The Conjectures of Birch and Swinnerton-Dyer, and of Tate

P. SWINNERTON-DYER

1. Introduction

In the last few years, it has become increasingly evident that the study of the zeta-function of an algebraic variety can yield valuable information about that variety, some of which cannot easily be obtained in any other way. Most of this information is number-theoretic – that is to say, it refers to objects which depend on the ground field and which are only of interest when the ground field is finitely generated. But some of it refers to objects, such as the Néron-Severi group, which are also of interest to classical algebraic geometers – and about which classical algebraic geometry has little to say.

The first indication of this should have been the pre-war work of SIEGEL on quadratic forms. Indeed Siegel himself wrote of that work that he hoped it would rescue the zeta-function from the neglect into which it was falling. But the influence of fashion, and the deeper and apparently more elegant reformulation of Siegel's work by TAMAGAWA in terms of measure theory, led to a general belief that zeta-functions were not essentially involved in Siegel's results.

Siegel's theorems were rigorously proved. Most of the subsequent work is conjecture, based on the examination of special cases and on ex post facto heuristic arguments which have been adequately described elsewhere. The next step was the conjecture of BIRCH and SWINNERTON-DYER, which connected the behaviour of the zeta-function of an elliptic curve at $s=1$ with its number-theoretic properties. Here the zeta-function is inescapably involved, both because its behaviour at $s=1$ can only be obtained by analytic continuation and because the conjecture involves not only its leading coefficient but the order of its pole at $s=1$.

Most of the subsequent work is due to, or inspired by, TATE. He has

put forward, and produced evidence for, conjectures which extract a good deal of information from the zeta-function of any algebraic variety; and for surfaces over finite fields he and ARTIN have gone far towards proving these conjectures.

2. Elliptic curves over Q

We define an 'elliptic curve' to be an Abelian variety of dimension 1. Thus an elliptic curve over a field k is a complete non-singular curve of genus 1 which is defined over k and which contains a distinguished point $\mathfrak{d}$ also defined over k; the curve then has the structure of an additive group whose zero is $\mathfrak{d}$, and the group law is defined over k. We shall denote by Γ an elliptic curve over $\mathbf{Q}$, the field of rational numbers. The restriction to $\mathbf{Q}$ is needed for the computations described in §§ 3 and 4; the theoretical results quoted in the present section hold, with trivial changes of notation, over an arbitrary algebraic number field.

To state Conjectures A and B, we must first define a satisfactory global L-series, or, which comes to the same thing, a satisfactory global zeta-function associated with Γ. The crude way to produce a global zeta-function is to multiply together the local zeta-functions for all 'good' primes; this gives an Euler product with finitely many factors apparently missing. For an elliptic curve, though not for a general Abelian variety, the correct form for these missing factors is known. However, the conjectures are only concerned with the behaviour of the zeta-function near $s=1$, and instead of supplying the missing factors as functions of s it is therefore only necessary to supply their values at $s=1$. We now show how to do this.

Let ω be a differential of the first kind on Γ. If Γ is written in the traditional form

$$y^2 = x^3 - Ax - B$$

then we can choose $\omega = dx/2y$; in any case ω is unique up to multiplication by a non-zero rational number, and the choice of this number does not affect what follows. For almost all primes p, Γ and ω both have non-degenerate reductions modulo p; hence they give rise to an elliptic curve Γ_p defined over $GF(p)$, the finite field of p elements, and a differential of the first kind ω_p on Γ_p. The zeta-function of Γ_p over $GF(p)$ is

$$\zeta_p(\Gamma_p, s) = \frac{(1 - \alpha_p p^{-s})(1 - \bar{\alpha}_p p^{-s})}{(1 - p^{-s})(1 - p^{1-s})}; \tag{2.1}$$

here α_p, $\bar{\alpha}_p$ are defined by the statement that for $q=p^n$ there are just

$$N_q = p^n - \alpha_p^n - \bar{\alpha}_p^n + 1 \tag{2.2}$$

points on Γ_p defined over $GF(q)$. From the local zeta-functions (2.1) we can form a crude global L-series

$$L(\Gamma, s) = \prod \{(1 - \alpha_p p^{-s})(1 - \bar{\alpha}_p p^{-s})\}^{-1},$$

the product being taken over those primes p for which Γ has a good reduction modulo p. The product is only known to converge in $\Re s > \frac{3}{2}$; but Weil has conjectured that $L(\Gamma, s)$ can be analytically continued over the whole complex plane, and that there is a functional equation connecting $L(s)$ and $L(2-s)$. In what follows, it will be assumed that $L(s)$ is at any rate well defined in some neighbourhood of $s=1$.

Let S be a finite set of primes which contains the infinite prime and any finite prime modulo which Γ or ω does not have a good reduction. For any finite prime p, whether in S or not, we can form

$$M_p(\Gamma) = \int_{\Gamma(\mathbf{Q}_p)} |\omega|_p \mu_p \tag{2.3}$$

where $\mathbf{Q}_p$ is the field of p-adic numbers, $\Gamma(\mathbf{Q}_p)$ is the set of points on Γ defined over $\mathbf{Q}_p$, $|\ |_p$ is the usual p-adic valuation, and μ_p is the usual Haar measure on $\mathbf{Q}_p$ which assigns measure 1 to the set of p-adic integers. For the infinite prime we replace (2.3) by

$$M_\infty(\Gamma) = \int \omega$$

taken over all real points on Γ. Now write

$$L_S^*(\Gamma, s) = \prod_{p \in S} \{M_p(\Gamma)\}^{-1} \prod_{p \notin S} \{(1 - \alpha_p p^{-s})(1 - \bar{\alpha}_p p^{-s})\}^{-1}. \tag{2.4}$$

It is easily verified that for fixed S this does not depend on the particular choice of ω. Moreover, it does not depend significantly on the choice of S; for if S_1, S_2 are two such sets then

$$L_{S_1}^*(\Gamma, s)/L_{S_2}^*(\Gamma, s) \to 1 \quad \text{as} \quad s \to 1.$$

To prove this it is enough to note that if Γ and ω both have a good reduction modulo p then

$$M_p(\Gamma) = N_p/p = (1 - \alpha_p p^{-1})(1 - \bar{\alpha}_p p^{-1}). \tag{2.5}$$

Henceforth we shall denote by $L^*(\Gamma, s)$ any Euler product which differs

from $L(\Gamma, s)$ only in finitely many factors and which satisfies

$$L^*(\Gamma, s)/L_S^*(\Gamma, s) \to 1 \quad \text{as} \quad s \to 1\,. \tag{2.6}$$

Note that we do not adopt the usual normalization condition that $L^*(\Gamma, s) \to 1$ as $s \to +\infty$, preferring instead to normalize at $s=1$.

We next define the Tate-Šafarevič group Ш and the Weil-Chatelet group WC; only the former of these occurs in the conjectures, but it is natural to describe both together. Let $\mathscr{S}$ be the set of all principal homogeneous spaces over Γ; in other words, an element of $\mathscr{S}$ is a complete non-singular curve C of genus 1 defined over $\mathbf{Q}$, together with a specific identification of Γ with its Jacobian. (Note that because Γ has non-trivial automorphisms, the curve C does not in itself determine the canonical map $C \times C \to \Gamma$.) For any two elements C_1, C_2 of $\mathscr{S}$, write $C_1 \sim C_2$ if there exists a birational map $C_1 \to C_2$ defined over $\mathbf{Q}$ for which the diagram

$$\begin{array}{ccc} C_1 \times C_1 & \to & C_2 \times C_2 \\ & \searrow \quad \swarrow & \\ & \Gamma & \end{array}$$

is commutative. This defines an equivalence relation in $\mathscr{S}$; and the set of equivalence classes in $\mathscr{S}$ is called the Weil-Chatelet set associated with Γ. It can be given the structure of a commutative group in a natural way; for the details see WEIL [*31*]. This group is a torsion group, and its identity element is the equivalence class consisting of all curves C which contain a rational point. Like most sets which unexpectedly have a natural group structure, it can also be defined as a cohomology group; it is $H^1(G, \Gamma(\overline{\mathbf{Q}}))$, where $\overline{\mathbf{Q}}$ is the algebraic closure of $\mathbf{Q}$ and G is the Galois group of $\overline{\mathbf{Q}}/\mathbf{Q}$.

Now consider those curves C in $\mathscr{S}$ which contain points defined over each p-adic field including the reals; these are just the curves which can play a significant part in an 'infinite descent' argument applied to Γ. Such curves precisely fill a certain number of equivalence classes in $\mathscr{S}$, and these classes form a subgroup of WC called the Tate-Safarevič group Ш. Unfortunately, very little is known about Ш, and there is no curve Γ for which it has completely determined. It is conjectured that it is always a finite group; and CASSELS [*5*] has shown that when it is finite its order must be a perfect square. It can be shown that Ш only contains finitely many elements of any given order; and the bound for the number of these elements, for a given Γ, is moderate and in principle constructive. There is no certain way of finding these elements, because there is no certain way of finding whether two curves in $\mathscr{S}$ are equivalent; in effect, this

comes down to determining whether a given curve C has a rational point. However, in practice one can usually find the elements of order 2 in Ш for any particular elliptic curve Γ, and the elements of order 3 or 4 for suitably chosen curves Γ, without intolerable labour.

In the description which follows, it will be implicitly assumed that Ш is finite. Conjectures A, B and C below, as they are stated here, do indeed each imply that Ш is finite; for each of them contains a formula in which the order of Ш appears. However, the evidence for these conjectures cannot really be regarded as evidence for the finiteness of Ш. In fact, each of these formulae contains a term which is certainly associated with Ш and whose value appears to be always a positive integer – and indeed a perfect square. It is natural to identify this term with the order of Ш; but one can give a more complicated interpretation of it which is equally compatible with the evidence and which would still make sense even if Ш were sometimes infinite.

MORDELL [*16*] has shown that $\Gamma(\mathbf{Q})$, the group of rational points on Γ, is finitely generated; and in any particular case his proof gives an explicit bound for the number of generators. It is easy to find the elements of finite order in $\Gamma(\mathbf{Q})$; see for example CASSELS [*6*], Theorem 22.1. There is no certain method of calculating g, the rank of $\Gamma(\mathbf{Q})$; but in practice one can usually find g without intolerable labour by the method of infinite descent. BIRCH and SWINNERTON-DYER [2] have given an alternative method of conducting the first descent, which avoids any use of algebraic number fields and is therefore suitable for machine computation. Moreover, on the assumption that Ш is finite CASSELS [*5*] has shown that the difference between the number of first descents and the value of g is even; thus the parity of g can be found even when g itself cannot.

We can now state the initial conjecture of BIRCH and SWINNERTON-DYER [*3*]. This can be regarded primarily as giving a necessary and sufficient condition for $g=0$ – that is, for $\Gamma(\mathbf{Q})$ to be finite.

Conjecture A. *With the notation and definitions above,*

$$L^*(\Gamma, 1) = \begin{cases} [Ш]/[\Gamma(\mathbf{Q})]^2 & \text{if } g = 0, \\ 0 & \text{otherwise,} \end{cases}$$

where square brackets denote the order of a group.

To produce a more detailed conjecture when $g>0$ we need a measure of the density of the rational points on Γ. We first define the height of a rational point on Γ, following the original approach of TATE as described in [*15*]. Assume that Γ is embedded in projective space, and fix a system

of co-ordinates in that space. For any rational point P on Γ, write

$$h(P) = \log(\max\{|x_0|, |x_1|, \ldots, |x_n|\})$$

where $(x_0, x_1, \ldots, x_n)$ is that representation of P for which the x_i are integers with no common factor. If nP denotes the sum of n copies of P under the standard addition law on Γ, then

$$\hat{h}(P) = \lim_{n\to\infty} n^{-2} h(nP)$$

exists and is called the height of P. Moreover $\hat{h}(P)$ behaves like a quadratic form, does not depend on the choice of a co-ordinate system in the ambient projective space, and vanishes at just those points of $\Gamma(\mathbf{Q})$ which are of finite order. We can derive from $\hat{h}(P)$ the bilinear form

$$\hat{h}(P, P') = \tfrac{1}{2}\{\hat{h}(P + P') - \hat{h}(P) - \hat{h}(P')\}.$$

The effect of a birational transformation of Γ is to multiply $\hat{h}$ by a constant; henceforth we normalize $\hat{h}$ by taking Γ to be a non-singular plane cubic curve. BIRCH has given an explicit formula (quoted in [25]) for $\hat{h}(P)$ for curves of the form

$$x^3 + y^3 = Dz^3 \tag{2.7}$$

and presumably this can be modified to be valid for all elliptic curves.

Now let $P_1, \ldots, P_g$ be a base for $\Gamma(\mathbf{Q})$ modulo torsion, and write

$$R = \det\{\hat{h}(P_i, P_j)\};$$

it is easy to show that R is positive and does not depend on the choice of base. The natural generalization of Conjecture A is as follows; it was first explicitly stated in STEPHENS [24], though its general shape had been suggested earlier.

Conjecture B. *With the notation and definitions above,*

$$L^*(\Gamma, s) \sim \frac{[Ш]\, R}{[\Gamma(\mathbf{Q})_{\text{tors}}]^2}(s-1)^g \quad as \quad s \to 1.$$

This of course includes Conjecture A; but so much of the evidence applies to the special case of Conjecture A that it is convenient to give both statements explicitly. There is no curve Γ for which Conjecture B has been proved to hold, because there is no curve for which Ш is completely determined; however, the supporting evidence is very strong. The direct evidence is of three kinds:

of co-ordinates in that space. For any rational point P on Γ, write

$$h(P) = \log(\max\{|x_0|, |x_1|, \ldots, |x_n|\})$$

where $(x_0, x_1, \ldots, x_n)$ is that representation of P for which the x_i are integers with no common factor. If nP denotes the sum of n copies of P under the standard addition law on Γ, then

$$\hat{h}(P) = \lim_{n\to\infty} n^{-2} h(nP)$$

exists and is called the height of P. Moreover $\hat{h}(P)$ behaves like a quadratic form, does not depend on the choice of a co-ordinate system in the ambient projective space, and vanishes at just those points of $\Gamma(\mathbf{Q})$ which are of finite order. We can derive from $\hat{h}(P)$ the bilinear form

$$\hat{h}(P, P') = \tfrac{1}{2}\{\hat{h}(P + P') - \hat{h}(P) - \hat{h}(P')\}.$$

The effect of a birational transformation of Γ is to multiply $\hat{h}$ by a constant; henceforth we normalize $\hat{h}$ by taking Γ to be a non-singular plane cubic curve. BIRCH has given an explicit formula (quoted in [25]) for $\hat{h}(P)$ for curves of the form

$$x^3 + y^3 = Dz^3 \tag{2.7}$$

and presumably this can be modified to be valid for all elliptic curves.

Now let $P_1, \ldots, P_g$ be a base for $\Gamma(\mathbf{Q})$ modulo torsion, and write

$$R = \det\{\hat{h}(P_i, P_j)\};$$

it is easy to show that R is positive and does not depend on the choice of base. The natural generalization of Conjecture A is as follows; it was first explicitly stated in STEPHENS [24], though its general shape had been suggested earlier.

Conjecture B. *With the notation and definitions above,*

$$L^*(\Gamma, s) \sim \frac{[Ш]\, R}{[\Gamma(\mathbf{Q})_{\text{tors}}]^2}(s-1)^g \quad as \quad s \to 1.$$

This of course includes Conjecture A; but so much of the evidence applies to the special case of Conjecture A that it is convenient to give both statements explicitly. There is no curve Γ for which Conjecture B has been proved to hold, because there is no curve for which Ш is completely determined; however, the supporting evidence is very strong. The direct evidence is of three kinds:

(i) invariance under isogeny;
(ii) calculations of $L^*(\Gamma, s)$ near $s=1$;
(iii) deductions from the functional equation of $L^*(\Gamma, s)$. Moreover, there is some analogy with the work of SIEGEL and TAMAGAWA on quadratic forms, and a close analogy with the work of ARTIN and TATE on surfaces over finite fields described in § 6 below.

Let Γ' be an elliptic curve which is isogenous to Γ over $\mathbf{Q}$. Cassels has shown that if Conjecture B holds for Γ it also holds for Γ'. All the terms in Conjecture B except for g are liable to change under isogeny. However, in each case the ratio between the values of a term for Γ and for Γ' is easier to determine than the two values themselves; in particular, the change in $L^*(\Gamma, s)$ comes entirely from the factors $M_p(\Gamma)$ corresponding to the bad primes. CASSELS' result is therefore a purely algebraic one, which does not involve s and which in particular throws no light on the problem of analytic continuation.

Experiment shows that $L^*(\Gamma, 1)$ cannot be satisfactorily calculated either by numerical analytic continuation or by setting $s=1$ in (2.4) and truncating the infinite product at a suitable point. It is known however that $L^*(\Gamma, s)$ can be analytically continued across $\Re s=\frac{3}{2}$ when one of two conditions holds; and in these cases $L^*(\Gamma, 1)$ can be calculated. These conditions are that Γ admits complex multiplication, discussed in § 3, or that Γ can be parametrized by elliptic modular functions, discussed in § 4. Here we consider just what the resulting figures show. Write

$$L^*(\Gamma, s) = a_0 + a_1(s-1) + a_2(s-1)^2 + \cdots.$$

It can be shown, under either condition, that $a_0 = L^*(\Gamma, 1)$ is a rational number, for whose denominator an explicit bound can be given; since it can be computed to any desired accuracy, it can be found exactly even though the computations themselves are not exact. By contrast, it is only practicable to compute the a_n with $n>0$ to two or three significant figures; and no theoretical statement about them is known. For curves with complex multiplication the numerical results are given in [3] and [24]. Of the 2024 curves for which $L^*(\Gamma, 1)$ has been calculated, there are 1744 for which the value of g is also known. Of these, 984 have $L^*(\Gamma, 1)=0$ and $g>0$, in accordance with Conjecture A; the other 760 have $g=0$ and $L^*(\Gamma, 1)>0$, and for these it is natural to use the formula of Conjecture A to give a hypothetical value of [Ш]. In each case the value is a perfect square, in accordance with the result of CASSELS [5]. Moreover, for each such curve either the 2-component or the 3-component of Ш was found

in the course of finding g; and these agree with the hypothetical values of [Ш]. There are 355 curves for which $g>0$ and both R and the a_n with $n>0$ have been calculated. These support the stronger Conjecture B, with the same interpretation of [Ш] as above, and with two minor reservations. Since the values of a_g and R are only approximate, so is that which is obtained for [Ш] from the formula. However this value is always close to a small integer, and so the hypothetical value of [Ш] is unambiguous. Again, for $g>1$ Conjecture B requires that $a_1=0$ and direct calculation can only show that this holds approximately. When $g=2$ we can use the functional equation for $L^*(\Gamma, s)$ and the exactly verifiable statement $a_0=0$ to prove that $a_1=0$; but in the two relevant cases when $g=3$ there is no known way to prove $a_1=0$, though the calculations make this plausible. As yet, there is only one curve without complex multiplication for which the value of $L^*(\Gamma, 1)$ is known. This case is fully described in § 4; it supports Conjecture A provided that Ш is trivial, which there is no reason to doubt.

In describing the functional equation, it is convenient to write

$$\Lambda^*(s) = (2\pi)^{-s}\,\Gamma(s)\,L^*(\Gamma, s). \tag{2.8}$$

WEIL has conjectured that for a suitable choice of the factors corresponding to the bad primes,

$$\Lambda^*(s) = \varepsilon f^{1-s}\,\Lambda^*(2-s). \tag{2.9}$$

Here $\varepsilon=\pm 1$ and f is the conductor of Γ, so that f is a product of suitable powers of the finite bad primes; for the precise definition of f see [*17*] or [*19*]. In general, no formula for ε is known; but DEURING has shown that if Γ admits complex multiplication then $L^*(\Gamma, s)$ is essentially a Hecke L-series with Großencharaktere, and hence (2.9) holds with an explicitly defined ε. Evidently $L^*(\Gamma, s)$ has a zero of odd order at $s=1$ if $\varepsilon=-1$, and of even order if $\varepsilon=+1$. According to Conjecture B, $L^*(\Gamma, s)$ has a zero of order g at $s=1$. For Γ of the form

$$y^2 = x^3 - Dx \tag{2.10}$$

or of the form (2.7), which correspond to the two simplest cases of complex multiplication, BIRCH and STEPHENS [*1*] have shown that the number of first descents is even when $\varepsilon=+1$ and odd when $\varepsilon=-1$; this supports the conjecture in view of the theorem of CASSELS quoted above, that provided Ш is finite the number of first descents has the same parity as g.

NERON [*17*] has given a birationally invariant theory of the reduction

of elliptic curves modulo p. This appears, inter alia, to give the right form for the factors of $L^*(\Gamma, s)$ corresponding to the bad primes; and I am indebted to TATE for pointing out to me that it also gives a simpler definition of the corresponding factors $M_p(\Gamma)$ than that of (2.3). In fact NERON shows that there is an essentially unique model for Γ of the form

$$Y^2 + \lambda XY + \mu Y = X^3 + \alpha X^2 + \beta X + \gamma \tag{2.11}$$

where $\lambda, \mu, \alpha, \beta, \gamma$ are integers and the discriminant of the equation (2.11) is as small as possible. For this model, every Γ_p is an irreducible curve. Write

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

with the α_p, $\bar{\alpha}_p$ of (2.1) if Γ_p is non-singular;

$$L_p(s) = (1 - p^{-s})^{-1}$$

if Γ_p has an ordinary double-point with distinct rational tangents;

$$L_p(s) = (1 + p^{-s})^{-1}$$

if Γ_p has an ordinary double point with irrational tangents; and

$$L_p(s) = 1$$

if Γ_p has a cusp. Moreover, let c_p be the number of irreducible components of multiplicity 1 in the Neron fibre associated with the reduction of (2.11) modulo p; thus $c_p = 1$ whenever Γ_p is non-singular. TATE has shown that

$$M_p(\Gamma) = c_p / L_p(1)$$

for all primes p, which generalizes (2.5). In view of this, the correct definition of $L^*(\Gamma, s)$ is presumably

$$L^*(\Gamma, s) = \{M_\infty(\Gamma) \prod c_p\}^{-1} \prod L_p(s).$$

Here the term in curly brackets has been introduced to preserve (2.6). According to SERRE, this is the L-series for which the functional equation (2.9) should hold.

3. Elliptic curves with complex multiplication

In this section we give an account of the calculation of $L^*(\Gamma, s)$ for curves of the form

$$y^2 = x^3 - Dx \tag{3.1}$$

where D is a rational integer which we can take to be fourth-power-free. Similar arguments apply to the other types of curve defined over $\mathbf{Q}$ which admit complex multiplication, but the formulae differ. Detailed calculations have also been carried out by STEPHENS [24] for the curves (2.7), and pupils of CASSELS are currently working on curves of the form

$$y^2 = x^3 + 4Ax^2 + 2A^2x$$

which admit complex multiplication by $\sqrt{(-2)}$.

For the curve (3.1) the bad primes are just those which divide $2D$. For any other prime p it is known that

$$N_p = \begin{cases} p + 1 - \bar{\pi}\left(\frac{D}{\pi}\right)_4 - \pi\left(\frac{D}{\bar{\pi}}\right)_4 & \text{for} \quad p \equiv 1 \bmod 4, \\ p + 1 & \text{for} \quad p \equiv 3 \bmod 4, \end{cases}$$

where in the upper line $(\,)_4$ denotes the biquadratic residue symbol in $\mathbf{Q}(i)$ and $\pi, \bar{\pi}$ are primes in $\mathbf{Q}(i)$ such that $p = \pi\bar{\pi}$ and

$$\pi \equiv \bar{\pi} \equiv 1 \mod (2 + 2i).$$

It follows after a little manipulation that

$$L(\Gamma, s) = \prod \left\{1 - \left(\frac{D}{\pi}\right)_4 \frac{\bar{\pi}}{(N\pi)^s}\right\}^{-1} = \sum \left(\frac{D}{\sigma}\right)_4 \frac{\bar{\sigma}}{(N\sigma)^s}, \tag{3.2}$$

where N denotes the norm from $\mathbf{Q}(i)$ to $\mathbf{Q}$, the product is taken over all real or complex Gaussian primes and the sum over all Gaussian integers subject to

$$\pi \equiv \sigma \equiv 1 \mod (2 + 2i)$$

in each case. Now let $\Delta \equiv 1 \bmod (2+2i)$ be the odd part of the square-free kernel of D, and write in (3.2)

$$\sigma = 16\Delta\mu + \varrho$$

where μ runs through all Gaussian integers and ϱ runs through a certain finite set. This gives, writing $\alpha = \varrho/16\Delta$ for convenience,

$$L(\Gamma, s) = (16\Delta)^{1-2s} \sum\sum \left(\frac{D}{\varrho}\right)_4 \frac{\bar{\mu} + \bar{\alpha}}{|\mu + \alpha|^{2s}}. \tag{3.3}$$

The sum over μ does not involve the biquadratic residue symbol, and it can be analytically continued into $\Re s > \frac{1}{2}$ as follows. Write

$$\psi(\alpha, s) = \frac{\bar{\alpha}}{|\alpha|^{2s}} + \sum_{\mu \neq 0} \left\{\frac{\bar{\alpha} + \bar{\mu}}{|\alpha + \mu|^{2s}} - \frac{\bar{\mu}}{|\mu|^{2s}}\left(1 - \frac{s\alpha}{\mu} + \frac{\bar{\alpha}(1-s)}{\bar{\mu}}\right)\right\}. \tag{3.4}$$

Since the expression in curly brackets is $O(\mu^{-2s-1})$ this defines an analytic function in $\Re s > \frac{1}{2}$; and moreover

$$\psi(\alpha, 1) = \frac{1}{\alpha} + \sum_{\mu \neq 0} \left\{ \frac{1}{\mu + \alpha} - \frac{1}{\mu} + \frac{\alpha}{\mu^2} \right\}$$

is just the Weierstrass zeta-function with periods 1, i. On the other hand, if $\Re s > \frac{3}{2}$ we can rearrange (3.4) to give

$$\sum_{\mu} \frac{\bar{\alpha} + \bar{\mu}}{|\alpha + \mu|^{2s}} = \psi(\alpha, s) + \bar{\alpha}(1-s) \sum_{\mu \neq 0} \frac{1}{(N\mu)^s} =$$

$$= \psi(\alpha, s) + 4\bar{\alpha}(1-s)\, \zeta_{\mathbf{Q}(i)}(s),$$

the other terms in the sum cancelling in pairs. Substituting into (3.3) we obtain

$$L(\Gamma, s) = (16\Delta)^{1-2s} \sum_{\varrho} \left\{ \left(\frac{D}{\varrho}\right)_4 \psi\left(\frac{\varrho}{16\Delta}, s\right) + \frac{(1-s)\, \zeta_{\mathbf{Q}(i)}(s)}{4\Delta} \bar{\varrho} \left(\frac{D}{\varrho}\right)_4 \right\}. \tag{3.5}$$

There are now two ways to proceed. For Conjecture A, we are only interested in the value of $L(\Gamma, 1)$ and can simply write $s = 1$ in (3.5). This gives a closed expression for $L(\Gamma, 1)$ in terms of values of the Weierstrass elliptic functions with periods 1, i. The resulting expression for $L^*(\Gamma, 1)$ is well suited to computation; moreover since the number-theoretic properties of division values of the Weierstrass $\wp$-functions are well known, one can show that $L^*(\Gamma, 1)$ is rational and can give an explicit bound for its denominator. For the full details, see [3].

For Conjecture B, on the other hand, we need to find the first few coefficients in the power series expansion of $L(\Gamma, s)$ about $s = 1$. It turns out that except when $\Delta = 1$, for which special devices are needed, we can arrange that

$$\sum \left(\frac{D}{\varrho}\right)_4 = \sum \varrho \left(\frac{D}{\varrho}\right)_4 = \sum \bar{\varrho} \left(\frac{D}{\varrho}\right)_4 = 0.$$

Assuming this, we can argue back from (3.5) and (3.4) in a way which shows that (3.3) converges in $\Re s > \frac{1}{2}$ provided that the inner sum is taken over ϱ and the outer sum over μ. From this we can deduce convergent series for the coefficients of the power series expansion of $L(\Gamma, s)$ about $s = 1$. Unfortunately the convergence is not very strong; even if one uses

devices from numerical analysis to accelerate the convergence, a large amount of computer time is needed and the results are only accurate to two or three significant figures. These calculations have not in fact been carried out for curves of type (3.1), because the computer available when the work reported in [3] was done was not fast enough. However, STEPHENS has carried out the corresponding calculations for curves of the form (2.7), on the Atlas I at Manchester University.

Curves of the form (3.1) can be parametrized by modular functions, and the methods described in the next section can therefore be applied to them. These methods have only recently become available, and one has too little experience of them yet to know how much labour they involve. At the moment it seems that the methods of the present section are preferable for calculating $L(\Gamma, 1)$, but those of the next section are preferable if further coefficients in the power series expansion of $L(\Gamma, s)$ are needed.

There is a third method of computing $L(\Gamma, s)$ which deserves mention, though as yet no one has tried to exploit it. We have already pointed out that for curves with complex multiplication $L(\Gamma, s)$ is a Hecke L-series with Großencharaktere. HECKE [12] has shown that every such function can be analytically continued over the whole plane, by expressing it in terms of integrals involving theta-functions. These integrals are quite convenient for numerical calculation. This approach has the disadvantage that it does not yield a closed formula for $L(\Gamma, 1)$, and hence all the results it produces are approximate. But it has the advantage that in principle it can be carried through for curves Γ defined over an arbitrary algebraic number field, provided they admit complex multiplication. In contrast, the methods of the present section applied to (3.1) work only if the ground field is $\mathbf{Q}$ or $\mathbf{Q}(i)$, and the methods of the next section apply only to curves defined over $\mathbf{Q}$.

4. Elliptic curves parametrized by modular functions

The work reported in this section has only been started very recently; consequently the calculations are incomplete and most of the proofs are missing. It is based on a conjecture of WEIL [32] and on theorems of EICHLER [7] and SHIMURA [23]. There is as yet only one curve Γ for which the value of $L^*(\Gamma, 1)$ has been calculated by these methods, and the first part of this section outlines this calculation. The second part describes the general method, and those results which have so far been obtained.

We shall use in this section the usual conventions of modular function theory; in particular τ is a complex variable, H is the upper half-plane $\operatorname{Im}\tau>0$, and if $q>0$ is an integer then $\Gamma_0(q)$ is the group of transformations

$$\tau \to \frac{a\tau + b}{c\tau + d}$$

where a, b, c, d are rational integers with $ad-bc=1$ and $q|c$.

Let $j(\tau)$ be the fundamental elliptic modular function. The quotient space $H/\Gamma_0(11)$ has genus 1, and the curve

$$\Gamma: y^2 + y = x^3 - x^2 - 10x - 20 \tag{4.1}$$

is a model for the associated function field $\mathbf{C}(j(\tau), j(11\tau))$. This is the reduced model in the sense of NÉRON, and may be deduced from equation (13) of FRICKE [8], p. 406. The only bad prime for Γ is $p=11$, for which in the notation of § 2 we have

$$L_{11}(s) = (1 + 11^{-s})^{-1}, \qquad c_{11} = 5.$$

With the canonical differential

$$\omega = \frac{dx}{2y + 1}$$

we can therefore write $L^*(\Gamma, s)=L(\Gamma, s)/5\, M_\infty(\Gamma)$ where

$$L(\Gamma, s) = (1 + 11^{-s})^{-1} \prod \{(1 - \alpha_p p^{-s})(1 - \bar{\alpha}_p p^{-s})\}^{-1} = \sum a_n n^{-s}$$

say. Now SHIMURA has shown that if $f(\tau)=\sum a_n e^{2\pi i n\tau}$ then $f(\tau)\, d\tau$ is a differential of the first kind on $H/\Gamma_0(11)$ and is therefore a multiple of ω; comparing the coefficients of $e^{2\pi i\tau}$ we obtain with the help of FRICKE

$$\omega = -2\pi i f(\tau)\, d\tau .$$

By the Mellin transform formula we therefore have

$$L(\Gamma, 1) = -2\pi i \int_0^{i\infty} f(\tau)\, d\tau = \int_{\tau=0}^{i\infty} \omega . \tag{4.2}$$

But the points $\tau=0$ and $\tau=i\infty$ correspond respectively to the points $(-6,5)$ and $(5,5)$ on Γ, both of which are 5-division points; and it now follows easily that

$$L(\Gamma, 1) = \tfrac{1}{5} \int \omega = \tfrac{1}{5} M_\infty(\Gamma), \quad L^*(\Gamma, 1) = \tfrac{1}{25},$$

in agreement with the known results $g=0$, $[\Gamma(\mathbf{Q})]=5$ and the conjectured results that Ш is trivial and that Conjecture A holds for the curve (4.1). It is no coincidence that the integral (4.2) can be explicitly evaluated in this way. On the one hand, using standard notation

$$\Delta(11\omega_1, \omega_2)/\Delta(\omega_1, \omega_2)$$

is a modular function invariant under $\Gamma_0(11)$ which has a ten-fold zero at $\tau=i\infty$ and a ten-fold pole at $\tau=0$; hence $(i\infty)-(0)$ is a 10-division point on Γ. On the other hand, x and y are rational functions of $j(\tau)$ and $j(11\tau)$ over $\mathbf{Q}$; hence their values must be rational (or infinite) at $\tau=0$ and $\tau=i\infty$, since these are both points about which $j(\tau)$ and $j(11\tau)$ have power series expansions with rational coefficients. These arguments, and the known fact that $[\Gamma(\mathbf{Q})]=5$, are enough to show that $L(\Gamma, 1)=\frac{1}{5}nM_\infty(\Gamma)$ for some integer n; and by finding the actual points on Γ which correspond to $\tau=0$ and $\tau=i\infty$ we see moreover that $n\equiv 1 \bmod 5$. The correct value of n can now be found by crude numerical estimation, or more elegantly by topological arguments based on a knowledge of where the real points of Γ correspond to on the Riemann surface $H/\Gamma_0(11)$.

There are just 12 values of q for which $H/\Gamma_0(q)$ has genus 1. The values of q and the corresponding curves Γ, in unreduced form, may be found in [8]. Presumably similar arguments will work for each of them.

The importance of this method, however, arises from a conjecture of Weil. The justification of this conjecture is given in [32] and need not be repeated here; but it should be emphasized that the theoretical reasons for it are much more powerful than the numerical evidence reported below. Let Γ be an elliptic curve defined over $\mathbf{Q}$, and let f be its conductor; then Weil's conjecture states that Γ can be parametrized by elliptic modular functions invariant under $\Gamma_0(f)$.

Because the difficulty of describing $H/\Gamma_0(f)$ explicitly increases rapidly with f, it is convenient to start from the other end; that is, to choose $q>0$ and ask what curves Γ of genus 1 are parametrized by modular functions invariant under $\Gamma_0(q)$. If $C_0(q)$ is the curve, defined over $\mathbf{Q}$, whose Riemann surface is $H/\Gamma_0(q)$, this is equivalent to looking for maps $C_0(q)\to\Gamma$. Let g be the genus of $C_0(q)$ – the previous meaning of g will not be needed in this section – and for any differential of the first kind Ω on $C_0(q)$ and any homology class α write

$$\langle\Omega, \alpha\rangle = \int_\alpha \Omega\,. \tag{4.3}$$

By a slight abuse of language this can be viewed as a bilinear form, Ω being in a vector space over the complex numbers and α in a vector space over $\mathbf{Q}$; and these spaces have dimension g and $2g$ respectively. Now suppose that there is a map $C_0(q)\to\Gamma$, and let ω be the unique differential of the first kind on Γ and Ω the induced differential of the first kind on $C_0(q)$; then for any homology class α on $C_0(q)$ whose image on Γ is trivial we have

$$\langle\Omega,\alpha\rangle=\int_\alpha\Omega=\int_0\omega=0.$$

Such homology classes form a subspace of dimension $2g-2$. Conversely, suppose that on $C_0(q)$ there is a differential of the first kind Ω such that the α for which $\langle\Omega,\alpha\rangle=0$ form a subspace of dimension $2g-2$. Choose a base $\alpha_1,\dots,\alpha_{2g}$ for the integral homology of $C_0(q)$ such that $\langle\Omega,\alpha_n\rangle=0$ for $n>2$; then the function ϕ on $C_0(q)$ defined by

$$\phi(P)=\int_P\Omega$$

is many-valued, and if one of its values is $\phi_0(P)$ the others are the

$$\phi_0(P)+n_1\langle\Omega,\alpha_1\rangle+n_2\langle\Omega,\alpha_2\rangle$$

where n_1 and n_2 are arbitrary integers. If Γ is the elliptic curve corresponding to the doubly periodic functions with periods $\langle\Omega,\alpha_1\rangle$ and $\langle\Omega,\alpha_2\rangle$ it follows that ϕ induces a map $C_0(q)\to\Gamma$.

Hence to find the curves Γ it is enough to find differentials Ω satisfying the conditions above. Unfortunately, direct methods are no use, for it is inconvenient to form the space of differentials of the first kind and impossible to evaluate the integrals $\langle\Omega,\alpha\rangle$ exactly. To progress, we introduce the Hecke operator. For a full account of this, see HECKE [*13*] and PETERSSON [*21*]; here I quote only the results which are needed. Let W denote the space of differentials of the first kind on $C_0(q)$, and let $\Omega=f(\tau)\,d\tau$ be an element of W, so that $f(\tau)$ is a cusp form of dimension -2. For each prime p not dividing q, we define an endomorphism T_p on W by the formula

$$T_p\Omega=\left\{pf(p\tau)+p^{-1}\sum_{n=0}^{p-1}f\left(\frac{\tau+n}{p}\right)\right\}d\tau.$$

(There are similar operators T_p^* for the p which divide q; they play a part

in the complete theory, but are omitted here for simplicity.) The T_p commute, and we can choose a base for W each of whose members is an eigenvector for each T_p. In view of the importance of the bilinear form (4.3), we ought to define a dual operator T_p' on V, the space of homology classes α on $C_0(q)$. Define T_p' as the map induced on V by the map of 0-cycles

$$(\tau) \to (p\tau) + \sum \left(\frac{\tau + n}{p} \right);$$

then it is easily verified that the T_p' are well defined, commute, and satisfy

$$\langle T_p \Omega, \alpha \rangle = \langle \Omega, T_p' \alpha \rangle . \tag{4.4}$$

Again, the map $\tau \to -\bar{\tau}$ induces a homeomorphism of $H/\Gamma_0(q)$ viewed merely as a topological space, and hence induces an automorphism of V which evidently commutes with each T_p. Let V^+ be the subspace consisting of those α which are fixed under this automorphism, and V^- the subspace of those α which are reversed in sign; then $V = V^+ \oplus V^-$, the T_p' induce endomorphisms of V^+ and V^-, and $\mathbf{C} \otimes V^+$ and $\mathbf{C} \otimes V^-$ are canonically dual to W, where $\mathbf{C}$ denotes the field of complex numbers. In particular, the eigenvalues of T_p for W, and of T_p' for V^+ and V^- are the same. Now let α^+ be an isolated eigenvector for the T_p' acting on V^+ – that is, an eigenvector which is determined up to multiplication by a constant by its eigenvalues. It is easy to see that there are corresponding eigenvectors Ω in W and α^- in V^-, and by (4.4) that the α in V for which $\langle \Omega, \alpha \rangle = 0$ form a subspace of dimension $2g-2$; hence α^+ induces a map $C_0(q) \to \Gamma$. Conversely, if we are given a map $C_0(q) \to \Gamma$ it can be shown that the corresponding Ω is an eigenvector for every T_p and that the corresponding eigenvalues are rational integers. Non-isolated eigenvectors do occur, but apparently they correspond to the proper factors q' of q, for each of which there exist several distinct canonical maps $C_0(q) \to C_0(q')$; hence they are not important.

It is a straightforward matter to find a base for V^+, say, and to compute the matrix which represents the effect of any T_p' on it; and in this way we can easily find, for any given q, the α^+ which induce maps $C_0(q) \to \Gamma$. Let

$$T_p' \alpha^+ = c_p \alpha^+$$

for each p, and let the corresponding differential be

$$\Omega = f(\tau)\, d\tau \quad \text{where} \quad f(\tau) = \sum a_n e^{2\pi i n \tau}.$$

Hecke [13] has shown that

$$\sum a_n n^{-s} = F \prod (1 - c_p p^{-s} + p^{1-2s})^{-1} \tag{4.5}$$

where F is a factor corresponding to the primes which divide q. In principle we can now find the two non-zero periods of Ω by numerical integration, and hence also the curve Γ; however, this method is unattractive and there is no guarantee that the resulting curve Γ will have integral coefficients. We have preferred to look for elliptic curves of conductor q and pair them off empirically with the isolated eigenvectors α^+. Despite some special results of OGG [20] and others, there is no certain way of finding all curves of conductor q. Instead, I have written a search program which examines all curves

$$y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6$$

with $b_1 = 0$ or 1, $b_2 = 0$ or ± 1, $b_3 = 0$ or 1, $|b_4| < 300$ and $|b_6| < 1000$. For each $q \leqslant 75$ the search program produces exactly as many non-isogenous curves of conductor q as there are isolated rational eigenvectors α^+. Moreover, it is easy to pair them off; for although no proof is yet available there are strong theoretical and numerical reasons for supposing that (4.5) is the L-series associated with Γ.

Assuming all this, the Mellin transform theorem gives

$$L(\Gamma, 1) = \int_0^{i\infty} -2\pi i \Omega ,$$

which is equal to the integral of a multiple of ω, the unique differential of the first kind on Γ, along a certain contour on Γ. As in the special case worked out at the beginning of this section, the ends of this contour will be rational points on Γ, and they will differ by a $(q-1)$-division point. Hence $L^*(\Gamma, 1)$ will be a rational number for whose denominator an explicit bound can be given. Similarly, the coefficients in the power series expansion of $L^*(\Gamma, s)$ about $s = 1$ can be obtained as definite integrals suitable for numerical calculation. However, the detailed programming of these calculations is a slow job.

5. Abelian varieties over an algebraic number field

It is natural to try to generalize Conjectures A and B, both by replacing the elliptic curve Γ by an Abelian variety A and by replacing the ground

field $\mathbf{Q}$ by an arbitrary algebraic number field κ. This has been done by TATE [29], and the result is Conjecture C below. It is known that the underlying theory remains much the same, though the proofs of the main theorems become harder.

Let A be an Abelian variety of dimension d, defined over an algebraic number field κ. For almost all primes $\mathfrak{p}$ of κ, A has a non-degenerate reduction $A_\mathfrak{p}$ modulo $\mathfrak{p}$ which is an Abelian variety defined over the finite field $GF(q)$ of $q = N\mathfrak{p}$ elements. Moreover there exist numbers $\alpha_{1\mathfrak{p}}, \ldots, \alpha_{2d\mathfrak{p}}$, each of absolute value $q^{1/2}$, such that the number of points on $A_\mathfrak{p}$ defined over $GF(q^n)$ is $\prod(1-\alpha_{i\mathfrak{p}}^n)$ for each n. From these we define the local L-series

$$L_\mathfrak{p}(s) = \{\prod(1 - \alpha_{i\mathfrak{p}} q^{-s})\}^{-1}.$$

Now let ω be a non-zero invariant exterior differential form of degree d on A, let $\kappa_\mathfrak{p}$ be the field of $\mathfrak{p}$-adic numbers, $A(\kappa_\mathfrak{p})$ the set of points on A defined over $\kappa_\mathfrak{p}$, $|\ |_\mathfrak{p}$ the usual $\mathfrak{p}$-adic valuation and $\mu_\mathfrak{p}$ the usual Haar measure on $\kappa_\mathfrak{p}$ which assigns measure 1 to the $\mathfrak{p}$-adic integers. For any finite prime $\mathfrak{p}$ we write

$$M_\mathfrak{p}(A) = \int_{A(\kappa_\mathfrak{p})} |\omega|_\mathfrak{p} \mu_\mathfrak{p}^d;$$

and we make a similar definition for the infinite primes. If ω and A both have good reductions modulo $\mathfrak{p}$ then

$$M_\mathfrak{p}(A) = \{L_\mathfrak{p}(1)\}^{-1}.$$

To define a global L-series for A, choose any finite set of primes S which includes all the infinite primes and all primes for which ω or A has a bad reduction; and write

$$L_S^*(A, s) = \prod_{\mathfrak{p} \in S} \{M_\mathfrak{p}(A)\}^{-1} \prod_{\mathfrak{p} \notin S} L_\mathfrak{p}(s).$$

This depends on S, but not in any vital way. Presumably there is a best possible form for the L-series, as there is with elliptic curves, but the details are not known. $L^*(A, s)$ is only defined in $\Re s > \frac{3}{2}$, but it is conjectured that it can be analytically continued over the whole complex plane.

The Tate-Šafarevič group Ш is defined as in § 2. It is conjectured to be finite, and TATE [26] has shown that if it is finite its order is a perfect square. WEIL [30] proved that $A(\kappa)$, the group of points on A defined over κ, is finitely generated; denote by g the rank of this group. Now

denote by $\hat{A}$ the Abelian variety dual to A; $\hat{A}$ is isogenous to A and so the groups $A(\kappa)$ and $\hat{A}(\kappa)$ must have the same rank, but they need not have the same torsion part. The canonical height is now defined as a bilinear function

$$\hat{h}: \hat{A}(\kappa) \times A(\kappa) \to \text{reals}.$$

It can be defined by methods similar to those of § 2, but it is preferable to use the ideas of NERON [*18*]. Now let $P_1, \ldots, P_g$ be a base for $A(\kappa)$ modulo torsion, and $\hat{P}_1, \ldots, \hat{P}_g$ be a base for $\hat{A}(\kappa)$ modulo torsion, and write

$$R = \det(\hat{h}(P_i, \hat{P}_j)).$$

Moreover let D be the discriminant of κ, and r the number of its complex infinite primes. TATE's generalization of Conjecture B is as follows:

Conjecture C. *With the notation and definitions above,*

$$L^*(A, s) \sim \frac{(2^r |D|^{-\frac{1}{2}})^d \, [Ш] \, |R|}{[A(\kappa)_{\text{tors}}] \, [\hat{A}(\kappa)_{\text{tors}}]} (s-1)^g \quad as \quad s \to 1.$$

The main surprise in this, in comparison with Conjecture B, is the appearance of the dual Abelian variety $\hat{A}$ in the denominator; for Γ, as a Jacobian, is canonically self-dual. The justification for it has been provided by TATE [*29*], who showed that Conjecture C is compatible with isogeny in its present form and would not be if $\hat{A}$ was replaced by A.

There is no direct evidence for Conjecture C beyond that which applies to the special case of Conjecture B, for no way of calculating $L^*(A, s)$ near $s=1$ is known. However, the method suggested at the end of § 3 could in principle be applied to varieties with sufficiently many complex multiplications, in view of the results of SHIMURA and TAMIYAMA [*22*].

For later reference, it is convenient to rephrase the special case in which A is the Jacobian of a curve C which is also defined over κ. The L-series can be defined in terms of the local zeta-functions

$$\{\prod (1 - \alpha_{ip} q^{-s})\} / (1 - q^{-s})(1 - q^{1-s})$$

of C, and $A(\kappa) = \hat{A}(\kappa)$ is just the group of divisors on C of degree 0 and defined over κ, modulo linear equivalence. The definition of Ш in § 2 becomes meaningless, but the definition by means of cohomology groups is easily extended; and similar remarks apply to $\hat{h}$ and hence to R. All the expressions in the Conjecture can therefore be expressed in terms of the curve C.

add this remark in new version of empirical evidence

6. Varieties over finite fields

Let V be a complete non-singular variety of dimension d, defined over the finite field $k=GF(q)$ of characteristic p. The zeta-function of V can be written in the form

$$\zeta_V(s) = \frac{P_1(q^{-s}) \dots P_{2d-1}(q^{-s})}{P_0(q^{-s})\, P_2(q^{-s}) \dots P_{2d}(q^{-s})} \tag{6.1}$$

where the P_i are polynomials (possibly of degree zero)

$$P_i(x) = \prod_{j=1}^{B_i} (1 - \alpha_{ij} x). \tag{6.2}$$

The original definition of the α_{ij} was that for each $n>0$ the number of points on V defined over $GF(q^n)$ is $\sum\sum(-1)^i \alpha_{ij}^n$; and they are assigned to the polynomials $P_i(x)$ by the conjectural relation

$$|\alpha_{ij}| = q^{i/2}. \tag{6.3}$$

Alternatively, one can define $P_i(x)$ as the characteristic polynomial of the Frobenius endomorphism acting on the i-dimensional cohomology of V with l-adic integer coefficients, where l is any prime other than p. It is believed that the $P_i(x)$ defined in this way do not depend on l; but this has only been proved for $i=0$, 1, $2d-1$ and $2d$, and of course for $\zeta_V(s)$ as defined by (6.1). In what follows we shall assume that the $P_i(x)$ are well-defined, but we shall not need (6.3).

Let ϱ_r be the rank of the group of classes of r-dimensional cycles defined over k on V, modulo algebraic equivalence. We can choose a base for the $2r$-dimensional cohomology of V such that ϱ_r of its elements come from these cycles. Since the Frobenius endomorphism acts trivially on these cycles, the characteristic polynomial $P_{2r}(x)$ must contain the factor $(1-q^r x)$ at least to the ϱ_rth power. TATE ([27], substantially repeated in [28]) has conjectured that this is the exact power – in other words, that every factor $(1-q^r x)$ arises from a rational r-dimensional cycle. This can be rephrased in terms of the zeta-function (6.1) as follows:

Conjecture D. *With the notation above, the order of the pole of $Z_V(s)$ at $s=r$ is equal to the rank of the group of classes of r-cycles defined over k on V, modulo algebraic equivalence.*

Tate has verified this for a number of special varieties. For the case when $d=2$, so that V is a surface, see below.

Clearly there can be no analogous statement when i is odd. It is known

that $P_1(x)$ depends only on the Albanese variety of V; and assuming the existence of Weil's 'higher Jacobians', some of the factors of $P_{2r+1}(x)$ must come from the higher Jacobian of V in dimension r. (One possible definition of the higher Jacobian is as follows. Let W be a variety which parametrizes some maximal family of r-dimensional subvarieties of V; then the higher Jacobian in dimension r is that Abelian variety which is universal for maps from any such W to any Abelian variety. Perhaps for good enough V it is even the Albanese variety of each such W.) For the special case of the cubic three-fold, see [4]. Such scanty evidence as exists suggests that all those factors of $P_{2r+1}(x)$ for which q^r divides $\alpha_{2r+1,j}$ arise in this way.

More generally, for any i and r with $r \leqslant \frac{1}{2}i \leqslant d$ we can pick out those factors $(1-\alpha_{ij}x)$ of $P_i(x)$ for which q^r divides α_{ij}. Is it true that these and only these factors arise from cohomology classes which are in some sense built up from r-dimensional cycles on V – not necessarily defined over k?

In the special case where V is a surface, ARTIN and TATE [29] have gone much further. Let NS denote the Néron-Severi group of V over k – that is, the group of classes of divisors defined over k on V, modulo algebraic equivalence; let ϱ be the rank of NS and let $D_1, \ldots, D_\varrho$ be a base for NS modulo torsion. Write

$$\alpha = p_g(V) - \delta(V) \geqslant 0,$$

where p_g is the geometric genus of V and $\delta(V)$ is the "defect of smoothness" of the Picard scheme of V over k. Let $\mathrm{Br}(V)$ be the Brauer group of V over k. For details of this see GROTENDIECK [9], [10] and [11]; the Brauer group is related to the Tate-Šafarevič group, but has the advantage that for many V it can be proved to be finite and even computed. The conjecture of ARTIN and TATE is as follows:

Conjecture E. *With the notation above,*

$$P_2(q^{-s}) \sim \frac{[\mathrm{Br}(V)]\,|\det\{D_i \cdot D_j\}|}{q^\alpha [\mathrm{NS}_{\mathrm{tors}}]^2} (1-q^{1-s})^\varrho \quad as \quad s \to 1,$$

where the curly brackets denote intersection multiplicity.

This is closely related to the variant of Conjecture C in which κ is a finitely generated field of transcendence degree 1 over a finite field. For the full details see [29]; here we only sketch the idea. Let C, defined over $\kappa = k(t)$, be a generic member of a pencil of curves on V. The zeta-function of C over κ is closely connected with that of V over k, because C is a generic fibre of V. The group of divisor classes defined over κ on C,

modulo linear equivalence, is isomorphic to the Néron-Severi group of V over k; this fact lies at the heart of Néron's proof of the Néron-Severi theorem – see for example LANG [*14*], Chapter V. It was pointed out at the end of § 5 that Conjecture C could be expressed entirely in terms of the curve C, without overt reference to its Jacobian A. The height, on C, is a bilinear form on the group of divisor classes on C defined over κ; and by the isomorphism above it becomes a bilinear form on NS. Since there is already one such form given by intersection number, these two ought to be the same; and this is confirmed by a detailed analysis.

The status of Conjecture E is much better than that of the previous conjectures, for ARTIN and TATE have proved that at least its non-p part follows from statements about V which are apparently much weaker. The precise result they prove is as follows:

Theorem. *For given V and k suppose that either*

(i) *the l-primary part of* $\mathrm{Br}(V)$ *is finite for some prime $l \neq p$; or*

(ii) $P_2(q^{-s})$ *has a zero of order precisely ϱ at $s=1$.*

Then the non-p *part of* $\mathrm{Br}(V)$ *is finite and*

$$P_2(q^{-s}) \sim \frac{[\mathrm{Br}(V)_{\mathrm{non}-p}]\,|\det\{D_i \cdot D_j\}|}{p^{\nu}[\mathrm{NS}_{\mathrm{tors}}]^2}(1-q^{1-s})^{\varrho} \quad \text{as} \quad s \to 1$$

for some integer ν.

Tate has proved that $\mathrm{Br}(V)$ is finite in a number of cases, in particular when V is a product of two curves. This last result is closely connected with his proof that if two Abelian varieties defined over a finite field have the same zeta-function, then they are isogenous.

7. Varieties over algebraic number fields

Let V be a complete non-singular variety of dimension d defined over an algebraic number field κ. For almost all finite primes $\mathfrak{p}$ of κ, V has a non-singular reduction $V_{\mathfrak{p}}$ modulo $\mathfrak{p}$; and if q is the absolute norm of $\mathfrak{p}$ then $V_{\mathfrak{p}}$ has a local zeta-function given by (6.1) and (6.2). For each i with $0 \leqslant i \leqslant 2d$, we can associate with V an L-series

$$L_i(V,s) = \prod_{\mathfrak{p}} \{P_i(q^{-s})\}^{-1} = \prod_{\mathfrak{p}} \{\prod_j (1-\alpha_{ij}q^{-s})\}^{-1}, \qquad (7.1)$$

where the outer product is taken over all $\mathfrak{p}$ for which V has a good reduction. (This is the process which we applied to elliptic curves in § 2, and implicitly to arbitrary curves in § 5. However, in contrast with these cases,

we shall not attempt here to supply any factors corresponding to the bad finite primes or the infinite primes.) Even assuming (6.3), the product (7.1) only converges in $\Re s > 1+\frac{1}{2}i$, except of course in the trivial case when $B_i=0$. However, it is generally believed that $L_i(s)$ can be analytically continued through the entire complex plane, and that there is a functional equation connecting $L_i(s)$ with $L_i(1+i-s)$.

The cases $i=0$ and 1 (and by symmetry $i=2d-1$ and $2d$) need no further discussion. $L_0(s)$ is, except for some missing factors, the classical Riemann zeta-function of κ; and it is well known that its behaviour near $s=1$ (the real point on the boundary of the half-plane of convergence) gives valuable information about κ. $L_1(s)$ depends only on the Albanese variety A of V, and is in fact the $L^*(A, s)$ of § 5 with some factors missing; according to Conjecture C its most interesting behaviour is at $s=1$, which is the real point a distance $\frac{1}{2}$ from the half-plane of convergence, and is the centre of the critical strip. As in § 6, we must therefore expect a fundamental difference between odd and even values of i.

When $i=2r$ is even, TATE [27] has suggested that the analogue of Conjecture D still holds, in the following form:

Conjecture F. *With the notation above, the order of the pole of $L_{2r}(V, s)$ at $s=r+1$ is equal to the rank of the group of classes of r-cycles defined over κ on V, modulo algebraic equivalence.*

It should be emphasized that the heuristic deduction of this from Conjecture D along the lines "$P_i(q^{-s}) \sim C_{\mathfrak{p}}(1-q^{r-s})^{\varrho}$ for some constants $C_{\mathfrak{p}}$; hence $L_i(V, s) \sim C\{\zeta_\kappa(s-r)\}^{\varrho} \sim C'(s-r-1)^{-\varrho}$ near $s=r+1$" is totally misleading; it is not even true that V and $V_{\mathfrak{p}}$ have the same ϱ_r for almost all $\mathfrak{p}$. The simplest counter-example is $V=\Gamma\times\Gamma$, where Γ is an elliptic curve which does not admit complex multiplication; here $\varrho_1=3$ for V, but $\varrho_1=4$ for almost all $V_{\mathfrak{p}}$. There is strong reason to suppose that any sufficiently general quartic surface is also a counter-example.

Tate has verified this conjecture in a few special cases. Moreover, by taking V to be the d-fold product of an elliptic curve Γ not admitting complex multiplication with itself, he has deduced from it some very interesting results on the distribution of the arg α_p as p varies. (Here α_p is defined by (2.1).) These results agree with the numerical evidence. The constant

$$\lim (s-r-1)^{\varrho} L_{2r}(V, s)$$

has been evaluated for a number of varieties V. The results suggest that the constant is significant, but as yet there is nothing with which it can be even conjecturally identified.

When $i=2r+1$ is odd almost nothing is known, except of course for the case $i=1$ treated in § 5 and the symmetric case $i=2d-1$. There is however one striking and wholly unexplained phenomenon. Suppose that $V=\Gamma\times\Gamma\times\Gamma$, where Γ is an elliptic curve; for convenience of notation we assume that Γ is defined over $\mathbf{Q}$ and its local zeta-function is given by (2.1). Now

$$P_3(p^{-s})=(1-\alpha_p^3 p^{-s})(1-\bar{\alpha}_p^3 p^{-s})(1-\alpha_p p^{1-s})^9(1-\bar{\alpha}_p p^{1-s})^9$$

and so $L_3(V,s)=L_3^0(\Gamma,s)\{L_1(\Gamma,s-1)\}^9$ say, where

$$L_3^0(\Gamma,s)=\prod\{(1-\alpha_p^3 p^{-s})(1-\bar{\alpha}_p^3 p^{-s})\}^{-1}.$$

It is reasonable to ascribe the term $\{L_1(\Gamma,s-1)\}^9$ to the higher Jacobian in dimension 1; and in any case its behaviour near $s=2$ is completely described by Conjecture B. We are therefore led to examine $L_3^0(\Gamma,s)$ near $s=2$.

Now suppose that Γ has the form

$$y^2=x^3-Dx. \tag{7.2}$$

Using the ideas of § 3, though in a more complicated form, it is possible to give a closed expression for $L_3^0(\Gamma,2)$ in terms of division values of elliptic functions; and this expression has been evaluated for about 100 values of D. The structure of the results closely resembles what we would be able to say about $L_1(\Gamma,1)$ if we had only the results of the calculation, and lacked any number-theoretic theory of elliptic curves to attach them to. To clarify this, I formulate a weak version of Conjecture A for the curve (7.2). For this purpose we employ "fudge factors" λ_∞ and λ_p for each prime p dividing $2D$. These have explicit definitions in terms of the local properties of D, which are too long to give here; but it should be noted that $\lambda_p=1$ or 2 for each finite p. They are in fact just the $\{M_p(\Gamma)\}^{-1}$, possibly multiplied by rational squares; but we are forbidden to use that interpretation in the present context. Write

$$\mu=L_1(\Gamma,1)\lambda_\infty\prod\lambda_p$$

the "fudged" value of $L_1(\Gamma,1)$.

Weak Conjecture A. *The rational integer μ is a perfect square. By local considerations involving only the sign of D and those primes which divide $2D$, we can state a sufficient condition for $\mu=0$; but this condition is not a necessary one.*

That μ is a rational integer can be proved from the explicit formula.

That μ is a perfect square is equivalent to saying that [Ш] is a perfect square. The sufficient condition for $\mu=0$ is just the necessary and sufficient condition for (7.2) to have an odd number of first descents, and so for g to be odd; this is sufficient, but not necessary, for $g>0$.

A precisely analogous conjecture fits the numerical evidence for $L_3^0(\Gamma, 2)$. We can define local "fudge factors" λ'_∞ and λ'_p; these are not the same as λ_∞ and λ_p above, but we do have $\lambda'_p=1$ or 2. Write

$$\mu' = L_3^0(\Gamma, 2)\,\lambda'_\infty \prod \lambda'_p.$$

It can be proved that μ' is a rational integer; and the numerical evidence shows that μ' must always be a square. (There is no possibility of coincidence, for the numbers involved are much larger than with μ.) Moreover one can state local conditions (not the same as for μ) which appear to be sufficient but not necessary for $\mu'=0$. Presumably there is a duality theory and a descent argument of some sort which underlies all this; but what it is I have no idea.

References

[1] BIRCH, B. J., and N. M. STEPHENS: The parity of the rank of the Mordell-Weil group. Topology 5, 295–299 (1966).

[2] BIRCH, B. J., and H. P. F. SWINNERTON-DYER: Notes on elliptic curves I, J. reine angew. Math. **212**, 7–25 (1963).

[3] BIRCH, B. J., and H. P. F. SWINNERTON-DYER: Notes on elliptic curves II, J. reine angew. Math. **218,** 79–108 (1965).

[4] BOMBIERI, E. and H. P. F. SWINNERTON-DYER: The zeta function of a cubic threefold. Annali di Pisa **21,** 1–29 (1967).

[5] CASSELS, J. W. S.: Arithmetic on curves of genus 1 (IV) Proof of the *Hauptvermutung*. J. reine angew. Math. **211**, 95–112 (1962).

[6] CASSLLS, J. W. S.: Diophantine equations with special reference to elliptic curves, J. Lond. Math. Soc. **41** ,193–219 (1966).

[7] EICHLER, M.: Quaternäre quadratische Formen und die Riemann Vermutung für die Kongruenzzetafunktion. Arch. Math. **5**, 355–366 (1954).

[8] FRICKE, R.: Die elliptischen Funktionen und ihre Anwendungen. Vol. **2**, Leipzig 1922.

[9] GROTHENDIECK, A.: Le groupe de Brauer I. Sém. Bourbaki **290** (1965).

[10] GROTHENDIECK, A.: Le groupe de Brauer II. Sém. Bourbaki **297** (1965).

[11] GROTHENDIECK, A.: Le groupe de Brauer III. Mimeo notes I.H.E.S. (1966).

[12] HECKE, E.: Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. Zweite Mitteilung. Math. Z. **6**, 11–51 (1920).

[13] HECKE, E.: Űber Modulfunktionen und die Dirichletschen Reihen mit Eulerschen Produktentwicklung. Math. Ann. **114**, 1–28 and 316–351, (1937).

[14] LANG, S.: Diophantine Geometry. New York 1962.

[15] LANG, S.: Les formes bilinéaires de Néron et Tate. Sém. Bourbaki **274** (1964).

[16] MORDELL, L. J.: On the rational solution of the indeterminate equations of the third and fourth degrees. Proc. Camb. Phil. Soc. **21**, 179–192, (1922).

[17] NÉRON, A.: Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. Publ. IHES **21** (1964).
[18] NÉRON, A.: Quasi-fonctions et hauteurs sur les variétés abéliennes. Ann. Math. **82**, 249–331, (1965).
[19] OGG, A. P.: Elliptic curves and wild ramification, Amer. J. Math. **89**, 1–21 (1967).
[20] OGG, A. P.: Abelian curves of 2-power conductor. Proc. Camb. Phil. Soc. **62**, 143–148, (1966).
[21] PETERSSON, H.: Konstruktion der sämtlichen Lösungen einer Riemannschen Funktionalgleichung durch Dirichlet-Reihen mit Eulerscher Produktentwicklung. Math. Ann. **116**, 401–412 (1939) and **117**, 39–64 and 277–300, (1940).
[22] SHIMURA, G. and TANIYAMA, Y.: Complex multiplication of Abelian varieties. Publ. Math. Soc. Japan **6** (1961).
[23] SHIMURA, G.: Correspondances modulaires et les fonctions zeta de courbes algébriques, J. Math. Soc. Japan **10**, 3–28, (1958).
[24] STEPHENS, N. M.: Thesis Manchester, (1965).
[25] STEPHENS, N. M.: Conjectures concerning elliptic curves. (In press).
[26] TATE, J.: Duality theorems in galois cohomology over number fields. Proc. Intern. Congress Math. Stockholm, 288–295, (1962).
[27] TATE, J.: Algebraic cohomology classes, Mimeo notes Woods Hole (1964).
[28] TATE, J.: Algebraic cycles and poles of zeta functions. Proc. Purdue Univ. Conf. 1963. New York 93–110, (1965).
[29] TATE, J.: On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. Sém. Bourbaki **306** (1966).
[30] WEIL, A.: L'arithmétique sur les courbes algébriques, Acta Math. **52**, 281–315, (1928).
[31] WEIL, A.: On algebraic groups and homogenous spaces, Amer. J. Math. **77**, 493–512, (1955).
[32] WEIL, A.: Űber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Ann. **168,** 149–156 (1967).