Proceedings of the AMS Centennial Symposium
August 8–12, 1988

Elliptic Curves and Modular Forms

BENEDICT H. GROSS

An elliptic curve E over the field k has a nonsingular plane model of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the coefficients a_i lie in k. The set $E(k)$ of solutions to this equation (in the projective plane) has the structure of an abelian group: the unique point on the line at infinity is taken as the origin and any three collinear points sum to zero. When $k = \mathbf{C}$ is the field of complex numbers, the theory of elliptic functions identifies $E(\mathbf{C})$ with a complex torus, so—as a topological group—with the product of two circles. When the field k is finite, $E(k)$ is clearly a finite group. When k is a number field (an extension of finite degree of the field $\mathbf{Q}$ of rational numbers) the famous theorem of Mordell and Weil states that the group $E(k)$ is finitely generated.

We will focus our attention on the case when $k = \mathbf{Q}$. Since $E(\mathbf{Q})$ is finitely generated, we have an isomorphism

$$E(\mathbf{Q}) \simeq \mathbf{Z}^r \oplus T,$$

where $r \geq 0$ is an integer and T is a finite group. The torsion subgroup T is easily determined in any given case, and the proof of the Mordell-Weil theorem yields an effective upper bound for the rank r of E. To determine if this upper bound is sharp requires a search for rational points.

The following example has been investigated by Bremner and Cassels. Let q be a prime number with $q \equiv 5 \pmod 8$, and let E be defined by the equation

$$y^2 = x^3 + qx.$$

Then the subgroup T of $E(\mathbf{Q})$ is cyclic of order 2, generated by the point $P = (0, 0)$, and the rank r satisfies $r \leq 1$. One suspects that $r = 1$ in all cases, although this is only known for $q < 20,000$. Occasionally, the search for a solution is quite time consuming: for example, when $q = 2437$ the

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G05, 11G40.

0-8218-0167-8 $1.00 + $.25 per page

smallest point $P = (x, y)$ of infinite order in $E(\mathbf{Q})$ has coordinates

$$x = \frac{1058218655773369472688280687468828399922014718555143690966617841}{27508198704124179442177085617703251309296618759637460058339690 0},$$

$$y = \frac{443090331670870476765298567239328435425666485280521498925653337454193713916697369438335483590388 9}{456239864063626703417836039335474295820718928066408691576766042122770828093177511858631495300 0}.$$

One approach to the determination of the rank is to study the number of solutions to the equation modulo p. Choose a plane model for E with integral coefficients and minimal discriminant Δ. Let A_p denote the number of solutions of the reduced equation (including the point at infinity) over $\mathbf{Z}/p\mathbf{Z}$, and write $A_p = p+1-a_p$. The L-function of E, which packages this information into an analytic function of the complex variable s, is defined by the Euler product

$$L(E, s) = \prod_{p|\Delta}(1 - a_p p^{-s})^{-1} \cdot \prod_{p\nmid\Delta}(1 - a_p p^{-s} + p^{1-2s})^{-1}$$

which converges in the half-plane $\Re(s) > 3/2$. Expanded out, this product is a Dirichlet series $\sum_{n\geq 1} a_n \cdot n^{-s}$ with integral coefficients a_n.

If we formally set $s = 1$ in the Euler product, we find the formal product $\prod(p/A_p^0)$, where A_p^0 is the number of nonsingular points on E modulo p. Motivated by the expectation that a large value of r should lead, on the average, to a large number of solutions modulo p, Birch and Swinnerton-Dyer conjectured that the order of vanishing of $L(E, s)$ at the point $s = 1$ is equal to the rank r. Aided by Cassels and Tate, they also gave an arithmetic interpretation for the leading term in its Taylor expansion there.

To begin to attack this conjecture, one needs the analytic continuation of $L(E, s)$ to a neighborhood of $s = 1$. Following Taniyama, Shimura, and Weil, one now hopes to prove that the function $L(E, s)$ is entire by showing that it is the Mellin transform of a modular form. More precisely, let N be the conductor of the curve E. This is an integer, with the same prime factors as the minimal discriminant Δ, which measures the ramification in the division fields of E.

CONJECTURE. *The function* $f(\tau) = \sum_{n\geq 1} a_n e^{2\pi i n\tau}$, *for* τ *in the upper half-plane, is a cusp form of weight* 2 *for the congruence subgroup* $\Gamma_0(N)$ *of* $\mathrm{SL}_2(\mathbf{Z})$.

The group $\Gamma_0(N)$ consists of integer matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $ad - bc = 1$ and $c \equiv 0$ (modulo N), and $f(\tau)$ is modular of weight 2 if for every such matrix we have the identity $f((a\tau+b)/(c\tau+d)) = (c\tau+d)^2 f(\tau)$. If $f(\tau)$ is a cusp form, its Mellin transform

$$\Lambda(f, s) = \int_0^\infty f(iy) y^s \frac{dy}{y} = (2\pi)^{-s}\Gamma(s)L(E, s)$$

is entire. Moreover, Carayol has shown that f is then a "newform" of level N, and hence an eigenfunction for the Fricke involution: $f(-1/N\tau) = \lambda \cdot N\tau^2 f(\tau)$, with $\lambda = \pm 1$. This implies that $\Lambda(f, s)$ satisfies the functional

equation

$$\Lambda(f, s) = \varepsilon \cdot N^{1-s}\Lambda(f, 2-s)$$

with $\varepsilon = -\lambda$.

There is now a great deal of theoretical and computational evidence in favor of the conjecture that $f(\tau)$ is modular, and for a given curve E it can be checked using a finite amount of computation. For example, the conjecture is true for the curves $y^2 = x^3 + qx$ mentioned above; its truth for all elliptic curves over $\mathbf{Q}$ implies Fermat's Last Theorem, by recent work of Ribet. In all that follows, we will assume the conjecture is true for the curve E, and will derive some geometric and arithmetic consequences.

Let $X_0(N)$ be the modular curve over $\mathbf{Q}$ which classifies elliptic curves with a cyclic subgroup of order N. The work of Eichler and Shimura shows that the newform $f(\tau)$ determines an elliptic quotient E_0 of the Jacobian of $X_0(N)$ over $\mathbf{Q}$, and Faltings' results on the isogeny conjecture show that E_0 is isogeneous to E. Hence there is a nonconstant regular map $\varphi\colon X_0(N) \to E$ over $\mathbf{Q}$ which takes the cusp ∞ of $X_0(N)$ to the origin of E. The differential $2\pi i f(\tau)\, d\tau$ on the upper half-plane is invariant under $\Gamma_0(N)$ and defines a regular differential on $X_0(N)$ over $\mathbf{Q}$. Once φ has been chosen, there is a unique invariant differential ω on E which satisfies $\varphi^*(\omega) = 2\pi i f(\tau)\, d\tau$ on $X_0(N)$.

The following method of constructing points on E over number fields is due to Birch. Let K be an imaginary quadratic field of discriminant $-D$, where all prime factors of N are split. Let H be the Hilbert class-field of K (the maximal abelian unramified extension, which has finite degree equal to the class-number of K). Using the theory of complex multiplication, one can construct Heegner points x on $X_0(N)$ over H. We then define P_K as the trace of the point $\varphi(x)$ from $E(H)$ to $E(K)$; this trace is calculated by adding $\varphi(x)$ to its conjugates, using the group law on E. Zagier and I found a formula for its canonical height $\hat{h}$, which measures the amount of paper required to record P_K, in terms of the derivative of the L-function of E over K:

$$L'(E/K, 1) = \frac{\iint_{E(C)} \omega \wedge \overline{\omega}}{\sqrt{D}} \cdot \hat{h}(P_K).$$

This formula implies that the point P_K has infinite order in $E(K)$ if and only if $L'(E/K, 1) \neq 0$.

The precise conjecture of Birch and Swinnerton-Dyer predicts that when P_K has infinite order, the group $E(K)$ has rank 1, and that the finite index $[E(K) : \mathbf{Z}P_K]$ annihilates the Tate-Šafarevič group of E over K. Kolyvagin has recently made a great advance, which essentially proves this. His work brings us close to a proof of the full conjecture of Birch and Swinnerton-Dyer, for modular elliptic curves E over $\mathbf{Q}$ where the order of $L(E, s)$ at $s = 1$ is either 0 or 1. But the conjecture for those curves where the L-function vanishes to order ≥ 2 remains completely mysterious, as does the central

problem of why the function $f(\tau)$ attached to an elliptic curve E over $\mathbf{Q}$ is a modular form.

Bibliographic Remarks

An excellent introduction to elliptic curves is the survey article by Tate [1]. This work also contains a long list of references. Some excellent introductory works on elliptic curves have also appeared recently in the Springer graduate text series, see [2–4]. For a discussion of modular forms on $\Gamma_0(N)$, and the theory of complex multiplication, I would recommend [5]. The formula for the heights of Heegner points is proved in [6]; Kolyvagin's work appears in [7].

1. J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.
2. D. Husemöller, *Elliptic curves*, Graduate Texts in Math., vol. 111, Springer, 1987.
3. N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Math., vol. 97, Springer, 1984.
4. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer, 1986.
5. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan II, Iwanomi Sholen and Princeton Univ. Press, 1971.
6. B. H. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.
7. V. A. Kolyvagin, *Euler systems*, Grothendieck Festschift, Birkhaüser, 1990.

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138