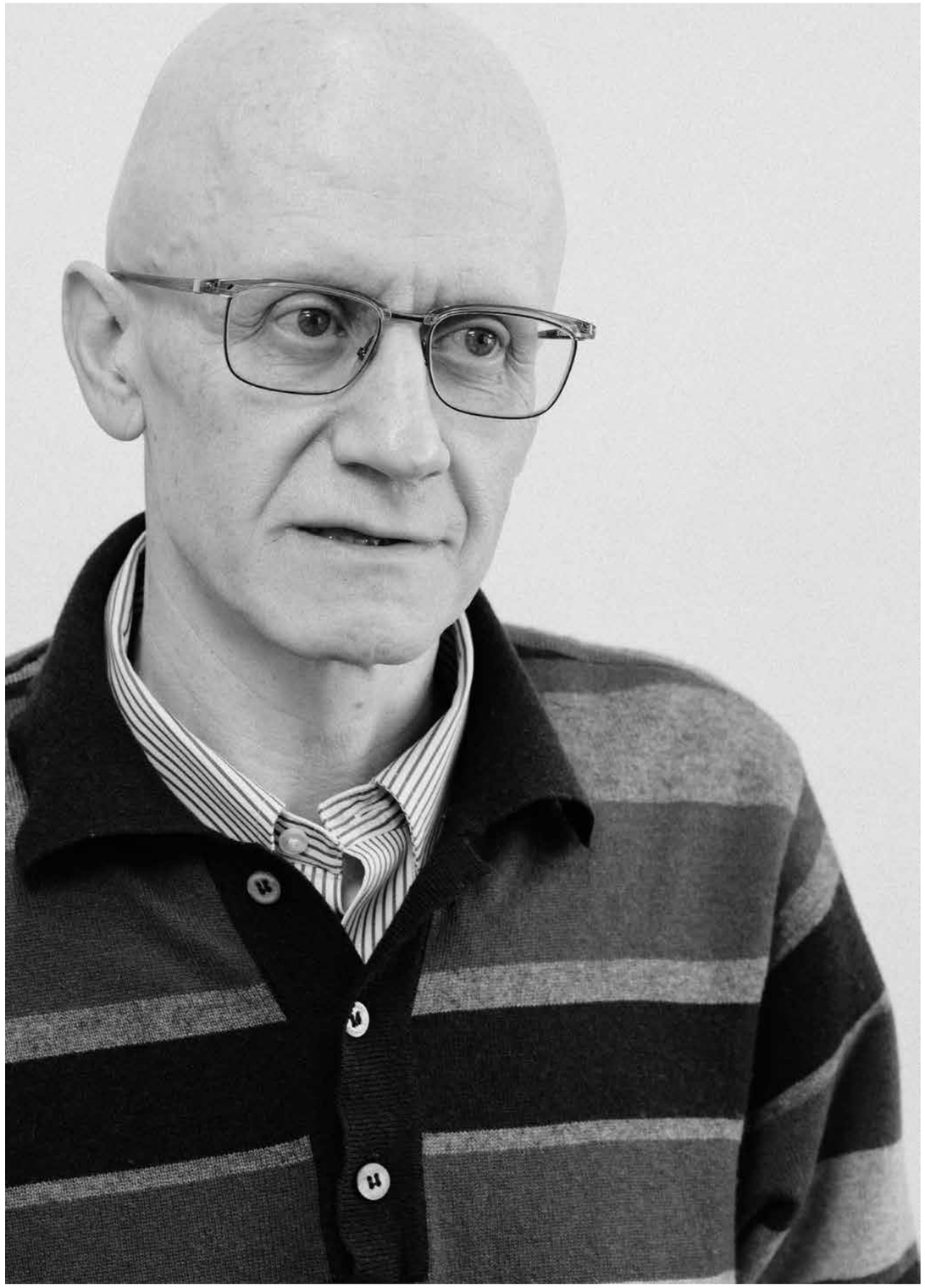


Massimo Bertolini. Foto: Vladimir Unkovic

Zahlentheorie ist ein Gebiet der Mathematik, das sich mit der Lösung von algebraischen Gleichungen mit ganzzahligen Koeffizienten beschäftigt. Sie befasst sich mit einer großen Anzahl von Problemen, die meist scheinbar einfach und elementar sind, aber manchmal sehr schwierig zu lösen.

Kubische Kurven

Von der Antike bis heute

Von Massimo Bertolini

Ein Sonderfall der Polynome mit Koeffizienten in ganzen Zahlen ist das Problem, die Lösungen von kubischen Gleichungen mit zwei Unbekannten in rationalen Zahlen zu finden. Dies ist ein seit langem bestehendes Problem, von dem einige Aspekte auf die alten Griechen zurückgehen und systematisch von den arabischen Mathematiker*innen des 10. Jahrhunderts untersucht wurden. Es entstand sowohl aus praktischen Erwägungen als auch aus reiner intellektueller Neugierde. Als ein Beispiel kann man die Gleichung $y^2=x^3-x$ betrachten. Diese gehört zu einer Klasse von Gleichungen, die aus dem Problem der kongruenten Zahlen hervorgehen, die weiter unten beschrieben werden.

Die **Birch und Swinnerton-Dyer-Vermutung** – im Folgenden abgekürzt **BSD** – ist für das Verständnis der kubischen Gleichungen von grundlegender Bedeutung. Es handelt sich um ein relativ junges Problem im Gebiet der Zahlentheorie, das in den 1960er Jahren formuliert wurde und noch weitgehend offen ist. Es ist eines der sieben **„Millennium Problems“**, die vom Clay Mathe-

matics Institute als eine der Herausforderungen der Mathematik des 21. Jahrhunderts vorgeschlagen wurden (siehe www.claymath.org/millennium-problems).

Bevor wir die BSD vorstellen, werden wir das viel ältere (aber noch immer ungelöste) **Problem der kongruenten Zahlen** beschreiben. Dieses befasst sich mit einer besonderen Klasse von kubischen Gleichungen und ist somit eng mit der BSD verbunden. Es wird das Versuchsgelände darstellen, auf dem wir unser Verständnis (und unsere Unkenntnis!) der BSD testen können.

Kongruente Zahlen

Eine positive ganze Zahl n wird kongruente Zahl genannt, wenn sie sich als Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seitenlängen darstellen lässt. Anders gesagt, es existieren positive rationale Zahlen A, B und C welche die Bedingung $A^2+B^2=C^2$ und AB=2n erfüllen. Wir können und werden im Folgenden immer annehmen, dass n quadratfrei ist, das heißt, dass es nicht durch das Quadrat einer Primzahl teilbar ist.

Das kongruente Zahlenproblem besteht darin, alle kongruenten Zahlen zu finden. Genauer gesagt, es hat das Ziel einen effektiven Algorithmus zu finden, der alle kongruenten Zahlen beschreibt.

Mit einem effektiven Algorithmus meinen wir einen Prozess, durch den man, wenn n wie oben definiert ist, nach einer vorhersehbaren Zeitdauer bestimmen kann, ob n eine kongruente Zahl ist oder nicht.

Eine wohlbekannte Formel für die pythagoreischen Tripel positiver ganzer Zahlen (a,b,c), welche die Bedingung $a^2+b^2=c^2$ erfüllen, führt zu einem nicht effektiven Algorithmus, der letztendlich alle kongruenten Zahlen auflistet. (Die Tatsache, dass eine ganze Zahl n nicht irgendwo in dieser Liste auftaucht, lässt jedoch nicht den Schluss zu, dass n keine kongruente Zahl ist.)

Bemerkungen:
Viele Probleme in der Zahlentheorie haben eine algorithmische Seite. Ein Beispiel ist das Problem, alle Primfaktoren einer ganzen Zahl zu finden. Die algorithmische Schwierigkeit dieses Problems stellt die Grundlage für viele Anwendungen der Zahlentheorie in der Kryptographie dar.

Wir listen einige Beispiele kongruenter Zahlen auf. Tatsächlich beginnen wir mit einem Nicht-Beispiel, indem wir bemerken, dass n=1 keine kongruente Zahl ist. Der Beweis dieser Tatsache folgt aus dem letzten Satz von Fermat für Exponent 4, das heißt die Gleichung $x^4+y^4=z^4$ hat keine Lösungen in ganzen Zahlen, die nicht Null sind.

Die kleinste kongruente Zahl ist n=5, die sich aus den Werten A=3/2, B=20/3 und C=41/6 ergibt.

Außerdem ist n=6 eine kongruente Zahl, da 3,4,5 die Seitenlängen eines rechtwinkligen Dreiecks darstellen.

Man überprüft, dass n=157 eine kongruente Zahl ist: Ein entsprechendes rechtwinkliges Dreieck hat die Seiten

A = 6803298487826435051217540
411340519227716149383203

B = 411340519227716149383203
2166655569371476130 9610

C = 2244035177043369699245575130906748631609484720 41
8912332268928859588025535178967163570016480830

Dieses rechtwinklige Dreieck ist das einfachste zugeordnete rechtwinklige Dreieck in dem Sinn, dass Zähler und Nenner von A,B,C die kleinstmögliche Anzahl von Ziffern haben. Dabei hat der Zähler von C 48 Ziffern!

Bemerkungen:
1. Um das letzte Beispiel zu erzeugen, muss man die Theorie der Heegner-Punkte auf elliptischen Kurven anwenden. Wie später erklärt wird, stellt diese Theorie eines der grundlegenden Werkzeuge dar, die in der modernen Mathematik verwendet werden, um die BSD-Vermutung anzugehen.
2. Mit der Formel für die pythagoreischen Tripel ist es nicht schwer zu zeigen, dass es unendlich viele kongruente Zahlen gibt.

Kongruente Zahlen und kubische Gleichungen

Was ist der Zusammenhang zwischen dem Problem kongruenter Zahlen und der Suche nach Lösungen kubischer Gleichungen?

Wie wir sehen werden, ist n genau dann eine kongruente Zahl, wenn eine bestimmte mit n assoziierte kubische Gleichung eine (nicht-triviale) rationale Lösung hat.

Genauer gesagt, wenn A, B und C (positive) rationale Zahlen sind, welche die Gleichung kongruenter Zahlen erfüllen, setzen wir $a=(C/2)^2$ und $b=(A^2-B^2)C/8$. Man prüft direkt, ob die rationalen Zahlen a und b die Beziehung $b^2=a^3-n^2a$ erfüllen. Anders gesagt, das Paar (a, b) ist eine rationale Lösung der kubischen Gleichung $y^2=x^3-n^2x$, die **elliptische Kurve** genannt wird. Beachten wir, dass b notwendigerweise nicht-null sein muss, da sonst A=B und $C^2/A^2=2$ wäre, was unmöglich ist, da 2 nicht das Quadrat einer rationalen Zahl ist. Umgekehrt kann man beweisen, dass n dann eine kongruente Zahl ist, wenn (a,b) eine Lösung der kubischen Gleichung $y^2=x^3-n^2x$ mit b ungleich null ist.

Wir kommen daher zu der Schlussfolgerung, dass n genau dann eine kongruente Zahl ist wenn die Gleichung $y^2=x^3-n^2x$ eine rationale Lösung mit y ungleich Null hat. (Wenn y gleich Null ist, findet man die „trivialen Lösungen“ (n,0),(-n,0) und (0,0)).

Bemerkung:
Die Menge rationaler Lösungen der elliptischen Kurven – rationale Punkte genannt – kann mit der Struktur einer sogenannten abelschen Gruppe ausgestattet werden. Diese Tatsache kann man nutzen um zu zeigen, dass ein rationaler Punkt (a,b) mit b ungleich Null unendlich viele rationale Lösungen erzeugen kann. Dies ist ein Beispiel für einen Punkt unendlicher Ordnung, während die trivialen Lösungen den Punkten endlicher Ordnung entsprechen.

Aufgrund der obigen Beobachtung kann man das Problem der kongruenten Zahlen neu formulieren, und zwar als das Problem nicht-triviale Lösungen kubischer Gleichungen der Form $y^2=x^3-n^2x$ zu finden. Dabei steht man jedoch vor der Schwierigkeit, dass **kein effektiver Algorithmus** bekannt ist, um zu bestimmen, ob eine elliptische Kurve eine nicht-triviale rationale Lösung hat. Die Existenz eines solchen effektiven Algorithmus ergibt sich aus der BSD-Vermutung, wenn man annimmt, dass diese richtig ist.

Kongruente Zahlen und die BSD

Wir beginnen mit einer vorläufigen Formulierung der BSD-Vermutung. Sie besagt, dass die elliptische Kurve E_n der Gleichung $y^2=x^3-n^2x$ genau dann einen rationalen Punkt mit y ungleich Null hat, wenn ihre L-Reihe im Punkt s=1 verschwindet.

Was ist die L-Reihe der elliptischen Kurve E_n? Es ist die Funktion $L(E_n,s)$ einer Variablen s deren Definition auf der Grundidee beruht, die Lösungen von $E_n: y^2=x^3-n^2x$ modulo p zu zählen, wobei p eine rationale Primzahl ist. Anders gesagt, man sucht nach den Paaren (x,y) in der endlichen Menge $R_p=\{0,1,...,p-1\}$, welche die Reste der Division einer ganzen Zahl durch p sind. Wenn x und y zu R_p gehören, sagt man, dass (x,y) eine Lösung modulo p ist, wenn p die ganze Zahl $y^2-x^3+n^2x$ teilt. Man setzt nun n_p für die Anzahl der Lösungen von En modulo p und ap für die Größe $p-n_p$.

Die **L-Reihe** der elliptischen Kurve E_n ist die Funktion einer komplexen Variablen s, die durch das unendliche Produkt

$$L(E_n,s) = \prod_p (1-a_p p^{-s}+p^{1-2s})^{-1}$$

definiert ist, wobei p über alle Primzahlen verläuft, die 2n nicht teilen.

Bemerkungen:
1. Aufgrund einer Schätzung von Hasse konvergiert das unendliche Produkt, das $L(E_n,s)$ definiert, wenn der Realteil von s größer als 3/2 ist. Darüber hinaus kann nach den Ergebnissen von Hecke, Eichler und Shimura die Funktion $L(E_n,s)$ analytisch in einzigartiger Weise auf alle komplexen Argumente erweitert werden.
2. Die L-Reihe verpackt einfache lokale Daten zu E_n in ein kompliziertes analytisches Objekt, von dem man annimmt, dass es globale Informationen zu E_n enthält. Sie stellt somit eine Art „lokal-globales-Prinzip“ dar.

Ergebnisse zum Problem der konvergenten Zahlen

Wie oben erklärt, können die Ergebnisse aus der BSD-Vermutung für die elliptischen Kurven En auf Ergebnisse zum Problem der kongruenten Zahlen übertragen werden. Wir beginnen mit der Überprüfung einiger Ergebnisse zur BSD.

Das erste Ergebnis wurde von **Coates-Wiles** in den 1970er Jahren erzielt. Es zeigt, dass, wenn E_n einen nicht-trivialen rationalen Punkt hat, $L(E_n,1)$ gleich Null ist.

Die Umkehrung, dass aus dem Verschwinden von $L(E_n,1)$ folgt, dass n eine kongruente Zahl ist, ist jedoch noch weit offen!

Ein anderes wichtiges Ergebnis ist das Theorem von **Tunnell** aus den 1980er Jahren. Es besagt, dass es einen effektiven Algorithmus gibt um zu bestimmen, ob $L(E_n,1)$ gleich Null ist oder nicht.

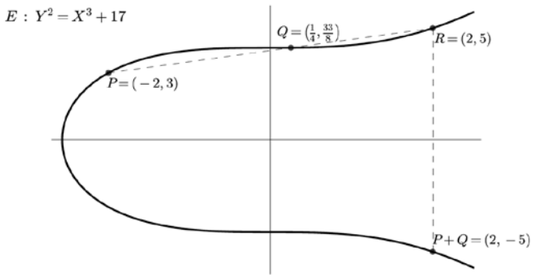
Zum Problem der kongruenten Zahlen können wir folgende Schlüsse ziehen. Erstens zeigt der Satz von Coates-Wiles, dass n keine kongruente Zahl ist, wenn $L(E_n,1)$ nicht Null ist. Zweitens folgt aus der BSD-Vermutung, dass n genau dann eine kongruente Zahl ist, wenn $L(E_n,1)=0$ ist. Aufgrund des Satzes von Tunnell hat man also einen effektiven Algorithmus um zu bestimmen, ob n eine kongruente Zahl ist, wenn man davon ausgeht, dass die BSD-Vermutung richtig ist.

Einige Bemerkungen:
1. Es gibt eine allgemeinere Version der BSD – auf die ich gleich noch eingehen werde – die für alle elliptischen Kurven gilt. Dies sind die kubischen Kurven der Form $E: y^2=x^3+ax+b$, wobei a,b rationale Koeffizienten sind, für welche die Größe $4a^3+27b^2$ nicht-null ist.
2. Wie erwähnt, gilt die BSD als eines der grundlegenden offenen Probleme der reinen Mathematik.
3. Das Problem der kongruenten Zahlen reicht bis in die Antike zurück, ist aber immer noch eine zentrale Frage in der modernen Zahlentheorie. Die „Nachhaltigkeit“ ihrer Fragestellungen ist eine bemerkenswerte Charakteristik der Zahlentheorie, die trotz der gewaltigen technischen Fortschritte, die in der Mathematik über mehrere Jahrhunderte hinweg stattgefunden haben, auch heute Bestand hat. Diese Eigenschaft grenzt die Zahlentheorie von anderen wissenschaftlichen Bereichen ab, in denen viele grundlegende Fragen schon nach wenigen Jahren als überholt gelten.

Grundlagen der elliptischen Kurven

Unter einer elliptischen Kurve versteht man eine ebene Kurve E, die durch eine Gleichung der Form

$y^2=x^3+ax+b$ definiert ist, wobei die Koeffizienten a und b rationale Zahlen sind, bei denen $4a^3+27b^2$ nicht-null ist. Es ist hilfreich, die Menge E(**Q**) rationaler Lösungen der obigen Gleichung zusammen mit dem sogenannten Fernpunkt OE zu betrachten, der erhalten wird, wenn man die Koordinaten x und y nach Unendlich tendieren lässt. (Genauer gesagt, ist O_E der Punkt mit projektiven Koordinaten [0,1,0].)



Eine bemerkenswerte Eigenschaft der Menge E(**Q**) ist, dass sie mit der Struktur einer abelschen (oder kommutativen) Gruppe mit dem Ursprung O_E ausgestattet werden kann, auf Grund der Definition, dass die Summe dreier (nicht notwendigerweise verschiedener) Punkte genau dann O_E ergeben, wenn sie die Schnittpunkte mit einer projektiven Geraden sind.

Ein Satz von Mordell besagt, dass E(**Q**) endlich erzeugt wird, das heißt es gibt eine endliche Menge von Elementen in E(**Q**), so dass alle anderen Elemente in E(**Q**) als Summe der Elemente in dieser endlichen Menge erhalten werden können, wobei Wiederholungen möglich sind. Anders gesagt, E(**Q**) besteht aus einem endlichen Teil – seiner Torsion $E(\mathbf{Q})_t$ – und einem sogenannten freien Teil $E(\mathbf{Q})_f$, der mit r_E Kopien der Gruppe Z der ganzen Zahlen identifiziert werden kann. Die nicht negative ganze Zahl r_E wird als **Rang von E** bezeichnet.

Eine fundamentale Tatsache in dieser Theorie ist, dass kein effektiver Algorithmus zur Bestimmung von E(**Q**) – und insbesondere zur Berechnung seines Rangs r_E – bekannt ist.

Zwei-Schritte-Erklärung

Wir stellen nun eine etwas technische Erklärung der oben genannten Tatsache in zwei Schritten vor. Der*/Die Leser*in kann diesen Absatz auch überspringen und nur die Existenz der **Shafarevich-Tate-Gruppe** zur Kenntnis nehmen, die in unserer nachfolgenden Formulierung der BSD-Vermutung eingeführt wird.

Schritt 1:
Es gibt die kanonische Néron-Tate Höhe
$<,>_{NT}: E(\mathbf{Q}) \times E(\mathbf{Q}) \to \mathbf{R}$. Diese ist eine symmetrische nicht-ausgeartete (modulo Torsion) bilineare Abbildung. Man könnte sagen: $<P,P>_{NT}$ „misst die arithmetische Komplexität des Punktes P in E(**Q**)". Die Existenz der kanonischen Néron-Tate Höhe hat die folgenden Konsequenzen:
(i) wenn für eine ganze Zahl m größer oder gleich zwei die Quotientengruppe E(**Q**)/mE(**Q**) endlich ist, dann wird E(**Q**) endlich erzeugt;
(ii) wenn E(**Q**)/mE(**Q**) effektiv berechenbar ist, dann ist E(**Q**) effektiv berechenbar.

Schritt 2:
Es gibt einen injektiven Gruppenhomomorphismus
δ_m: E(**Q**)/mE(**Q**) → $\mathbf{S}_m(E)$, wobei $\mathbf{S}_m(E)$ die sogenannte m-te Selmer Gruppe von E ist. Dies ist eine abelsche Gruppe, die endlich und berechenbar ist.

Daraus folgt, dass der Cokern von m die Berechenbarkeit von E(**Q**)/mE(**Q**) behindern kann. Er ist mit der m-Torsion $\mathbf{Sha}(E)_m$ der Shafarevich-Tate Gruppe **Sha**(E) von E identifiziert. Um E(**Q**)/mE(**Q**) zu berechnen, müsste man sicher sein, dass **Sha**(E) endlich ist (was zu erwarten, aber nicht für alle Fälle bewiesen ist) und ihre Ordnung ein wenig kennen.

In diesem Falle wäre es möglich m so zu wählen, so dass $\mathbf{Sha}(E)_m$ trivial ist, so dass E(**Q**)/mE(**Q**) mit $\mathbf{S}_m(E)$ identifiziert wird.

Die Birch und Swinnerton-Dyer-Vermutung

Die BSD-Vermutung liefert eine mutmaßliche Antwort auf das grundlegende Problem der effektiven Berechnung von E(**Q**). Sie wurde in den 1960er Jahren von Birch und Swinnerton-Dyer aufgestellt, die eine erste umfangreiche numerische Studie zu elliptischen Kurven durchgeführt haben, mit dem Einsatz von Maschinen, deren Rechenleistung unvergleichlich viel schwächer als die aktuelle war.

Ähnlich wie bei den speziellen elliptischen Kurven En definiert man die L-Reihe einer allgemeinen elliptischen Kurve E der Gleichung $y^2=x^3+ax+b$ durch Zählen der Punkte von E modulo p. Genauer gesagt, sei n_p die Anzahl der Punkte von E modulo p und schreibe a_p für die Größe p-np. Definieren wir die **L-Reihe**

$$L(E,s) = \prod (1-a_p p^{-s}+p^{1-2s})^{-1}$$

wobei p über alle Primzahlen verläuft, die $4a^3+27b^2$ nicht teilen. Dann konvergiert dieses unendliche Produkt für den reellen Teil von s größer als 3/2 und lässt eine analytische Erweiterung auf alle komplexen Argumente zu. Diese letzte Tatsache folgt aus dem grundlegenden **Modularitätssatz** von **Wiles** und Mitarbeitern, die zum

Beweis des berühmten Fermatschen Großen Satzes führten.

Rufen wir den Rang $\mathbf{r}=r_E$ von E zurück. Definieren wir den **analytischen Rang** $\mathbf{t}=t_E$ von E als die Verschwindungsordnung von L(E,s) wenn s=1 ist. Dies bedeutet, dass man in der Nähe von s=1, L(E,s) in der Form $(s-1)^t$ g(s) schreiben kann, wobei g(s) eine Funktion ist, bei der g(1) nicht-null ist. Damit ist es uns möglich, die BSD-Vermutung in einer präziseren Form als zuvor für E_n anzugeben.

Die BSD-Vermutung
1) („das Millennium Problem") $r_E=t_E$.
2) („die genaue Formel") $L^r(E,1)=\mathbf{C}_E\mathbf{R}_E\mathbf{\#Sha}(E)$.

Der erste Teil der BSD, welcher Inhalt des oben erwähnten Millennium-Problems ist, besagt, dass der Rang von E alternativ auch als der analytische Rang von E beschrieben werden kann. Im zweiten Teil bezeichnet $L^r(E,1)$ die r_E-te Ableitung von L(E,s) die am Punkt s=1 ausgewertet wird, und $\mathbf{C}_E$ ist eine explizite Konstante von nachgestellter Wichtigkeit für diese Darstellung. Darüber hinaus ist **#Sha**(E) die Anzahl der Elemente der Shafarevich-Tate-Gruppe (es wird stillschweigend angenommen, dass diese endlich ist, was in einer Vermutungsaussage legitim ist). Schließlich ist $\mathbf{R}_E$ der sogenannte Regulator von E, definiert in Bezug auf die Néron-Tate-Höhe des vorhergehenden Absatzes. Er ist ein Maß für die „Größe" der Gruppe E(**Q**), insbesondere ist er gleich 1, wenn $r_E=0$ ist.
Bemerkungen:
1) Die BSD besagt, dass die Gruppe E(**Q**) der rationalen Punkte von E eng mit einem Objekt analytischer Natur verbunden ist, nämlich der L-Reihe L(E,s). Sie postuliert also die Existenz einer tiefen und mysteriösen Verbindung zwischen Konzepten aus den Gebieten der Algebra und der Analysis. Diese Art von Verbindungen erscheint in verschiedenen wichtigen klassischen Ergebnissen der Zahlentheorie, wie zum Beispiel in den Dirichlet-Formeln zu Klassenzahlen. Sie sind außerdem ein vereinendes Merkmal, das sich in einer Vielzahl von Vermutungen wiederfindet, die BSD erheblich verallgemeinern und ein fruchtbares Forschungsgebiet der modernen Mathematik darstellen.
2) Manin hat gezeigt, dass es, wenn die BSD wahr ist (einschließlich der genauen Formel), einen effektiven Algorithmus gibt, um E(**Q**) zu bestimmen. Man kann daher BSD als eine Vermutungs-Lösung für das fundamentale Problem der Theorie elliptischer Kurven ansehen. Insbesondere zeigt sie eine Möglichkeit auf, um das kongruente Zahlenproblem anzugehen.

Ergebnisse zur BSD

Dieser Abschnitt beschreibt einige der bekannten Ergebnisse von BSD. Es dient als Einführung zu einem Teil der Forschung, mit der sich meine Arbeitsgruppe beschäftigt.

Das erste Ergebnis verbindet Sätze von **Gross-Zagier** und **Kolyvagin** aus den 1980er Jahren. Es besagt, dass Teil 1 von BSD gilt und zudem, dass **Sha**(E) eine endliche Gruppe ist, wenn der analytische Rang t_E entweder Null oder Eins ist.

Daher wissen wir, dass ein großer Teil der BSD gilt, wenn der analytische Rang t_E „klein" ist. Es sollte erwähnt werden, dass dieses Ergebnis für eine bestimmte Klasse elliptischer Kurven, die sogenannten elliptischen Kurven mit komplexer Multiplikation, zu denen die aus dem Problem der kongruenten Zahlen hervorgehenden Kurven En gehören, durch die Sätze von Coates-Wiles (siehe oben) und Rubin bereits bekannt war.

Wie oben erwähnt und im Folgenden näher erläutert, spielt der Modulariätssatz von Wiles für den Nachweis dieses ersten Ergebnisses und der nachfolgend beschriebenen eine entscheidende Rolle. Insbesondere erlaubt er die Definition von expliziten nicht-trivialen Punkten auf elliptischen Kurven, den sogenannten Heegner-Punkten, wenn der analytische Rang klein ist. Das Fehlen einer ähnlichen Konstruktion von Punkten für den Fall, dass der analytische Rang größer als eins ist, stellt eines der Haupthindernisse für das Angehen der BSD im allgemeinen Fall dar.

Das zweite Ergebnis, das wir hier erwähnen, ist eine Art Umkehrung des Satzes von Gross-Zagier-Kolyvagin. Es nimmt an, dass für eine Primzahl p die die Konstante a_p nicht teilt, der Rang r_E höchstens Eins ist und dass die Menge der Elemente von **Sha**(E) der p-Potenzordnung endlich ist. Dann ist r_E gleich dem analytischen Rang t_E und **Sha**(E) ist endlich.

Dieses Ergebnis wurde etwa im Jahr 2010 von **Skinner-Urban** für r_E gleich Null bewiesen. Für r_E gleich eins ist es auf **Skinner** im Jahr 2013 zurückzuführen, dessen Methoden auf früheren Ergebnissen von Xin Wan und Bertolini-Darmon-Prasanna basieren sowie auf dem Satz von Gross-Zagier. Weitere Ansätze stammen von **Wei Zhang, Skinner-W. Zhang und Venerucci** (der Mitglied meiner Forschungsgruppe in Essen ist), unter Verwendung der Sätze von Skinner-Urban und Gross-Zagier und der Arbeit von Bertolini-Darmon. Die Beweise stützen sich auf die **Iwasawa-Theorie**, welche die arithmetischen Eigenschaften von elliptischen Kurven auf bestimmten Sammlungen endlicher Erweiterungen des Körpers **Q** rationaler Zahlen untersucht, wie sie zum Beispiel erhalten werden, wenn man **Q** um die Wurzeln von eins erweitert, deren Ordnung eine Potenz von p ist, wobei p eine feste Primzahl ist.

Die beiden soeben beschriebenen Ergebnisse beziehen sich hauptsächlich auf den ersten Teil der BSD und auf die Endlichkeit von **Sha**(E). Das nächste Ergebnis behandelt den zweiten Teil von BSD, indem es eine exakte Formel für die r_E-te Ableitung von L(E,s) bei s=1

vorhersagt. Nehmen wir wie beim ersten Ergebnis an, dass der analytische Rang t_E entweder Null oder Eins ist. Dann gilt Teil 2 von BSD bei p für alle Primzahlen p, die a_p nicht teilen, deren Anzahl jedoch endlich ist. Genauer gesagt heißt das, dass die exakte Potenz von p, die **#Sha**(E) teilt, mit derjenigen identisch ist, welche die Menge $L^r(E,1)/\mathbf{C}_E\mathbf{R}_E$ teilt.

Für t_E gleich Null folgt dies aus dem oben erwähnten Satz von **Skinner-Urban**. Für t_E gleich Eins wurde dies in zwei unabhängigen Arbeiten von **Wei Zhang** und von **Berti-Bertolini-Venerucci** um 2013 unter Verwendung des Ergebnisses von Skinner-Urban und des Werks von Bertolini-Darmon bewiesen.

Das letzte Ergebnis, das wir erwähnen möchten, betrifft BSD aus „statistischer Sicht". Es besagt, dass die BSD für einen positiven Anteil elliptischer Kurven gilt, wenn man diese in Bezug auf die Größe der Koeffizienten a und b zählt, die in ihren Gleichungen erscheinen.

Dieses Ergebnis wurde von **Bhargava-Shankar, Bhargava-Skinner, Barghava-Skinner-Wei Zhang** nach 2013 bewiesen. Die Verleihung der Fields-Medaille (dem „Nobelpreis der Mathematiker*innen") an Bhargava auf dem Internationalen Kongress der Mathematiker*innen im Jahr 2014 ist teilweise auf diese Arbeit zurückzuführen.

Die Beweisstrategie besteht darin, elliptische Kurven zu zählen, deren p-te Selmer-Gruppe $\mathbf{S}_p(E)$ entweder Null ist oder eine zyklische Gruppe der Ordnung p, wenn p eine kleine Primzahl ist (höchstens 5). Sie ruft dann eine Spielart des ersten und zweiten Ergebnisses auf, die oben beschrieben wurden.

Es wird erwartet, dass für 100 Prozent der elliptischen Kurven die Selmer-Gruppe $\mathbf{S}_p(E)$ entweder Null ist oder aber zyklisch in der Ordnung p, wenn p unbeschränkt ist. Selbst wenn man unser letztes Ergebnis (die BSD aus statistischer Sicht betreffend) für 100 Prozent der elliptischen Kurven zeigen könnte, würde dies die BSD nicht beweisen! Mit anderen Worten, die mysteriösen Fälle von elliptischen Kurven mit Rang größer Eins, für welche die Methoden, die zu den obigen Ergebnissen führten, nicht anwendbar sind, sind statistisch vernachlässigbar.

Einige zusätzliche Überlegungen

1) Um das Problem der kongruenten Zahlen zu lösen, müsste man eine Umkehrung des Satzes von Coates-Wiles aufstellen. Dies wäre ein Spezialfall einer stärkeren Version des obigen zweiten Satzes, in dem die Endlichkeitsbedingung für den p-Teil von **Sha**(E) nicht vorhanden ist. Die Endlichkeit von **Sha**(E) bleibt ein fundamentales offenes Problem in der Theorie elliptischer Kurven.
2) Die BSD ist immer noch weit offen, wenn der Rang größer als Eins ist, und neue Ideen werden hier benötigt. Zum Beispiel ist kein Beispiel einer elliptischen Kurve, für die t_E größer als 3 ist, bekannt, obwohl Beispiele, bei denen r_E mindestens 28 ist, von Elkies konstruiert wurden.
3) Die Tatsache, dass elliptische Kurven Modulformen zugeordnet sind, spielt für alle oben erwähnten Ergebnisse eine grundlegende Rolle. Sie ermöglicht es, die L-Reihe analytisch zu erweitern und somit ihre Ableitung bei s=1 zu betrachten. Dies führt insbesondere zur Formel von Gross-Zagier, die $L^1(E,1)$ mit Hilfe von Heegner-Punkten beschreibt, die durch die Theorie der komplexen Multiplikation definiert sind.
4) Die vorhergehenden Sätze verbinden analytische Techniken mit algebraischen, ausgehend von der Idee der Deformation von Modulformen und Kohomologie-Klassen: die sogenannte **Theorie der Euler-Systeme**.

Elliptische Kurven und Modulformen

Wie wir gesehen haben, postuliert BSD die Existenz einer tiefen Beziehung zwischen kubischen Gleichungen und ihren zugehörigen L-Funktionen. Eine Verbindung dieser algebraischen und analytischen Objekte wird durch den Modularitätssatz von Wiles hergestellt, der besagt, dass jede elliptische Kurve einer spezifischen modularen Form entspricht.

Um diese Verbindung zu erklären, kehren wir zur L-Funktion L(E,s) einer elliptischen Kurve zurück. Durch die Erweiterung des unendlichen Produkts, das L(E s) definiert, erhält man eine Reihe $\sum_n a_n n^{-s}$, wobei die Summe über die positiven ganzen Zahlen genommen wird und die Koeffizienten a_n mit den Größen $a_p=p-n_p$ übereinstimmen, wenn n=p eine Primzahl ist.

Setzen wir nun $q=\exp(2\pi iz)$, wobei z ein Argument ist, das zur komplexen oberen Halbebene **H** gehört, die aus den komplexen Zahlen z=x+iy besteht, deren imaginärer Teil y positiv ist. Dann ergibt L(E,s) die q-Reihe $f_E(z)= \sum_n a_n q^n$, deren Eigenschaften Gegenstand des Modularitätssatzes sind.

Der **Modularitätssatz**, früher bekannt als **Shimura-Taniyama-Vermutung**, besagt, dass $f_E(z)$ eine **Modulform** des Gewichts 2 und der Stufe N_E ist. Dabei ist N_E eine positive ganze Zahl, die auch Führer von E genannt wird, in Termen der Gleichung von E berechnet werden kann und eng mit der Diskriminante $4a^3+27b^2$ verwandt ist. Dies bedeutet, dass die q-Reihe, die $f_E(z)$ definiert, gegen eine analytische Funktion auf **H** konvergiert, das heißt differenzierbar ist (sie liefert ihre Fourier-Erweiterung). Außerdem erfüllt f_E die Funktionsgleichungen $f_E((\alpha z+\beta)/(\gamma z+\delta)=(\gamma z+\delta)^2 f_E(z)$ für alle ganzen Zahlen $\alpha,\beta,\gamma,\delta$ so dass $\alpha\delta-\beta\gamma$ gleich 1 ist und N_E γ teilt. Weitere, hier nicht aufgeführte Eigenschaften von f_E sind, dass f_E spezifische Wachstumsbedingungen erfüllt („es verschwindet an den Spitzen") und eine Eigenfunktion für die Hecke-Operatoren ist.

Dieser Satz wurde in den 1990er Jahren von **Wiles** und **Taylor-Wiles** für die Klasse der elliptischen Kurven bewiesen, deren Führer N_E nicht durch Quadrate von Primzahlen teilbar ist (die sogenannten semistabilen elliptischen Kurven). Kurz darauf wurde es von **Breuil-Conrad-Diamond-Taylor** auf alle elliptischen Kurven erweitert. Eine Beschreibung der Beweisstrategie geht über den Rahmen dieses Textes hinaus. Wir beleuchten hier stattdessen einige seiner Konsequenzen.

Wie bereits erwähnt, zeigt eine Schätzung von Hasse bezüglich der Anzahl der Punkte modulo einer Primzahl einer elliptischen Kurve, dass das unendliche Produkt, das L(E,s) definiert, zu einer analytischen Funktion auf der Menge komplexer Zahlen konvergiert, deren realer Anteil größer als 3/2 ist. Um seinen Wert am Punkt s=1 zu berücksichtigen wie in der BSD-Anweisung gefordert, muss man L(E,s) auf eine analytische Funktion um s=1 erweitern. Aus der Tatsache, dass f_E eine modulare Form ist, folgt direkt, dass L(E,s) tatsächlich auf eine analytische Funktion erweitert werden kann, die über die gesamte komplexe Ebene definiert ist. Zusammenfassend ist der Modularitätssatz das Werkzeug, welches die Untersuchung der analytischen Eigenschaften der L-Funktionen elliptischer Kurven möglich macht. Dieses Werkzeug war in den 1960er Jahren noch nicht verfügbar, als Birch und Swinnerton-Dyer die gleichnamige Vermutung formulierten. Wie John Tate hervorhob, ergab diese Vermutung eine Beziehung zwischen dem Wert einer Funktion (der L-Funktion) an einem Punkt an dem sie nicht definiert war, und der Anzahl der Elemente einer Gruppe (der Shafarevich-Tate-Gruppe) von der nicht bekannt war, ob sie endlich ist!

Die algebraische Seite von BSD beinhaltet das Studium der Gruppe E(Q) rationaler Punkte. Der Modularitätssatz kann in bestimmten Fällen verwendet werden, um Elemente in E(Q) zu konstruieren. In der Tat erhält man durch Integration des Differentials $f_E(z)$ dz auf der komplexen oberen Halbebene eine Funktion

ϕ_E: **H** → E(**C**), wobei E(**C**) die Menge der komplexen Punkte von E bezeichnet, d.h. die Menge von Lösungen der Gleichung $y^2=x^3+ax+b$, die zum Körper **C** der komplexen Zahlen gehören. Die aus dem „Kronecker Jugendtraum" hervorgegangene und unter anderem von David Hilbert entwickelte **Theorie der Komplexen Multiplikation** zeigt folgende bemerkenswerte Eigenschaft der obigen Abbildung auf. Wenn z ein Element von **H** der Form $c+d\sqrt{(-D)}$ ist, wobei c,d rationale Zahlen sind und -D eine negative ganze Zahl ist, dann sind die Koordinaten des Punktes $f_E(z)$ in E(**C**) nicht einfach komplexe Zahlen, sondern tatsächlich algebraische Zahlen (d.h. Lösungen einer algebraischen Gleichung) eines bestimmten Typs. Geeignete Kombinationen dieser Punkte, die sogenannten **Heegner-Punkte**, können verwendet werden, um rationale Punkte in E(**Q**) zu definieren.

Heegner-Punkte spielen eine wesentliche Rolle im oben erwähnten Satz von Gross-Zagier-Kolyvagin, der das bis heute beste Ergebnis zur BSD liefert. Tatsächlich verbindet die Gross-Zagier-Formel die erste Ableitung $L^1(E,1)$ der L-Funktion von E mit einem Heegner-Punkt. Kolyvagins Methode zeigt dann, dass dieser Heegner-Punkt im Wesentlichen E(**Q**) erzeugt, so dass r_E genau dann gleich 1 ist wenn $L^1(E,1)$ nicht Null ist, d.h. der analytische Rang t_E ist gleich 1.

Eine Variante der Heegner-Punkt-Konstruktion wurde im Jahr 1990 von **Paul Monsky** auf die elliptischen Kurven E_n angewendet, die sich aus dem kongruenten Zahlenproblem ergeben, um das folgende Ergebnis zu erzielen. Eine Primzahl p, bei der p-5 oder p-7 durch 8 teilbar ist, ist immer eine kongruente Zahl. Wir erinnern uns, dass man für den Beweis dieses Ergebnisses darauf zurückgreifen kann um zu zeigen, dass der Rang der elliptischen Kurve E_p der Gleichung $y^2=x^3-p^2x$ mindestens eins ist. Mit anderen Worten, man steht vor der Aufgabe einen Punkt unendlicher Ordnung in E_p(**Q**) zu konstruieren. Diese Konstruktion wird durch die Theorie der Heegner-Punkte ermöglicht.

Bemerkung:
Die Korrespondenz zwischen elliptischen Kurven und Modulformen, die im Modularitätssatz beschrieben wird, ist ein Beispiel für allgemeinere Beziehungen zwischen mathematischen Objekten, die in den Bereichen Algebra und Analysis entstehen und durch das sogenannte Langlands-Programm vorhergesagt werden. Diese noch weitgehend konjekturale Forschungsrichtung stellt eine der anspruchsvollsten und aktuellsten Gebiete der modernen Zahlentheorie und der arithmetischen Geometrie dar.

Elliptische Kurven und der große Fermatsche Satz

Wie oben erwähnt, stellt der Modularitätssatz einen grundlegenden Schritt für den Beweis des **Großen Fermatschen Satzes (GFS)** dar. Zum Abschluss dieser Exposition wollen wir den Zusammenhang zwischen dem GFS und elliptischen Kurven aufrufen.

Der GFS besagt, dass die Gleichung $X^n+Y^n=Z^n$ keine Lösungen (a,b,c) in ganzen Zahlen hat, die nicht Null sind, wenn der Exponent n eine positive ganze Zahl größer als 2 ist. Wenn n=2 ist, ergibt die obige Gleichung natürlich die pythagoreische Beziehung der Seitenlängen eines rechtwinkligen Dreiecks, für die bekanntermaßen Lösungen in ganzen Zahlen existieren. Ein Beispiel für eine solche Lösung ist (3,4,5), welche die kongruente Zahl 6 ergibt, wie am Anfang unserer Exposition bemerkt. Zudem gibt es unendlich viele solcher Lösungen, wie die Formel für die pythagoreischen Tripel zeigt.

Um 1630 behauptete der französische Mathematiker (und Richter) Pierre de Fermat, einen Beweis für den

GFS in einer Notiz am Rand einer lateinischen Übersetzung des Buches „Arithmetica“ von Diophantus zu haben, der wirklich wunderbar, aber für diesen limitierten Rahmen zu lang sei. Die spätere Geschichte hat gezeigt, dass Fermat einen Beweis für den GFS nur im Spezialfall n=4 hatte, und zwar durch seine Methode des unendlichen Abstiegs, welche benötigt wird um zu zeigen, dass 1 keine kongruente Zahl ist. Die zahlreichen Versuche in den folgenden Jahrhunderten, einen Beweis für den GFS zu finden, haben eine wichtige Rolle in der Entwicklung der modernen Zahlentheorie gespielt, insbesondere durch die Bemühungen der Mathematiker Legendre, Dirichlet und Kummer aus dem 19. Jahrhundert. Es dauerte etwa 350 Jahre, bis Wiles einen Beweis für GFS fand und somit dieses Problem löste. Er führte dazu fundamentale neue Ideen ein, die vielen wichtigen Entwicklungen der Mathematik des 21. Jahrhunderts zugrunde liegen, zum Beispiel im Zusammenhang mit dem Langlands-Programm.

Was hat der GFS mit elliptischen Kurven und den in diesem Text behandelten Fragen zu tun? Wir skizzieren hier den Eröffnungsgambit des Beweises von GFS. Beachten Sie, dass es ausreicht, die Fermat-Gleichung für den Fall zu betrachten dass der Exponent n eine ungerade Primzahl p ist. Wenn man im Widerspruch argumentiert, nimmt man an, dass es ein Tripel (a,b,c) von ganzen Zahlen ungleich Null gibt, so dass $a^p+b^p=c^p$ ist. Auf der Basis dessen, was bereits über GFS bekannt ist, können wir auch verlangen dass p größer als 7 ist. Darüber hinaus ist es elementar zu sehen, dass man annehmen kann dass a,b,c keine gemeinsamen Faktoren haben, dass b eine gerade Zahl und a eine ganze Zahl ist, bei der a+1 durch 4 teilbar ist. Wir assoziieren mit (a,b,c) (mit einer Lösung die unserer Widerspruchsargumentation entstammt aber eigentlich nicht existieren soll!) die elliptische Kurve $E_{a,b}$ der Gleichung $y^2=x(x-a^p)(x+b^p)$. Diese Kurve wird Frey-Kurve genannt (benannt nach **Gerhard Frey**, einem der Gründer des Instituts für Experimentelle Mathematik der Universität Duisburg-Essen). Man beachte, dass diese Gleichung nicht genau der Form entspricht, die wir zuvor für elliptische Kurven gesehen haben, dass sie jedoch durch eine einfache Transformation der Koordinaten (x,y) in diese Form gebracht werden kann.

Der Beweis des GFS ist nur dadurch zu führen, dass man zeigt dass die obige elliptische Kurve $E_{a,b}$ nicht existieren kann. Aus dem Modularitätssatz ergibt sich, dass es eine Modulform $f_{a,b}$ vom Gewicht 2 gibt, die zu $E_{a,b}$ gehört. Darüber hinaus zeigt die Theorie der modularen Formen (insbesondere die Ergebnisse von **Barry Mazur** und **Kenneth Ribet**), dass $f_{a,b}$ wiederum einer Modulform $g_{a,b}$ vom Gewicht 2 und Stufe 2 mit ähnlichen Eigenschaften wie $f_{a,b}$ zugeordnet ist. Man betrachte den kompakten Raum **S**, der durch die Identifikation der Elemente z und z' der oberen Halbebene **H** erhalten wird, wenn sie die Beziehung $z'=(\alpha z+\beta)/(\gamma z+\delta)$ für ganze Zahlen $\alpha,\beta,\gamma,\delta$ erfüllen, so dass $\alpha\delta-\beta\gamma$ gleich 1 und γ durch 2 teilbar ist. Aus der geometrischen Theorie, die der Existenz von ga,b zugrunde liegt, ergibt sich, dass **S** wie eine Oberfläche mit mindestens einem Loch aussehen sollte. Eine direkte Berechnung zeigt jedoch, dass dieser Raum in Wirklichkeit eine Kugel ist und daher keine Löcher haben kann. Dies ist der gesuchte Widerspruch!

Summary

The Birch and Swinnerton-Dyer conjecture (BSD), proposed in the 1960s, is one of the fundamental open questions in pure Mathematics. It establishes a connection between the algebraic properties of the rational points of an elliptic curve and the analytic features of its associated L-function. This article provides an informal and relatively elementary introduction to the circle of ideas surrounding BSD. It does so by first introducing the much older problem of congruent numbers, which dates back to antiquity. This problem, which is to date still open, can be reformulated as a question about the rational points of a certain class of elliptic curves. The validity of BSD would lead to a positive answer to the congruent number problem. In turn, this problem is used in the text as a convenient testing ground for the state of our knowledge on BSD.
The article ends by recalling the fundamental role played by elliptic curves in the proof by Wiles and Taylor in the 1990's of the famous Fermat's Last Theorem. This proof relies on the deep and unexpected connection between elliptic curves and modular forms, which also implies the analytic continuation of the L-functions of elliptic curves.

Literatur

– Bertolini, Massimo: Report on the Birch and Swinnerton-Dyer conjecture, Milan Journal of Mathematics 78 (2010), no. 1, 153-178.
– Darmon, Henri, Diamond, Fred und Taylor, Richard: Fermat's last theorem. Elliptic curves, modular forms & Fermat's last theorem (Hong Kong 1993), 2-140, Int. Press, Cambridge, MA, 1997.
– Koblitz, Neal: Introduction to elliptic curves and modular forms, Second edition, Graduate Texts in Mathematics, 97, Springer-Verlag, New York, 1993.
– Sing, Simon: Fermats letzter Satz: Die abenteuerliche Geschichte eines mathematischen Rätsels, DTV, 2000.

Der Autor

Massimo Bertolini, geboren 1961, studierte Mathematik in Pavia (BSc 1984), an der Harvard University (MSc 1988) und an der Columbia University (PhD 1992). Danach war er „Ricercatore“ (Juniorprofessor, 1992–1999) und „Professore Associato“ (1999–2000) in Pavia und wurde dann Professor für Geometrie in Padua (2000–2003) und in Mailand (2003–2013). Seit 2013 ist Bertolini Professor für Arithmetische Geometrie an der Universität Duisburg-Essen.
Massimo Bertolinis Arbeitsgebiet ist die Zahlentheorie und die arithmetische Geometrie, insbesondere die arithmetische Theorie der elliptischen Kurven und Modulformen. Er forscht über die Beziehungen zwischen komplexen oder p-adischen L-Funktionen und rationalen Punkten sowie Zyklen der Shimura Varietäten. Die Birch und Swinnerton-Dyer Vermutung – welche im Text erklärt ist – stellt eine grundlegende motivierende Frage für Bertolinis Forschung dar.