ELLIPTIC CURVES OVER Q: A PROGRESS REPORT

B. J. BIRCH

Let E be an elliptic curve defined over the rationals Q; we may take E in Weierstrass form $y^2 = x^3 + Ax + B$, with A, B integers. Its rational points form a group, which we denote by E_Q; the theorem of Mordell tells us that E_Q is finitely generated. A principal problem of the theory is to determine the group E_Q, and in particular to determine its rank g; well-known conjectures, described in [14], connect E_Q with the zeta function of the curve. Let us recall the appropriate definitions.

If p does not divide $6(27B^2 + 4A^3)$ then the reduction E_p, defined over the finite field k_p, is an elliptic curve; we call such primes *good.* The local zeta function of E_p over k_p is

$$\zeta_p(E_p, s) = \frac{(1 - \alpha_p p^{-s})(1 - \bar{\alpha}_p p^{-s})}{(1 - p^{-s})(1 - p^{1-s})}$$

where α_p, $\bar{\alpha}_p$ are the eigenvalues of the Frobenius transformation; so $\alpha_p\bar{\alpha}_p = p$ and $\alpha_p + \bar{\alpha}_p = 1 + p - N_p$, where N_p is the number of points of E_p with coordinates in k_p. We may define an L-function by

$$L_E^{\dagger}(s) = \prod (1 - \alpha_p p^{-s})^{-1}(1 - \bar{\alpha}_p p^{-s})^{-1}$$

where the product is taken over good primes. We know that $|\alpha_p| = p^{1/2}$, so $L_E^{\dagger}(s)$ converges for $\mathrm{Re}\,(s) > 3/2$.

Now let ω be a differential on E; we may take $\omega = dx/2y$. Then ω gives a Haar measure on the various completions of E, and we may form

$$M_p(E) = \int_{E(Q_p)} |\omega|_p, \qquad M_\infty(E) = \int_{E(\mathbf{R})} \omega$$

where the integral $M_p(E)$ is over the p-adic points of E, and $M_\infty(E)$ is an integral over the real points of E. Note that if p is good, then $M_p(E) = N_p/p = (1 - \alpha_p p^{-1})(1 - \bar{\alpha}_p p^{-1})$. For any set S of primes including all primes dividing $6(27B^2 + 4A^3)$ and the infinite prime, define

$$L^*_{E,S}(s) = \prod_{p\in S} M_p(E)^{-1} \prod_{p\notin S} (1 - \alpha_p p^{-s})^{-1}(1 - \bar{\alpha}_p p^{-s})^{-1}.$$

We will be interested in whether $L^*_{E,S}(s)$ may be continued past $s = 1$, and, if it may, in its behavior near $s = 1$; none of this depends on the particular choice of the set S, so in assertions for which S is irrelevant we will write simply L^*_E instead of $L^*_{E,S}$.

Now we state the standard conjectures; in order for the others to make sense, we need (not at full strength)

(I) $L_E(s)$ may be continued as a meromorphic function over the whole plane, and has a functional equation.

Given this, we may state the others.

(II) $L_E(s)$ has a zero of order g at $s = 1$.

(III) If $g = 0$, then $L^*_E(1) = |\text{Ш}|/|E_Q|^2$, where $|\text{Ш}|$ is the order of the Tate-Safarevic group, and $|E_Q|$ is the order of E_Q.

(IV) $L^*_E(s) \sim |\text{Ш}|R|\text{Tors}\,(E_Q)|^{-2}(s - 1)^g$ as $s \to 1$, where now $|\text{Tors}\,(E_Q)|$ is the number of points of E_Q of finite order, and R is an analogue of the regulator of an algebraic number field, and measures the size of the generators of E_Q.

For curves with complex multiplication, (I) is a theorem of Deuring [7]; accordingly, it was natural that such curves should be examined first. Curves of the shape $y^2 = x^3 - Dx$, which have complex multiplication by i, were treated in [2]; we proved

(V) $L^*_E(1)$ is rational, with bounded denominator,

and for a very large number of values of D, we verified (II) and (III) in a weakened form. To be precise, we found that $L^*(E, 1) = 0$ whenever $g > 0$, and $|E_Q|^2L^*_E(1)$ was a positive square when $g = 0$; there is no known way of calculating Ш, so at present we cannot verify (III) as stated, but $|\text{Ш}|$ is a square if it is finite.

Subsequently, Stephens [13] has treated curves of the shape $x^3 + y^3 + Az^3 = 0$, with complex multiplication by $\sqrt[3]{1}$; he proved (V), and verified (II), (III), and (IV) (with the same gloss about Ш, and (IV) only approximately) in several thousand cases. Rajwade [11] and Damerell [6] have completed the theory for all elliptic curves over Q with complex multiplication; they have proved (V), and Damerell has made a few computations.

In all this published work, the methods have followed [2] fairly closely; $L^*_E(1)$ is evaluated in terms of a closed formula involving $\wp$-functions. It seems unlikely that this is really the right way to do it. Curves with complex multiplication are a much smaller class than the class of elliptic curves that may be parametrized by modular functions. For modular function curves, (I) is usually provable and methods of evaluating $L^*_E(1)$ are available which seem much simpler and more effective than those involving $\wp$-functions (the ideas go back essentially to Shimura). Though the methods applicable to curves parametrized by modular functions were in fact sketched in [14], no one seems to have noticed, so it seems worthwhile to publicize them further.

We call E: $y^2 = x^3 + Ax + B$ a 'good' elliptic curve if, for some N, E is parametrized by functions on $H/\Gamma_0(N)$, and 'corresponds to' a differential

$f(z)\,dz = \sum a_n \exp(2\pi i n z)\,dz$ on $H/\Gamma_0(N)$. It corresponds in two senses: the curve E is obtained by integrating f along paths on $H/\Gamma_0(N)$, and also the zeta function of E is

$$L_E(s) = \sum a_n n^{-s} = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(iz) z^{s-1}\,dz.$$

In taking this formula for $L_E(s)$, we have implicitly made a canonical choice for factors of the Euler product corresponding to the bad primes. The analytic conductor of E is the minimal N for which all this is possible.

The above properties are more than enough to characterize 'good' elliptic curves. It is generally believed that if E has analytic conductor N then it also has algebraic conductor N, in the sense of [10] and [16]; in view of results of Igusa [9], a good curve with analytic conductor N has good reduction at primes not dividing N. If E is a good curve, its L-function satisfies a functional equation, for the involution W_N: $z \leftrightarrow -1/Nz$ of $H/\Gamma_0(N)$ takes $f(z)\,dz$ to $\epsilon f(z)\,dz$, with $\epsilon = \pm 1$, and then $\Lambda_E(s) = -\epsilon N^{1-s}\Lambda_E(2-s)$ where $\Lambda_E(s) = (2\pi)^{-s}\Gamma(s)L_E(s)$, and $L_E(s)$ may be continued over the whole plane; in a similar way $L_E(s, \chi) = \sum a_n \chi(n) n^{-s}$ has a functional equation for any character χ with conductor D prime to N.

Virtue in the sense we have just described appears to be a great deal to ask of a curve. However, no one has yet found an elliptic curve over Q which is not isogenous to a 'good' curve; following Weil [16] we may conjecture that every elliptic curve over Q is isogenous to a good curve. A necessary corollary of such a conjecture would be that two elliptic curves with the same zeta function should be isogenous—this seems likely, in fact Serre [12] goes a long way toward proving it (see also Tate [15]). For fixed N, it is not too difficult to list all isogeny classes of elliptic curves with analytic conductor N—it comes down to a question of factoring the Jacobian of $H/\Gamma_0(N)$ (up to isogeny) as a product of simple abelian varieties, and this may be accomplished by studying the operation of the Hecke algebra on the one-dimensional homology of $H/\Gamma_0(N)$. A computational procedure is described in some detail in [14, pp. 146–148]. (At the time, the procedure was not guaranteed to work, but necessary information, that certain Hecke operators have distinct eigenvalues, has since been supplied by Atkin and Lehner [1].) It is desirable to make a comparison with lists of all curves with algebraic conductor N; using Baker's theorem, it is now possible to make such lists, and we hope to do so.

There are obvious advantages in looking at good curves—they are born equipped with an almost excessively rich structure. One has simply to pull out the information one needs. Let us give a few examples.

First, let us check that $L_E^*(1)$ is rational, and show how to compute it. $L_E^*(1)$ is a rational multiple of $L_E(1)/M_\infty(E)$, and $M_\infty(E)$ is essentially the real period of E. On the other hand, $L_E(1) = -2\pi i \int_0^{i\infty} f(z)\,dz$; there is a function on $H/\Gamma_0(N)$ with all its zeros at 0 and all its poles at $i\infty$, so it is clear that $L_E(1)$ is a rational multiple of a real period of the Jacobian of $H/\Gamma_0(N)$, and reasonable to suppose that this period is actually the real period of E. So $L_E^*(1)$ is computable, using no more than qualitative information about the differential on $H/\Gamma_0(N)$ corresponding to E.

We have control not only over the L-function of E over Q, but also of E over K whenever K is an abelian extension of Q. If χ is a character with conductor D

prime to N, then

$$L_E(s, \chi) = \sum a_n \chi(n) n^{-s} = -2\pi i \int_0^{i\infty} \sum a_n \chi(n) \exp(2\pi i n z)\, dz$$
$$= \sum_{0 \leq b < D} \lambda_b I(b/D), \quad \text{say},$$

where

$$\lambda_b = D^{-1} \sum_{(a,D)=1} \exp(-2\pi i a b/D) \chi(a)$$

is a Gauss sum, and

$$I(b/D) = -2\pi i \int_0^{i\infty} f\left(z + \frac{b}{D}\right) dz = -2\pi i \int_{b/D}^{i\infty} f(z)\, dz$$

is an integral of a differential along a path. To compute $L_E(1, \chi)$ in terms of the periods of E is a matter of one-dimensional homology, expressing the paths $[b/D, i\infty]$ (or, directly, the 1-chain $\sum \lambda_b [b/D, i\infty]$) in terms of the homology cycles on $H/\Gamma_0(N)$. The homology computation is a simple one, reminiscent of the continued fraction expansion of b/D; it is easy to do by hand and not hard to program.

In particular, if χ happens to be the quadratic character corresponding to $Q(\Delta^{1/2})$, then the L-function of the curve $E(\Delta)$: $\Delta y^2 = x^3 + Ax + B$ is essentially $L_E(s, \chi)$; so we may compute all of these. The functional equation of $L_E(s, \chi)$ contains a factor $\epsilon\chi(N)$, so (II) predicts that the parity of g should depend on the quadratic character of N modulo D—this seems consistent with the Selmer conjecture, that g has the same parity as the number of first descents.

One would like very much to evaluate $L'_E(1)$ exactly. Unhappily, even if $L_E(1) = 0$, $L'_E(1) = 2\pi \int_0^{i\infty} f(iz) \log z\, dz$ is a thoroughly unmanageable function, about which we have as yet nothing good to say.

A most enticing hope is that, besides being able to evaluate the L-functions involved in the conjectures more easily, we should actually be able to prove the conjecture sometimes. The idea originates with Heegner [8]; its point is that $H/\Gamma_0(N)$, and hence any 'good' curve, is born equipped with points on it whose coordinates are in predictable class fields. In favorable circumstances, it is possible to pull down these points, so that we may explicitly construct generators for E_Q, just as the conjectures predict. I have given details elsewhere [3], [4], [5] but so far I have only been able to make the 'pull down' argument work for curves $E(p)$ of the pencil $py^2 = x^3 + Ax + B$ for which $\pm p$ is prime.

REFERENCES

1. A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann.

2. B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves.* II, J. Reine Angew. Math. **218** (1965), 79–108. MR **31** #3419.

3. B. J. Birch, *Diophantine analysis and modular functions*, Proc. Conf. Algebraic Geometry (Bombay, 1968), pp. 35–42.

4. ———, *Elliptic curves and modular functions*, Proc. Conf. Number Theory (Rome, 1968).

5. ———, *Weber's class invariants*, Mathematika **16** (1969), 283–294.

6. M. Damerell, Ph. D. Thesis, Cambridge, 1969.

7. M. Deuring, *Die Zetafunktion einer algebraischen Kurve von Geschlechte Eins.* I, II, III, IV, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. IIa **1953,** 85–94; **1955,** 13–42; **1956,** 37–76; **1957,** 55–80. MR **15,** 779; MR **17,** 17; MR **18,** 113; MR **19,** 637.

8. K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253. MR **14,** 725.

9. J.-I. Igusa, *Kroneckerian model of fields of elliptic modular functions*, Amer. J. Math. **81** (1959), 561–577. MR **21** #7214.

10. A. P. Ogg, *Abelian curves of small conductor*, J. Reine Angew. Math. **226** (1967), 204–215. MR **35** #1592.

11. A. R. Rajwade, *Arithmetic on curves with complex multiplication by* $\sqrt{-2}$, Proc. Cambridge Philos. Soc. **64** (1968), 659–672. MR **37** #4079.

12. J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968.

13. N. M. Stephens, *The diophantine equation* $X^3 + Y^3 = DZ^3$ *and the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **231** (1968), 121–162. MR **37** #5225.

14. H. P. F. Swinnerton-Dyer, *The conjectures of Birch and Swinnerton-Dyer, and of Tate*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 132–157. MR **37** #6287.

15. J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR **34** #5829.

16. A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149–156. MR **34** #7473.

MATHEMATICS INSTITUTE
OXFORD, ENGLAND