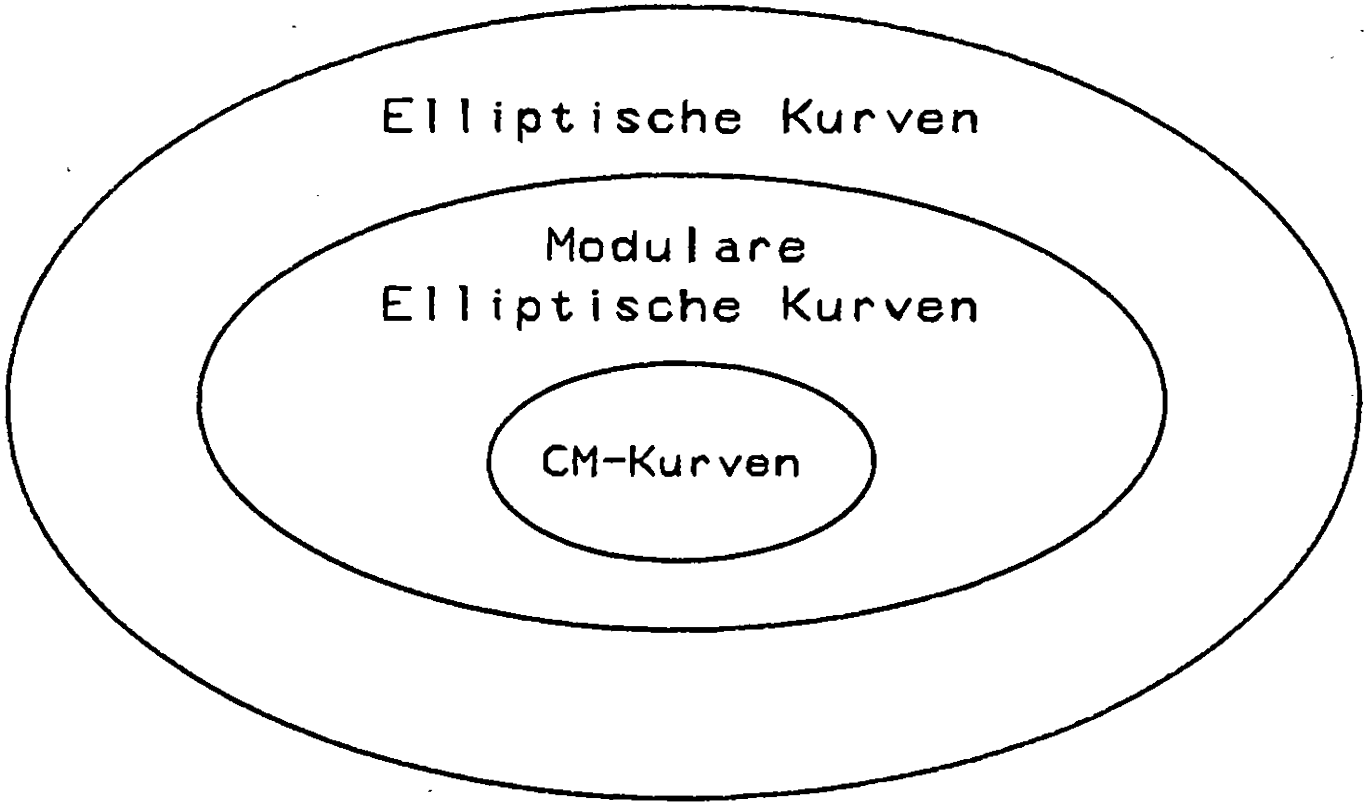


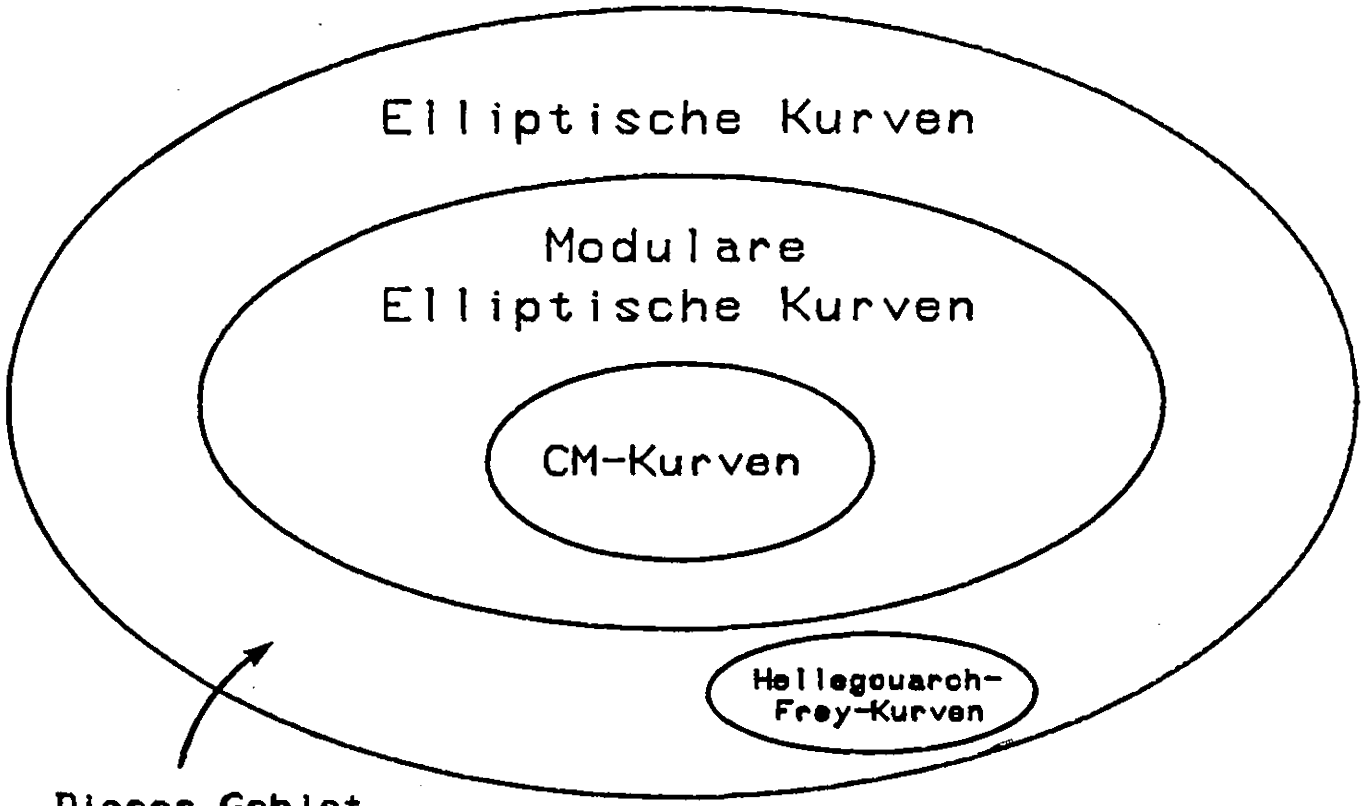
S. 7 links



S. 7 rechts




Elliptische Kurven
Modulare
Elliptische Kurven
CM-Kurven


Elliptische Kurven
Modulare
Elliptische Kurven
CM-Kurven
Hellegouarch-
Frey-Kurven
Dieses Gebiet
ist nach der
Taniyama-Weil-
Vermutung leer!