CONJECTURES CONCERNING ELLIPTIC CURVES

BY N. M. STEPHENS[1]

Communicated by A. Mattuck, March 14, 1966

1. The elliptic curve

$$\Gamma_D: X^3 + Y^3 = DZ^3,$$

where D in a cube-free positive integer, admits complex multiplication by $(-3)^{1/2}$. By the Mordell-Weil theorem, the group of rational points on Γ_D has a finite number of independent generators of infinite order, g say. The zeta-function of Γ_D has the form

$$\zeta(s)\zeta(s-1)/L_D(s),$$

where $\zeta(s)$ is the Riemann zeta-function and $L_D(s)$ is a Hecke L-series. Denote by $L_D'(s)$ the derivative of $L_D(s)$ with respect to s.

This note is a description of some numerical results obtained for the values of $L_D(1)$ and $L_D'(1)$ for many D, with special reference to the conjectures of Birch and Swinnerton-Dyer, [1]. In particular, when $g=1$, the value of $L_D'(1)$ is compared with a canonical measure for the density of the rational points on Γ_D. With the aid of further computations of second and third derivatives of $L_D(s)$ for a few values of D, a relation can be conjecturally formulated as

$$L_D^{(g)}(1)/f = g!\gamma\kappa/\eta^2.$$

Here, f is a product of factors due to "bad" primes, γ the order of the Tate-Šafarerič group, κ the inverse of the measure of the density, and η the number of points on Γ_D of finite order.

2. The conjectures of Birch and Swinnerton-Dyer, [1], are stated for general elliptic curves, especially for those which admit complex multiplication. They will be restated here for the curve Γ_D only.

CONJECTURE 1. *$L_D(s)$ has a zero at $s=1$ of order precisely g.*

For all cube-free D of the form 2^r3^sM, where r, $s=0$, 1, 2 and where M is such that the product of its distinct prime divisors ($\neq 2$, 3) is less than 100 (676 D in all), the values of $L_D(1)$ and $L_D'(1)$ were computed from approximation formulae. It can be shown that $L_D(1)$ is the product of a rational integer and a predictable factor, so that any

[1] These results are part of the author's doctoral thesis submitted to Manchester University, England, in 1965. The author wishes to thank Dr. B. J. Birch for his guidance.

reasonably good approximation is sufficient. The value of $L_D'(1)$ when $L_D(1)$ is nonzero can be found explicitly by using the functional equation; hence the error involved in the approximation formula could be calculated for those D and was found to be within $\pm 0.1\%$—but the difference between actual and computed values was never more than 0.01. The group of rational points on Γ_D has been determined explicitly by Selmer [5], for all $D<500$ and his method of 3-descents has been used for all $D>500$ of the above form.

Within the experimental errors already referred to and for those curves where g could be determined, it is found that:

(1) $L_D(1)=0$ if and only if $g\geqq 1$;

(2) $L_D'(1)=0$ if and only if $g\geqq 2$.

A summary table is included in §4.

The "integer" property of $L_D(1)$ leads to the construction of the analogue of the Tamagawa number, τ, for the group of rational points on Γ_D, in precisely the same way as Birch and Swinnerton-Dyer constructed it for the curves with complex multiplication by $(-1)^{1/2}$. Essentially

$$\tau = f/L_D(1),$$

where f is a factor due to "bad" primes.

CONJECTURE 2. *Let η be the number of rational points of finite order on Γ_D and let γ be the order of the Tate-Šafarerič group of Γ_D. Then*

$$L_D(1)/f = \gamma/\eta^2 = 1/\tau.$$

When $g=0$, the computed values of $L_D(1)$ support this conjecture in the sense that γ is the square of an integer and that γ is divisible by exactly the right powers of 2 and 3 whenever it is easy to check. There is further corroboration when the curve isogenous to Γ_D is also considered; for then the γ's, for any particular D, differ only by a multiple of an integral power of 9. In fact, for most of the curves Γ_D, and the curves isogenous to Γ_D, γ is 1; the other values found are 4, 9, 16, 25, 36, 81 and 144.

3. It remains to give an account of the interpretation of the non-zero value of $L_D'(1)$, when $g=1$, in terms of the canonical heights of the basic generators; for an account of the Tate-Néron canonical height, see Néron [3], or Cassels [2].

For the curve Γ_D, an explicit formula for the Tate-Néron height of a rational point has been given by Birch (unpublished). By means of a birational transformation, Γ_D may be rewritten in the general form for an elliptic curve:

$$\Gamma_D: y^2z = x^3 - 2^4 3^3 D^2 z^3.$$

Suppose $\bar{\Gamma}_D$ has a point (x, y, z) where x, y and z are integers in their lowest form. Denote (x, y, z) by $P(u)$ where u is a real elliptic argument such that

$$\wp(u) = \frac{x}{2^2 3 D^{2/3} z^2};$$

here, $\wp(u)$ is the Weierstrass $\wp$-function satisfying

$$\wp'^2(u) = 4\wp^3(u) - 1.$$

Write (x_n, y_n, z_n) for the coordinates of the point $P(nu)$. Then the canonical height $\hat{h}(u)$ may be defined as

$$\hat{h}(u) = \lim_{n\to\infty} \frac{1}{n^2} \max (|x_n|, |y_n|, |z_n|).$$

If n is an integer such that $(x_n, 6D) = 1$, then explicitly

$$\hat{h}(u) = \frac{1}{n^2} \left\{ \log_e \left(\frac{2^2 3 D^{2/3} z_n^2}{\sigma^2(nu)} \right) + \frac{\pi}{2 \cdot 3^{1/2}} (nu)^2 \right\}$$

where $\sigma(u)$ is the Weierstrass σ-function; the right-hand side is well defined, is independent of n, and behaves like a quadratic form.

Hence, if Γ_D has g generators, $P(u_1), \cdots, P(u_g)$, say, there exist h_{ij} $(i, j = 1, \cdots, g)$ such that for all $a_1, \cdots, a_g$,

$$\hat{h}(a_1 u_1 + \cdots + a_g u_g) = \sum_{i,j=1}^{g} h_{ij} a_i a_j.$$

The inverse of the determinant, $\det(h_{ij})$, is then a good measure for the density of rational points on the curve; the value of the determinant for Γ_D is denoted by κ.

There are a large number of curves with $g = 1$; all the numerical evidence points to

$$L'_D(1)/f = \gamma\kappa/\eta^2.$$

In order to see how this formula generalizes, $L_D^{(g)}(1)$ was computed in four cases when $g = 2$ and one when $g = 3$. The accuracy for these derivatives is bad (about $\pm 2\%$; it can be determined by using the functional equation in much the same way as before), but, within these terms of error, there are reasonable grounds for supposing that

$$L_D^{(g)}(1)/f = g!\gamma\kappa/\eta^2.$$

In terms of Conjecture 1, which may be restated as

$$L_D(s) \sim C(s - 1)^g,$$

this means that

$$C = f\gamma\kappa/\eta^2;$$

this is in essence a formula suggested by Tate and others, by analogy with the work of Ono [4].

The values of γ which occur in the one generator case are usually 1, but there are cases when γ is 4 or 9. The power of 3 in γ (or lack of it) is always predictable and in some cases so too is the power of 2. All the results are consistent with the conjectures.

4. The numerical evidence relating to the order of the zero of $L_D(s)$ at $s=1$ is summarized below in Table 1. It was not possible in every case to determine g. The curves headed $g \leqq 1$ are thought in fact to have $g=1$ with a large basic solution (corresponding to a large value of $L_D'(1)$); the curves headed $g \leqq 2$ are thought to have $g=0$, despite everywhere locally possible descents. The latter have the conjectured value of γ divisible by 9 both for the curve Γ_D and its isogenous curve.

It is impossible to show how compelling the evidence is which relates $L_D'(1)$ and κ, when $g=1$, without presenting a full table. At present, may it suffice to say that $\eta^2 L_D'(1)/f\gamma$ ranges from 0.298 to over 200; in almost all cases where it is less than 50, the generator has been found and κ turns out to be correct within $\pm .01$. For $\kappa=50$ the value of X in the basic solution will be of the order 10^{32}.

It is hoped that full details will be published soon elsewhere.

TABLE 1

No. of curves considered with $g=$	0	1	2	3	$\leqq 1$	$\leqq 2$
No. of curves with $L_D(1)\neq 0, L_D'(1)\neq 0$	262	0	0	0	0	16
No. of curves with $L_D(1)=0, L_D'(1)\neq 0$	0	297	0	0	43	0
No. of curves with $L_D(1)=0, L_D'(1)=0$	0	0	56	2	0	0

REFERENCES

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

2. J. W. S. Cassels, *Survey Article: Diophantine equations with special reference to elliptic curves*, J. Jondon Math. Soc. 41 (1966), 193–291.

3. A. Néron, *Quasi fonctions et hauters sur les variétés abéliennes*, Ann. of Math. 82 (1965), 249–331.

4. T. Ono, *On the Tamagawa number of algebraic tori.* Ann. of Math. (2) 78 (1963), 47–72.

5. E. S. Selmer, *The Diophantine equation* $ax^3+by^3+cz^3=0$, Acta Math. 85 (1951), 203–362.

UNIVERSITY OF EAST ANGLIA, ENGLAND