Norbert Schappacher

Neuere Forschungsergebnisse in der Arithmetik elliptischer Kurven[1]

Anhand der Geschichte des Problems der sogenannten „kongruenten Zahlen" wird der Fortschritt moderner arithmetischer und algebraisch-geometrischer Methoden im Vergleich zu älteren, elementaren Techniken der Zahlentheorie illustriert. Der Artikel wirbt für Offenheit der Schulmathematik gegenüber neueren Entwicklungen der reinen Mathematik. Weder in historischer noch in mathematischer Hinsicht strebt er Vollständigkeit an.

0. Vorbemerkung

Bei manchen Gesprächspartnern ruft die Auskunft, ich beschäftigte mich beruflich mit Forschung in der reinen Mathematik, die erstaunte Frage hervor: „Ja, kann man denn da noch etwas erforschen?" – Auch Menschen, die sonst eine hohe Bildung haben, tragen die meistens verschwommene, jedenfalls aber völlig falsche Vorstellung mit sich herum, die Mathematik sei ein statischer Wissensbestand, der sich seit Euklid, oder jedenfalls seit der Entwicklung der Infinitesimalrechnung nicht wesentlich verändert habe. Dies ist ein bemerkenswerter Mißstand, weil bei Wissenschaften wie der Physik oder der Biologie der rapide Fortschritt, der dort doch nicht schneller oder tiefgreifender ist als in der heutigen Mathematik, vom öffentlichen Bewußtsein durchaus wahrgenommen wird.

Meines Erachtens haben die Mathematiklehrer in der Schule auch die Aufgabe, die Anzahl der Menschen, die eine solche falsche Vorstellung von der Mathematik haben, zu verkleinern.

Nun ist es allerdings nicht ganz leicht, neue Ergebnisse der reinen Mathematik darzustellen, und diese Schwierigkeit dürfte wohl ein Hauptgrund für den beschriebenen Mißstand sein. Worin diese Schwierigkeit *genau* besteht, ist mir selber übrigens nicht klar. Auch die Physik der Elementarteilchen z. B. ist sehr kompliziert und abstrakt, und doch werden ihre Fortschritte sogar in den Wissenschaftssparten großer Tageszeitungen kolportiert. Bei neuen mathematischen Ergebnissen vergleichbarer Bedeutung – wenn auch mit unvergleichlich geringerem Geldaufwand erzielt – ist dies fast nie der Fall. Wie dem auch sei – die entscheidende *inhaltliche* Schwierigkeit mathematische Ergebnisse darzustellen (ob sie nun spezifisch für die Mathematik ist oder auch auf andere Wissenschaften zutrifft, bleibe dahingestellt) liegt in der rasanten Theoriebildung der Mathematiker selber: Um ein schwieriges mathematisches Problem richtig zu sehen und einer Lösung näherzubringen, muß man erst eine Menge jeweils nicht leichter Begriffe, hinter denen ganze Theorien stehen, einführen.

Ich will dies hier am Beispiel des auch heute noch nicht vollständig gelösten *Problems der kongruenten Zahlen* erläutern, indem ich es durch die Mathematikgeschichte verfolge. Ich werde dabei versuchen anzudeuten, wo Unterrichtseinheiten zu diesem Fragenkreis anset-

1 Erweiterte Fassung eines Vortrags gehalten anläßlich des 1. Eichstätter Kolloquiums zur Didaktik der Mathematik am 23. Febraur 1988.

zen könnten. Es ist mir aber klar, daß der Ausblick auf die moderne Forschung, der doch eigentlich das Problem selbst erst so spannend machen würde, in der Schule sehr andeutungshaft bleiben muß. Trotzdem scheinen mir Schüler von einem Lehrer profitieren zu können, der um die Existenz weitergehender aufregender Forschungen weiß.

Gleichsam nebenbei wird man in meiner Darstellung eine andere Besonderheit der modernen reinen Mathematik bemerken können: – Seit sich im 19. Jh. im Wesentlichen die heutigen mathematischen Disziplinen herausgebildet haben, rechtfertigen sich die reinen Mathematiker gewissermaßen *intern*, nicht etwa durch eine mögliche Anwendung ihrer Ergebnisse. Eine solche kommt, wenn sie denn eintritt, häufig überraschend. In meinem Beispiel wird das daran deutlich, daß das Problem der kongruenten Zahlen *gerade dadurch Interesse* gewinnt, daß es so faszinierender Theoriebildungen bedarf, um es zu verstehen und dann hoffentlich auch eines Tages zu lösen. Die Lösung wäre weniger interessant als der tiefe Verstehenszuwachs, den uns die allgemeinen Theorien liefern, die zur Lösung beitragen. Wären Ingenieure an der Lösung interessiert, so wäre dem nicht so.

Die Freude an den allgemeinen Theorien ist aber deshalb nicht rein kontemplativ; denn sie umfassen viele und vielerlei einzelne Probleme, von denen man anfangs gar nicht ahnt, daß sie unter einem Dach Platz finden. So zöge der Beweis der Vermutungen von Birch und Swinnerton-Dyer, auf die das Problem der kongruenten Zahlen hier zurückgeführt wird, die Lösung vieler verschiedener zahlentheoretischer Probleme nach sich, nicht nur die des besonders elementar erklärbaren über die kongruenten Zahlen!

1. Das Problem

Definition: Eine rationale Zahl k heißt *kongruent*, wenn sie Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seitenlängen ist, d. h. wenn es rationale Zahlen a, b, c gibt, die $a^2 + b^2 = c^2$ erfüllen, so daß $2k = ab$ ist.

(Das Rechteck mit den Seiten a, b zerlegt sich diagonal in zwei Dreiecke mit Seiten a, b, c. Daher der Flächeninhalt ab/2 dieser Dreiecke.)

Problem: Gegeben eine (positive) rationale Zahl k, entscheide, ob sie kongruent ist oder nicht.

Reduktion der Fragestellung: Ersetzt man a, b, c durch ta, tb, tc, für eine rationale Zahl t, so ändert sich der Flächeninhalt k des rechtwinkligen Dreiecks zu $t^2 k$. Zu jeder rationalen Zahl k gibt es ein t, so daß $t^2 k$ eine quadratfreie (d. h. durch kein Quadrat einer Primzahl teilbare) ganze Zahl ist. Es genügt also, das Problem für quadratfreie positive ganze Zahlen k zu behandeln. Wir werden meistens annehmen, daß k diese Eigenschaft hat.

Primitive pythagoräische Tripel: Mitunter aber ist diese Normalisierung nicht günstig, sondern vielmehr die folgende. Wenn k kongruent ist, $2k = ab$, so findet man t, so daß die drei Zahlen ta, tb, tc ganze Zahlen mit größtem gemeinsamen Teiler 1 sind. Solche ganzen Zahlen A, B, C mit ggT 1 und der Relation $A^2 + B^2 = C^2$ heißen primitive pythagoräische Tripel. Entweder A oder B und nicht beide müssen dann gerade sein [denn C^2 kann nicht $\equiv 2 \pmod 4$ sein], und wir kommen überein, daß B immer die gerade der beiden Zahlen bezeichnen soll.

Schon die alten Griechen wußten nicht nur, daß es unendlich viele primitive pythagoräische Tripel gibt, sondern konnten sie auch schon mit zwei freien Variablen parametrisieren. Bevor wir das tun und auf unser Problem anwenden, erst einmal einige

2. Beispiele

Beispiel 1: Die erste kongruente Zahl, der man begegnet, ist k = 6, Fläche des kleinsten pythagoräischen Dreiecks mit den Seiten (a, b, c) = (3, 4, 5) – in der Tat ist ja 9 + 16 = 25.

Beispiel 2: Um k = 5, die kleinste quadratfreie ganze kongruente Zahl, als kongruent zu erkennen, muß man schon in die rationalen Zahlen greifen:

$$(a, b, c) = \left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right).$$

Beispiel 3: Don Zagier hat vor einigen Jahren mit der Abstiegsmethode (vgl. S. 154) bewiesen, daß das kleinste rationale rechtwinklige Dreieck mit Fläche k = 157 die folgenden Katheten hat:

$$a = 6803298487826435051217540 \,/\, 411340519227716149383203$$
$$b = 411340519227716149383203 \,/\, 21666555693714761309610$$

Und der Zähler der Hypotenuse c ist

$$224403517704336969924557513090674863160948472041;$$

ihr Nenner ist

$$8912332268928859588025535178967163570016480830.$$

Durch naives Probieren wird man dem Problem also wohl nicht beikommen ...

3. Der Aufzählungsalgorithmus

Das Problem der kongruenten Zahlen findet sich zum ersten Mal in arabischen Manuskripten des 9. und 10. Jh.s. Dort wird auch der jetzt zu erklärende Algorithmus entwickelt und anscheinend als Lösung gepriesen. – Wir werden sehen, daß dies eine enorme Überschätzung dieses Algorithmus war.

Wir knüpfen an 1. an und formulieren zunächst die Parametrisierung der primitiven pythagoräischen Tripel:

Satz 1: Für positive ganze Zahlen A, B, C gilt *genau dann*

(i) $A^2 + B^2 = C^2$

(ii) ggT(A, B, C) = 1 [wegen (i) ist dies gleichbedeutend damit, daß A, B, C paarweise teilerfremd sind], sowie

(iii) B gerade,

wenn es positive ganze Zahlen $\alpha > \beta$ mit $\mathrm{ggT}(\alpha, \beta) = 1$ und $\alpha - \beta$ ungerade gibt, so daß gilt

$$A = \alpha^2 - \beta^2 \qquad B = 2\alpha\beta \qquad C = \alpha^2 + \beta^2.$$

Dies kann man natürlich mit ein bißchen Sorgfalt algebraisch beweisen. Es ist aber wichtiger sich klar zu machen, woher diese Parametrisierung kommt (und wie man sie wiederfindet, wenn man sie mal vergessen hat ...): $(x, y) = (A/C, B/C)$ ist ein Punkt mit rationalen Koordinaten auf dem Einheitskreis $x^2 + y^2 = 1$. Alle solche Punkte findet man, ausgehend von einem offensichtlichen – z. B. $(-1, 0)$ –, indem man den anderen Schnittpunkt mit dem Kreis der Gerade durch $(-1, 0)$ mit der veränderlichen rationalen Steigung β/α bestimmt. Diese Gerade hat, nach x aufgelöst, die Gleichung $x = (\alpha/\beta)y - 1$. Ihre Schnittpunkte mit dem Einheitskreis haben also die y-Koordinaten 0 bzw. $2(\alpha/\beta)/((\alpha/\beta)^2 + 1)$. Letzterer liefert $x = ((\alpha/\beta)^2 - 1)/((a/\beta)^2 + 1)$. Erweitern mit β^2 ergibt den Satz 1.

Bemerkung: Kurven wie der Kreis, bei denen dieses Verfahren funktioniert – das ist keine ganz korrekte Definition ... –, heißen *rationale Kurven* oder *Kurven vom Geschlecht* 0. Diophantische Probleme – wie das der pythagoräischen Tripel –, die auf rationale Kurven führen, sind in einem gewissen Sinne leicht. Das Problem der kongruenten Zahlen führt auf *elliptische Kurven* oder *Kurven vom Geschlecht* 1. – Siehe 5. unten. Es ist also ganz andersartig.

Aus Satz 1 folgt, daß man alle ganzen quadratfreien kongruenten Zahlen irgendwann in folgendem Aufzählverfahren erhält.

Algorithmus:

- Zähle alle (α, β) wie in Satz 1 (z. B. in lexikographischer Reihenfolge) auf.
- Zu jedem (α, β) bestimme A, B – der Vollständigkeit halber vielleicht auch C – nach den Formeln von Satz 1.
- Berechne den Flächeninhalt $K = AB/2 = \alpha\beta(\alpha + \beta)(\alpha - \beta)$.
- Bestimme die quadratfreie ganze Zahl k, so daß $K = t^2 k$, für eine ganze Zahl t ist.

Dieser Algorithmus ist ganz und gar unbrauchbar! Man kann nämlich keine Schranke N(k) angeben, so daß k nach höchstens N(k) Schritten ausgespuckt wird, wenn es kongruent ist. Eine Zahl, die in der Liste, soweit wir sie gerade hingeschrieben haben, auf-

Anfang der Aufzählung:

α	β	A	B	C	K	k
2	1	3	4	5	6	6
3	2	5	12	13	30	30
4	1	15	8	17	60	15
4	3	7	24	25	84	21
5	2	21	20	29	210	210
5	4	9	40	41	180	5
6	1	35	12	37	210	210
6	5	11	60	61	330	330
7	2	45	28	53	630	70
7	4	33	56	65	924	231

etc.

taucht, ist sicher kongruent. Aber wie weit wir auch den Algorithmus treiben, wir können durch ihn nie *beweisen*, daß eine nicht auftretende Zahl *nicht* kongruent ist. Dieser theoretische Mangel ist durchaus praktischer Natur. Das Verfahren liefert die kongruenten k's in völlig wilder Reihenfolge und mit zahlreichen Wiederholungen.

Bemerkung: Bisher – und das wird sich auch im nächsten Abschnitt noch nicht ändern – sind wir noch ganz und gar im Rahmen elementarer Schulmathematik. Man muß aber bei der Darstellung des Geschilderten sorgfältig verhindern, daß eine Verwirrung zwischen den verschiedenen Normalisierungen in 1. entsteht, deren Unterschied ja der Unbrauchbarkeit des Algorithmus zugrundeliegt und fundamental für das Verständnis des Problems ist. Der Unterschied zwischen Aufzählbarkeit und Entscheidbarkeit, der hier gelernt werden kann, tritt an vielen Stellen in der Mathematik auf.

4. Fermat's Abstieg

Obwohl Fibonacci den folgenden Satz schon um 1225 in seinem *liber quadratorum behauptete*, war doch Fermat der erste, der ihn, in der Mitte des 17. Jh.s, *bewies* – und bei dieser Gelegenheit anscheinend seine neue Methode der *descente infinie*, des unendlichen Abstiegs, entwickelte.

Satz 2: 1 ist keine kongruente Zahl. Anders gesagt: Es gibt kein rationales rechtwinkliges Dreieck, dessen Flächeninhalt eine rationale Quadratzahl ist.

Beweis: Wäre die 1 kongruent, so käme sie in unserer Aufzählung irgendwann vor, d. h. es gäbe α, β wie in Satz 1 und eine ganze Zahl t mit $t^2 = \alpha\beta(\alpha+\beta)(\alpha-\beta)$. Man prüft nach, daß die vier Faktoren dieses Produktes paarweise zueinander teilerfremd sind. Da ihr Produkt ein Quadrat ist, muß also jede von ihnen ein Quadrat sein:

$$\text{(i) } \alpha = u^2 \qquad \text{(ii) } \beta = v^2 \qquad \text{(iii) } u^2 + v^2 = p^2 \qquad \text{(iv) } u^2 - v^2 = q^2.$$

Nimmt man (iii)–(iv), so ergibt sich: $2v^2 = (p+q)(p-q)$.

Jetzt muß man wieder sorgfältig die Teilerfremdheitseigenschaften studieren, anhand der Primfaktoren, die in $p, q, p+q, p-q$ aufgehen können. Man findet, daß $\text{ggT}(p+q, p-q) = 2$ ist. Also haben wir, für geeignete ganze Zahlen m, n mit m ungerade und n gerade, *entweder* $p+q = 2m^2$ und $p-q = n^2$, *oder* $p+q = n^2$ und $p-q = 2m^2$.

Aus (iii) + (iv) hat man $2u^2 = ((p+q)^2 + (p-q)^2)/2$; mithin: $u^2 = (m^2)^2 + (n^2/2)^2$. Das bedeutet, wir haben wieder ein rechtwinkliges Dreieck mit ganzen Seiten gefunden, dessen Fläche $F = m^2n^2/4$ ebenfalls ein Quadrat ist. Das neue Dreieck ist aber echt kleiner als das vorige, dessen Seiten A, B, C durch α, β nach Satz 1 gegeben sind. Die Hypotenuse des neuen Dreiecks: u, ist ein Teiler einer der Kathetenlängen des alten: $2\alpha\beta$.

Da es keine unendliche strikt absteigende Folge positiver ganzer Zahlen geben kann, war die ursprüngliche Annahme falsch, und 1 ist keine kongruente Zahl.

q.e.d.

Diesen großartigen Beweis kann man sicher in der Schule bringen; allerdings erfordert es wohl etwas Geschick, keines der Zwischenargumente (über ggT's ...) zu unterschlagen, und doch den Schwung des Gedankenganges im Ganzen noch spürbar zu halten. – Eine

Unterrichtseinheit über diesen Themenkreis sollte auch die Querverbindung zur Fermatschen Vermutung schlagen: – aus Satz 2 folgt, daß die Gleichung $x^4 + y^4 = z^4$ keine ganzzahligen Lösungen x, y, z mit $xy \neq 0$ hat ...

„Aufstieg": Fermats Methode besteht darin, mit einer gewissen Virtuosität aus einer („großen") Lösung des jeweiligen Problems eine andere („kleine") desselben – oder mitunter auch eines verwandten – Problems zu konstruieren. Das kann in manchen Fällen durchaus auch zur Lösung des Problems führen, wenn man von trivialen Anfangsdaten, die je nach Situation z. B. offensichtliche Lösungen eines Teilproblems sein können, rückwärts zu einer Lösung des Problems aufsteigt. So bestimmte Fermat z. B. 1643 das kleinste rechtwinklige ganzzahlige Dreieck, dessen Hypotenuse und Kathetensumme beide Quadrate sind. Es hat die Seiten 4565486027761, 1061652293520, 4687298610289.

5. Elliptische Kurven

Bis zum Beginn unseres Jahrhunderts waren keine wesentlich anderen Methoden zur Behandlung des Problems der kongruenten Zahlen bekannt als die bisher geschilderten. Eine neue Qualität dämmert in einer Arbeit des eher obskuren Mathematikers Turrière von 1915 auf: er zeigte „geometrisch", daß es unendlich viele rationale rechtwinklige Dreiecke mit Flächeninhalt 5 gibt. Dies Resultat verstehen wir heute als Folgerung aus dem fundamentalen

Satz 3: Die quadratfreie ganze Zahl k ist genau dann kongruent, wenn die Gleichung $y^2 = x^3 - k^2x$ unendlich viele Lösungen in rationalen Zahlen x, y hat.

Beweis: Wir beweisen zunächst die schwächere Aussage:

(*) k ist genau dann kongruent, wenn $y^2 = x^3 - k^2x$ eine rationale Lösung (x, y) mit $y \neq 0$ hat.

k kongruent bedeutet es gibt positive ganze Zahlen a, b, c, e mit $a^2 + b^2 = c^2$ und $ab = 2ke^2$. Mit Hilfe von Satz 1 finden wir eine rationale Zahl μ $(= \alpha/\beta)$, so daß $a = c(\mu^2 - 1)/(\mu^2 + 1)$, $b = 2c\mu/(\mu^2 + 1)$ ist. Also wird $((\mu^2 + 1)e/c)^2k = \mu^3 - \mu$, was für $x = k\mu$ und $y = k^2(\mu^2 + 1)e/c$ gerade in die Gleichung $y^2 = x^3 - k^2x$ übergeht. Man verfolgt in diesen Substitutionen, daß $y = 0$ genau dem Fall entspricht, wo a, b, c, e nicht alle positiv sind. Damit ist (*) bewiesen.

Um von (*) zu Satz 3 zu gelangen, müssen wir die Theorie der elliptischen Kurven bemühen.
Elliptische Kurven werden (jedenfalls über den rationalen Zahlen) stets durch eine Gleichung der Form

$$E: y^2 = x^3 + Ax + B,$$

mit rationalen Zahlen A, B, die $4A^3 - 27B^2 \neq 0$ erfüllen, gegeben. Zwei solche Gleichungen $y^2 = x^3 + Ax + B$ und $y^2 = x^3 + A'x + B'$ definieren dieselbe elliptische Kurve E (über den rationalen Zahlen), falls es eine rationale Zahl $u \neq 0$ gibt mit $A' = u^4A$, $B' = u^6B$.

Warnung: Die Ellipse ist *keine* elliptische, sondern eine rationale Kurve. Der Ausdruck „elliptische Kurve" kommt historisch daher, daß die Bogenlänge der Ellipse einen Integranden der Form dx/y hat, wo x, y eine Gleichung wie oben erfüllen.

Geometrisch unterscheiden sie sich von den rationalen Kurven – vgl. oben – dadurch, daß eine Gerade sie in drei Punkten schneidet. Dies macht eine Parametrisierung ihrer rationalen Punkte wie in Abschnitt 3, unmöglich; aber wir können zwei verschiedene Lösungen der Gleichung zu einer neuen verknüpfen! Mit etwas Geschick kann man aus dieser ersten Verknüpfung eine Gruppenstruktur auf den Punkten einer elliptischen Kurve konstruieren. Das neutrale Element dieser Gruppe – den „Nullpunkt" – wählt man als den „Punkt in ∞" auf der Kurve, der in projektiven Koordinaten durch $[0, 1, 0]$ repräsentiert wird. [In diesem geometrischen Zugang zum „Gruppengesetz auf den nichtsingulären Punkten einer Kubik" sind alle Axiome für abelsche Gruppen leicht nachzuprüfen – *außer der Assoziativität*!]

Im Lichte der Gruppenstruktur besehen, gibt es in der Menge $E(\mathbb{Q})$ der Punkte mit rationalen Koordinaten auf der elliptischen Kurve E: $y^2 = x^3 + Ax + B$ zwei Sorten von Elementen: Punkte $P = (x, y)$, für die es eine ganze Zahl $n \neq 0$ gibt, so daß die n-fache Verknüpfung $[n]P = P + \ldots + P$ der Nullpunkt ist, und solche, für die alle Vielfachen $[n]P$ voneinander verschieden sind. Punkte der ersten Sorte heißen *Torsionspunkte* oder Punkte endlicher Ordnung, die übrigen Punkte *von unendlicher Ordnung*. Um Satz 3 aus (*) zu folgern, genügt es, sich davon zu überzeugen, daß für die elliptische Kurve $E[k] : y^2 = x^3 - k^2x$ gilt:

(**) Der Nullpunkt und die Punkte $P = (x, y)$ mit $y = 0$ sind die einzigen Torsionspunkte in $E[k](\mathbb{Q})$.

Denn sobald man einen Punkt unendlicher Ordnung auf $E[k]$ gefunden hat, erhält man aus ihm unendlich viele Elemente von $E[k](\mathbb{Q})$.

Der Beweis von (**), auf den ich hier nicht näher eingehe, benutzt einen auf den ersten Blick ungewöhnlichen zahlentheoretischen Kunstgriff: man liest die Gleichung $y^2 = x^3 - k^2x = x(x + k)(k - k)$ als Gleichung in Zahlen *modulo* p, für alle Primzahlen p, die nicht 2k teilen. Es entsteht dann eine elliptische Kurve über dem Körper mit p Elementen, die wir $E(p)$ nennen wollen, und durch das Zählen Ihrer Punkte, für genügend viele p, kann man (**) zeigen. Allerdings geht dabei noch Dirichlet's Satz über „Primzahlen in arithmetischen Progressionen" (bewiesen 1837) ein: daß es nämlich, für je zwei gegebene teilerfremde ganze Zahlen a und m, unendlich viele Primzahlen $p \equiv a \pmod m$ gibt.

Wenn man Satz 3 anschaut, kann man den Eindruck bekommen, er sei wenig nützlich, insofern er das Problem, ob k kongruent ist – d. h. die Existenz *einer* rationalen Lösung der Gleichungen $a^2 + b^2 = c^2$, $2ke^2 = ab$ – durch die Bedingung ersetzt, daß eine andere Gleichung *unendlich viele* rationale Lösungen besitzt. Daß dies nicht so ist, liegt daran, daß [*vermutlich*] eine völlig andersartige Charakterisierung der elliptischen Kurven mit unendlich vielen rationalen Punkten im Unterschied zu denen mit endlich vielen rationalen Punkten möglich ist. Wie so häufig in der Mathematik brauchen wir dafür einen neuen Begriff ...

6. Die L-Funktion

Nun verlassen wir wohl definitiv den Bereich dessen, was man mit Oberstufenschülern noch behandeln könnte. Ich möchte aber trotzdem kurz die L-Funktion einführen, um danach ungewunden reden zu können.

Die L-Funktion der elliptischen Kurve $E[k]$: $y^2 = x^3 - k^2x = x(x+k)(x-k)$ ist eine Funktion $L(E[k], s)$ des komplexen Argumentes s, die für Realteil (s) > 3/2 durch das in dieser rechten Halbebene konvergente unendliche Produkt der Faktoren – ein Faktor für jede Primzahl p, die nicht in 2k aufgeht –

$$1/(1 - a_p p^{-s} + p^{1-2s})$$

gegeben ist. Hierbei ist a_p dadurch bestimmt, daß die reduzierte Kurve $E[k](p)$ genau $N(p) = 1 + p - a_p$ Punkte über dem Körper mit p Elementen hat (einschließlich dem „Nullpunkt" im Unendlichen).

Im allgemeinen weiß man nicht – vermutet es aber –, daß sich die L-Funktion einer elliptischen Kurve für alle komplexen Argumente s definieren und zu einer auf der ganzen komplexen Ebene holomorphen Funktion fortsetzen läßt. Für den Fall unserer elliptischen Kurven, die aus dem Problem der kongruenten Zahlen entstehen, ist dies aber bekannt. Genauer beweist man mit der analytischen Fortsetzung der L-Funktionen auch eine Funktionalgleichung, die für jedes komplexe s die Werte $L(E[k], s)$ und $L(E[k], 2 - s)$ in Zusammenhang bringt. Aus ihr erhält man die folgende Zusatzinformation:

Lemma 1: Ist $k \equiv 5, 6$ oder 7 (mod 8), so ist $L(E[k], 1) = 0$.

Tun wir mal so, als wäre das unendliche Produkt $L(E[k], s)$ auch für $s = 1$ konvergent (dies ist definitiv falsch – was folgt, ist nur Heuristik!). Dann wäre $L(E[k], 1)$ das unendliche Produkt der Terme

$$1/(1 - a_p/p + 1/p) = p/N(p).$$

Man sollte also erwarten, daß $L(E[k], 1) = 0$ ist, wenn es durchschnittlich „sehr viele" Punkte auf den reduzierten Kurven $E[k](p)$ gibt. Dies sollte sicher dann der Fall sein, wenn $E[k](\mathbb{Q})$ aus unendlich vielen Punkten besteht. Die Präzisierung dieser heuristischen Überlegung findet sich in den

7. Vermutungen von Birch und Swinnerton-Dyer

Mit der Einführung der L-Funktion sind wir in die Mathematik unserer Tage eingedrungen. Genauer begann die Beschäftigung mit den L-Funktionen elliptischer Kurven in den 30er Jahren unseres Jahrhunderts. Daß sich für unsere speziellen elliptischen Kurven $E[k]$ die L-Funktion $L(E[k], s)$ auf die ganze komplexe Ebene fortsetzen läßt, ist seit den fünfziger Jahren bekannt, beruht allerdings letztlich auf einer analytischen Theorie aus den Jahren 1918/19. Die Vermutungen von Birch und Swinnerton-Dyer entstanden, schon mit der Unterstützung von Beispielrechnungen auf den damaligen Computern, in den späten fünfziger Jahren.

Die gröbste dieser Vermutungen besagt:

Vermutung 1: E besitzt genau dann einen rationalen Punkt unendlicher Ordnung, wenn $L(E, 1) = 0$ ist.

Auf unser Problem angewandt, besagt dies gemäß Satz 3 und (**):

Vermutung 2: Die quadratfreie positive ganze Zahl k ist genau dann kongruent, wenn $L(E[k], 1) = 0$ ist für die elliptische Kurve $E[k]$: $y^2 = x^3 - k^2x = x(x + k)(x - k)$.

Wir stehen jetzt vor einer typischen Situation in der Entwicklung der Mathematik: *Scheinbar* wurde eine einfache Frage in eine abstrus komplizierte allgemeine Theorie übersetzt – so als ob alles, was die Mathematiker zu tun haben, darin bestünde, für den Rest der Welt unverständlich zu werden. *In Wirklichkeit* aber ist diese Umformulierung von unmittelbarer Bedeutung für die ursprünglichen elementaren Probleme. Am Beispiel der kongruenten Zahlen läßt sich das in besonders eindrucksvoller Weise demonstrieren:

8. Die neueren Resultate

Die folgenden Ergebnisse beziehen sich insbesondere auf alle Kurven $E[k]$: $y^2 = x^3 - k^2x = x(x + k)(x - k)$, für positive quadratfreie ganze Zahlen k.

Satz 4 (Coates – Wiles, 1977): Hat E unendlich viele rationale Punkte, so ist $L(E, 1) = 0$.

Dies war der erste große Schritt in Richtung auf die Vermutungen von Birch und Swinnerton-Dyer. Uns gibt er ein potentielles Kriterium dafür, wann eine Zahl k nicht kongruent ist.

Satz 5 (Gross – Zagier, 1983): Ist $L(E, 1) = 0$ aber die Ableitung $L'(E, 1) \neq 0$, so hat E unendlich viele rationale Punkte.

Für viele Werte $k \equiv 5, 6$ oder 7 (mod 8) kann man numerisch auf dem Computer nachprüfen, daß $L'(E[k], 1) \neq 0$ ist. In diesen Fällen liefert Satz 5 dann einen Beweis, daß k kongruent ist!

Formel [Waldspurger – Tunnell, 1981/82]: $L(E[k], 1) = 0$ genau dann, wenn $c(k) = 0$ ist, wobei $c(k)$ die Summe der Vorzeichen $(-1)^w$ ist, summiert

- über alle Darstellungen von k in der Form $k = u^2 + 2v^2 + 8w^2$, falls k ungerade ist;
- über alle Darstellungen von $k/2$ in der Form $k/2 = u^2 + v^2 + 8w^2$, falls k gerade ist.

Damit hat man – Vermutung 2 einmal angenommen – eine sehr leichte rechnerische Methode – ohne analytische Rechnungen –, um zu entscheiden, ob ein gegebenes k kongruent ist oder nicht. Und jedenfalls in der negativen Richtung von Satz 5 haben wird die Aussage von Vermutung 2 ja zur Verfügung!

Mit diesen weitreichenden Resultaten ist es zum ersten Mal in der Geschichte der Mathematik möglich, alle positiven ganzen quadratfreien kongruenten Zahlen unter einer gegebenen Schranke (im Bereich der Rechenkapazität) zu bestimmen. So geben wir zum Abschluß folgende Übersicht über die kongruenten Zahlen unter 2000.

- Es gibt 1215 quadratfreie ganze Zahlen k mit $0 < k < 2000$.
- Davon sind 602 Zahlen $k \equiv 1, 2$ oder 3 (mod 8).
- Unter diesen haben (gemäß obiger Formel) 496 Zahlen $L(E[k], 1) \neq 0$ und sind damit nicht kongruent nach Satz 4.
- Bei den restlichen 106 Werten von k ist $L(E[k], 1) = L'(E[k], 1) = 0$, und man ist bei dem momentanen Wissensstand darauf angewiesen, wirklich Punkte unendlicher Ordnung auf $E[k]$ nachzuweisen, d.h. mit dem Rechner Lösungen der Gleichung $y^2 = x^3 - k^2x$ mit $y \neq 0$ zu finden. Das gelingt aber in diesen Fällen gerade sehr leicht – eine Tatsache, die übrigens durch feinere Vermutungen von Birch und Swinnerton-Dyer durch das Vorliegen einer mindestens doppelten Nullstelle von $L(E, s)$ bei $s = 1$ erklärt wird.
- 613 der k's sind $\equiv 5,6$ oder 7 (mod 8). Hier kann man jeweils numerisch testen, ob $L'(E[k], 1) \neq 0$ ist. Der einzige Fall, in dem dies nicht gelingt und wo tatsächlich $L'(E[k], 1) = 0$ gilt, ist $k = 1254$. Hier findet man, ähnlich wie in den eben diskutierten 106 Fällen, leicht Punkte unendlicher Ordnung auf $E[k]$. Für $k \neq 1254$ braucht man wegen Satz 5 nicht eigens nachprüfen, daß k in der Tat kongruent ist.

Anschrift des Verfassers: Dr. Norbert Schappacher, Max-Planck-Institut für Mathematik, Gottfried-Claren-Straße 26, 5300 Bonn 3

Eingangsdatum: 20.5.1988

Literatur

Ein elementar geschriebenes, für den Reichtum an in ihm behandelten Einzelresultaten berühmtes, allerdings (besonders in seiner Darstellung der arabischen Mathematik) etwas veraltetes unhistorisch gegliedertes Buch zur Geschichte der Zahlentheorie, in dem dem Problem der kongruenten Zahlen ein eigenes Kapitel gewidmet ist, ist:

[1] Dickson, L.E.: History of the Theory of Numers. Chelsea 1952

Eine nicht ganz elementare, aber recht gute Einführung in den Gedankenkreis des Vortrags bietet

[2] Koblitz, H.: Introduction to elliptic cures and modular forms, Graduate Texts in Mathematics 97. Springer Verlag 1984
Dort findet man auch die Verweise auf die (natürlich sehr schwer lesbaren) Originalarbeiten zu den Resultaten von Abschnitt 8.

Am Schluß des Vortrags stüze ich mich auf

[3] Kramarz, G.: All congruent numbers less than 2000; Mathematische Annalen 273 (1986), S. 377–340.

Ein grundlegendes Lehrbuch über die Arithmetik elliptischer Kurven ist

[4] Silverman, J.H.: The Arithmetic of Elliptic Curves; Graduate Texts in Mathematics 106. Springer Verlag 1986