Proc Symp Pure Math Vol VIII, 106–112
Amer Math Soc, 1965

Conjectures Concerning Elliptic Curves

BY

B. J. BIRCH

The subject of this lecture is rather a special one. I want to describe some computations undertaken by myself and Swinnerton-Dyer on EDSAC, by which we have calculated the zeta-functions of certain elliptic curves. As a result of these computations we have found an analogue for an elliptic curve of the Tamagawa number of an algebraic group; and conjectures (due to ourselves, due to Tate, and due to others) have proliferated. A preliminary account of this work has been given in his Stockholm lecture [8] by Cassels, who has been very helpful to us at all stages. I would like to stress that though the associated theory is both abstract and technically complicated, the objects about which I intend to talk are usually simply defined and often machine computable; experimentally we have detected certain relations between different invariants, but we have been unable to approach proofs of these relations, which must lie very deep.

As is well known, any elliptic curve over the rationals with a rational point on it can be normalised to the form C: $y^2z=x^3-axz^2-bz^3$, with a, b integers. The points of C form an abelian group, and the rational points of C form a subgroup, which I will denote by A; by the Mordell-Weil theorem (in the form first given by Mordell [17]; see Weil [27] and Lang [14] for more conceptual proofs) we know that A is a finitely generated abelian group.

We write g for the number of independent generators of infinite order of A, and f for the number of points of A of finite order. It is fairly easy, for a given curve, to compute f; methods have been given for curves over the rationals by Nagell [18] and for curves over a $\mathfrak{p}$-adic field by Lutz [16]; Nagell has conjectured that for elliptic curves over the rationals f is absolutely bounded, but this appears to be a very difficult question. There remains the problem of finding an effective method of computing g.

Some years ago, Swinnerton-Dyer and I began a series of experiments by which we attempted to relate the global properties of an elliptic curve to its local properties; that is, we tried to relate the group A of rational points on C to the groups $C^{(p)}$ of p-adic points on C, or, what is nearly the same thing, to the numbers N_p of points on the (projective) curves

$$C_p\colon\ y^2z\equiv x^3-axz^2-bz^3\ (p).$$

At first, we were fairly naïve; we simply computed $\prod_{p\leq 439} N_p/p$ for various curves C, and we were able to verify that this product was small, medium or large according as $g=0$, $g=1$ or $g\geqq 2$. We formulated the conjecture that

$\prod_{p<X} N_p/p \sim K(\log X)^g$ as $X \to \infty$. Unfortunately, in the range of our computations the product $\prod_{p<X} N_p/p$ oscillated violently as X increased, so the evidence for this conjecture was not really convincing.

However, there is often a better way of proceeding. For each prime p, the curve C_p has a zeta function, defined in the usual way (see for instance [28; 11]); it turns out to be

$$\zeta_{C_p}(s) = \frac{1+(N_p-p-1)\,p^{-s}+p^{1-2s}}{(1-p^{-s})(1-p^{1-s})}.$$

If we take the product over all p, we get

$$\zeta_C(s) = \prod_p \zeta_{C_p}(s) = \zeta(s)\,\zeta(s-1)/L_C(s),$$

where $\zeta(s)$ is the Riemann zeta function and

$$L_C(s) = \prod |1+(N_p-p-1)p^{-s}+p^{1-2s}|^{-1}.$$

Trivially, $L_C(s)$ is analytic for $\mathrm{Re}(s)>2$; Hasse has conjectured that $L_C(s)$ can be continued analytically over the whole plane. Formally,

$$L_C(1) = \prod (N_p/p)^{-1};$$

so it was natural for us to reformulate our conjecture as:

If $L_C(s)$ can be continued past $s=1$, then $L_C(s)$ has a zero of order g at $s=1$.

In general, this cannot be checked, as we know far too little about ζ_C. We looked at the particular case C_D: $y^2z = x^3 - Dxz^2$, where there is complex multiplication by i. In this case, there is an explicit formula for N_p in terms of quartic residues (see [9; 10]); so the relevant L-function $L_{C_D}(s)$, which we write $L_D(s)$ for short, turns out to be a Hecke L-series with Grossencharakter,

$$L_D(s) = \sum_{\sigma \equiv 1 (1+i)^3;\, \sigma \in \mathbf{Z}[i]} \left(\frac{D}{\sigma}\right)_4 \frac{\bar{\sigma}}{(\sigma\bar{\sigma})^s}.$$

By good fortune and with help from Davenport, we found that $L_D(1)$ may be evaluated explicitly in terms of the Weierstrass $\mathfrak{p}$-function satisfying $\mathfrak{p}'^2 = 4\mathfrak{p}^3 - 4\mathfrak{p}$, with periods ω, $i\omega$; for instance, if $D>1$ and $D \equiv 1$ (4) then

$$L_D(1) = \frac{\omega}{D} \sum \left(\frac{\beta}{D}\right)_4 \frac{\mathfrak{p}}{\mathfrak{p}^2 - 2\mathfrak{p} - 1},$$

where the sum is over a set of representatives β of the Gaussian integers modulo D, and $\mathfrak{p}$ is short for $\mathfrak{p}(\beta\omega/D)$.

Using this apparent analogue of a Gauss sum, we computed $L_D(1)$ in

about 2000 cases; in all cases that could be checked, our conjecture that $L_D(1)=0$ if and only if $g>0$ was confirmed. But we had a surprise; our computations indicated that

If $D>1$ and $4\nmid D$, then $\sigma(D)=D^{1/4}L_D(1)/\omega$ and $\sigma(-D)=(4D)^{1/4}L_{-D}(1)/\omega$ are integers.

Once one guesses that this is likely to be true, it is in fact rather easy to prove with a bit of classifield theory—essentially Kronecker's Jugendtraum. Rather more appears to be true, namely that $\sigma(D)\geqq 0$, and $\sigma(D)$ is a power of 2 times a square, but this we have not proved. (We have not even shown that $\sigma\geqq 0$, which is formally obvious.)

How should one interpret the integer $\sigma(D)$? It seems that we are constructing an analogue of the Tamagawa number of an algebraic group (see Weil [29], Ono [19; 20; 21], Borel [2]); our analogue is actually somewhat simpler than the original. Let us consider C in affine form, $y^2=x^3-ax-b$; then C has a Haar measure given by the differential dx/y. We define the Tamagawa measure of C formally by $\tau(C)=\int_{C(\infty)}dx/y\cdot\prod_p\int_{C(p)}|dx/y|_p$, where $\int_{C(\infty)}$ is over all real and $\int_{C(p)}$ over all p-adic points of C. Note that taking a different differential adx/y makes no difference, by the product formula. We call a prime p *good* if p is finite and the mod p reduction C_p has genus 1; if $p=\infty$ or if C_p is no longer an elliptic curve we call p *bad*; so the bad primes are just the factors of $(4a^3-27b^2)\infty$. Then for good primes $\int_{C(p)}=N_p/p$, so for the particular curve $C_D: y^2=x^3-Dx$ we have

$$\tau(C_D)=\prod_{p\mid 2D\infty}\int_{C(p)}|dx/y|_p\cdot(L_D(1))^{-1}.$$

The factors other than $L_D(1)$ are easily computed; in all cases that we can check we find that

$$\text{if } g=0, \text{ then } \tau(C_D)=f^2/|TS|.$$

Here f is as before the number of points of finite order of C_D, and $|TS|$ is the conjectured order of the Tate-Šafarevič group. I must explain this briefly. (The standard presentation is that given by Lang and Tate [15].)

In order to compute A/nA, one uses the method of descent. Following Cassels [4; 5], I like to do this in terms of coverings. An n-covering consists of a curve D defined over Q, together with a commutative triangle

$$\begin{array}{ccc} C & \xrightarrow{\times n} & C \\ \iota\,\downarrow & \nearrow_{\pi} & \\ D & & \end{array}$$

with associated generic points

$$\begin{array}{ccc} x_1 & \longrightarrow & x=nx_1 \\ \downarrow & \nearrow & \\ X & & \end{array}\quad;$$

the rational map $X \to x$ is defined over Q, and the map $X \leftrightarrow x_1$ is a birational equivalence but only defined over the algebraic closure $\bar{Q}$. Two n-coverings given by D, D' are equivalent if there is a birational equivalence over Q between their generic points X, X' such that the obvious diagram with $x = nx_1 = nx_1'$ commutes. Equivalence classes of n-coverings form a group (as is seen most easily by identifying them as elements of a homology group $H^1(G_{\bar{Q}/Q}, \Delta_n)$, see [15]); there is a natural isomorphism between A/nA and the subgroup consisting of classes such that D has a rational point.

Unfortunately, this subgroup is not effectively computable, as one has no certain method of telling whether a curve D has a point or not; the best we can do at present is to compute what Cassels calls the Selmer group, $S^{(n)} \cong$ |*Classes of coverings for which D has a point in every completion of Q*|. The Selmer group is a finite computable object, computable in the logical sense and also in the more practical sense that there is a working machine program |1| for computing $S^{(2)}$. So, for each n, $S^{(n)}$ gives us a computable upper bound, call it $\nu(n)$, for g ($\nu(n)$ is the rank of the group $\Sigma^{(n)}$ obtained by factoring out the image of the torsion subgroup of A from $S^{(n)}$.)

Selmer |22| found experimentally that the difference $\nu(n) - g$ was always even; this has been partly explained in an important series of papers |3; 4; 5; 6; 7| by Cassels. Cassels shows inter alia that $\nu(p^{r+1}) - \nu(p^r)$ is always even when p^r is a prime power; in view of this, Selmer's observation would follow from the very natural conjecture that

$$\nu(p^r) = g \text{ as soon as } r \text{ is large enough};$$

from now on, we call this stronger statement the Selmer conjecture.

Since A/nA is mapped to a subgroup of $S^{(n)}$, we can form an exact sequence $0 \to A/nA \to S^{(n)} \to (TS)_n \to 0$. Then $(TS)_n$ measures the difference between A/nA and $S^{(n)}$; it is the part of the Tate-Šafarevič group TS consisting of elements whose order divides n. We get the whole of the Tate-Safarevič group by using the inclusion $(TS)_n \subseteq (TS)_m$ if $n|m$ and taking limits.

The so-called Tate-Šafarevič conjecture (adopted by Lang, Cassels and Tate, but apparently disowned by Šafarevič) asserts that TS is always a finite group; this is a very natural strengthening of the Selmer conjecture. Unfortunately, the evidence is very weak; in fact, TS has not yet been fully computed for a single curve. It is very difficult to compute more than $(TS)_2$ for a general elliptic curve over Q, and $(TS)_3$ for a curve of shape $y^2 = x^3 - B$. Cassels' theorem implies that if TS is finite then its order must be a square. In our computations leading to the formula

$$\text{“}\tau(C_D) = f^2/|TS| \text{ if } g = 0\text{”}$$

we actually verified that $f^2/\tau(C_D)$ was an integer square, usually 1, and was divisible by the order of $(TS)_n$ when this could be calculated.

There is one attractive way in which the formula $\tau(C) = f^2/|TS|$ has

been tested by Cassels. Suppose that C, C' are l-isogenous over Q, so that there are rational maps

$$C \xrightarrow{\lambda} C' \xrightarrow{\lambda'} C$$

with $\lambda'\lambda$ a multiplication by l on C, and $\lambda\lambda'$ a multiplication by l on C'. Suppose that l is prime. We may estimate $|A/lA|$ by means of $|A/\lambda' A'|$ and $|A'/\lambda A|$. It is enough to describe the estimation of $|A/\lambda' A'|$; we do this by means of λ'-coverings: let $S^{(\lambda')}$ correspond to $A/\lambda' A'$ as $S^{(n)}$ corresponds to A/nA, then the order of $S^{(\lambda')}$ gives an estimate for $|A/\lambda' A'|$. Between them, $S^{(\lambda)}$ and $S^{(\lambda')}$ give an estimate $\nu(\lambda)+\nu(\lambda')$ for g (the "number of first descents," in the classical terminology); for $l=2$, this estimate is very easy to obtain, even by hand. Using the methods of [5] one can show without real difficulty that $\nu(l) \equiv \nu(\lambda)+\nu(\lambda') \pmod 2$.

Returning to our formula, C and C' taken modulo p have the same number of points for all good p, so the Tamagawa ratio

$$\tau(C)/\tau(C') = \prod_{\text{bad } p} \int_{C^{(p)}} \Big/ \int_{C'^{(p)}}$$

is in fact a finite product taken over $p=\infty$ and those primes for which one of C, C' has a bad reduction. According to our formula, we should have $\tau(C)/\tau(C') = |f^2(C)/f^2(C')\,|\,|TS(C')|/|TS(C)|\,|$; here both sides are elementary, so it ought to be possible to verify this.

This Cassels has done. In fact, with the above notations, l prime, but g not necessarily zero, he proves that

$$\tau(C)/\tau(C') = |S^{(\lambda')}/S^{(\lambda)}| \cdot |\ker\lambda'/\ker\lambda|;$$

when $g=0$ and TS is finite, this gives the identity we require; the analogue with the work of Ono [21] is very striking. There is another deduction to be made from Cassels' formula. Let us assume the Selmer conjecture; then $g \equiv \nu(l) \equiv \nu(\lambda)+\nu(\lambda') \pmod 2$; so the parity of g is determined by the Tamagawa ratio. This ratio is easy to compute, and whether it is an odd or an even power of l is essentially a matter of congruences; for instance, for the curve C_D: $y^2=x^3-Dx$ it depends on the residue class of D mod 16, on the sign of D, and on the number of primes $\equiv 3 \pmod 4$ whose squares divide D exactly. So the Selmer conjecture leads to a simple sufficient condition determining a very large class of curves with infinitely many rational points.

There are several other ways in which our conjectures should be tested. I have described the results obtained for the particular class of curves $y^2=x^3-Dx$, with complex multiplication by i. The other complex multiplication cases (see Deuring [10]) may be checked; in particular, fairly extensive results consistent with our conjectures have been obtained by N. M. Stephens using ATLAS for the Selmer case $y^3=x^3-D$, with complex multiplication by $\sqrt{(-3)}$.

There is another class of elliptic curves with good zeta-function, as Shimura has kindly pointed out to me. Let $j(\tau)$ be the modular function; then for

any integer n, $j(n\tau)$ is algebraic over $Q(j(\tau))$; so $Q(j(\tau), j(n\tau))$ is the function field of a curve, call it Γ_n for short. This curve has been investigated by Fricke [12], who describes twelve cases ($n = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49$) in which Γ_n has genus 1; write J_n for the Jacobian curve of Γ_n. (J_n is equivalent to Γ_n except when $n = 17$, when Γ_{17} appears to be a 2-covering of J_{17}.) The zeta-function of J_n may be identified (see Shimura [24]) as an Euler product investigated by Hecke [13], and may be continued meromorphically over the whole plane. As Shimura points out, $L_J(1)$ is an integral of a modular function, and is certainly positive; so according to our conjecture J_n should have only finitely many points. Fortunately, this seems to be so; it is fairly easy to verify in the nine cases where n is composite. (In these cases, J_n has a rational point of order 2, so we can find another curve 2-isogenous to J_n; one can then show that J_n has only finitely many points by computing λ-coverings.) Shimura also exhibited a large class of curves related to J_n (equivalent to J_n over $Q(D^{1/2})$ but not over Q) for which $L(1) = 0$; for n composite, one presumes that these are cases in which Cassels' theorem on the Tamagawa ratio predicts that the number of generators should be odd.

Finally, what if g is positive? Here, nothing is known yet, but one can make guesses; Tate has given a fairly detailed conjecture. One feels that $L_C(s)/(s-1)^g$ at $s = 1$ should give a measure of the density of rational points on the curve C; so first one must decide how to measure this density. To do this, one needs a canonical measure for the size of the generators of A. This has been provided; I can give no reference beyond a letter from Tate to Cassels. The idea arises very naturally, for instance, from Lang's discussion of heights in his book on Diophantine geometry [14]. Let $h(P)$ be any sensible measure of height; if for instance P is the point (x, y, z) with x, y, z coprime integers satisfying $y^2z = x^3 - axz^2 - bz^3$, one might take $h(P) = |x| + |y| + |z|$ or $\max(|x|, |y|, |z|)$. Then $\lim[n^{-2} \log h(nP)]$ exists; call this limit $H(P)$. Then $H(P)$ is a canonical measure of the height of a point; it is in fact a quadratic form on A, and may be computed explicitly — it is bound up with the Weierstrass σ-function. Tate suggests an analogue of the classical class number formula (and of Ono's formula for algebraic tori) in which the determinant of the quadratic form H takes the place of the regulator, and in which the order of TS takes the place of the class number.

I have not attempted to cover more than a corner of the theory of elliptic curves; for a wider survey with an excellent list of references, I refer to Cassels [8], and for the associated Galois cohomology I refer to Tate [26]. In a footnote, Cassels refers to valuable work of Serre [23], which has subsequently become available.

References

1. B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves*. I, J. Reine Angew. Math. 212(1963), 7-25.

2. A. Borel, *Arithmetic properties of linear algebraic groups*, Proc. Internat. Congress Math. (Stockholm 1962), pp. 10-22.

3. J. W. S. Cassels, *Arithmetic on curves of genus* 1. I. *On a conjecture of Selmer*, J. Reine Angew. Math. **202**(1959), 52-99.

4. ———, *Arithmetic on curves of genus* 1. II. *A general result*, ibid. **203**(1960), 174-208.

5. ———, *Arithmetic on curves of genus* 1. III. *The Tate-Šafarevič and Selmer groups*, Proc. London Math. Soc (3) **12**(1962), 259-296.

6. ———, *Arithmetic on curves of genus* 1. IV. *Proof of the Hauptvermutung*, J. Reine Angew. Math. **211**(1962), 95-112.

7. ———, *Arithmetic on curves of genus* 1. V. *Two counter examples*, J. London Math. Soc. **38**(1963), 244-248.

8. ———, *Arithmetic on an elliptic curve*, Proc. Internat. Congress Math. (Stockholm 1962), pp. 234-246.

9. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172**(1934), 151-182.

10. M. Deuring, *Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins*. I, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. Math.-Phys.-Chem. Abt. (1953), 85-94; II, Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa **1955**, 13-42; III, ibid. **1956**, 37-76; IV, ibid. **1957**, 55-80.

11. B. Dwork, *A deformation theory for the zetafunction of a hypersurface*, Proc. Internat. Congress Math. (Stockholm 1962), pp. 247-259.

12. R. Fricke, *Die Elliptischen Funktionen*, Vol. 2, pp. 335-458, Teubner, Leipzig and Berlin, 1922.

13. E. Hecke, *Über Modulfunktionen und die Dirichletschen Riehen mit Eulerscher Produktentwicklung*. I, Math. Ann. **114**(1937), 1-28; II, ibid. **114**(1937), 316-351.

14. S. Lang, *Diophantine geometry*, Interscience, New York and London, 1962.

15. S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80**(1958), 659-684.

16. E. Lutz, *Sur l'équation* $y^2 = x^3 - Ax - B$ *dans les corps* $\mathfrak{p}$*-adiques*, J. Reine Angew. Math. **177**(1937), 237-247.

17. L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Philos. Soc. **21**(1922), 179-192.

18. T. Nagell, *Solution de quelques problèmes dans la théorie arithmetique des cubiques planes du premier genre*, Vid. Akad. Skrifter Oslo I (1935), No. 1.

19. T. Ono, *On some arithmetic properties of linear algebraic groups*, Ann. of Math. **70**(1959), 266-290.

20. ———, *Arithmetic of algebraic tori*, ibid. **74**(1961), 101-139.

21. ———, *On the Tamagawa number of algebraic tori*, ibid. **78**(1963), 47-73.

22. E. S. Selmer, *The diophantine equation* $ax^3+by^3+cz^3=0$, Acta Math **85**(1951), 203-362; *The diophantine equation* $ax^3+by^3+cz^3=0$. *Completion of the tables*, ibid. **92**(1954), 191-197.

23. J.-P. Serre, *Sur les groups de congruence des variétés abéliennes*, mimeographed notes.

24. G. Shimura, *Correspondances modulaires et les fonctions* ζ *de courbes algébriques*, J. Math. Soc. Japan **10**(1958), 1-28.

25. ———, *On the zeta-functions of the algebraic curves uniformised by certain automorphic functions*, J. Math. Soc. Japan **13**(1961), 275-331.

26. J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congress Math. (Stockholm 1962), pp. 288-295.

27. A. Weil, *Sur un théorème de Mordell*, Bull. Sci. Math. (2) **54**(1930), 182-191.

28. ———, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55**(1949), 497-508.

29. ———, *Adelès and algebraic groups*, Lecture notes, Institute for Advanced Study, Princeton, N. J., 1961.

UNIVERSITY OF MANCHESTER