Heegner Points and Rankin L-Series
MSRI Publications
Volume **49**, 2004

Heegner Points: The Beginnings

BRYAN BIRCH

1. Prologue: The Opportune Arrival of Heegner Points

Dick Gross and I were invited to talk about Heegner points from a historical point of view, and we agreed that I should talk first, dealing with the period before they became well known. I felt encouraged to indulge in some personal reminiscence of that period, particularly where I can support it by documentary evidence. I was fortunate enough to be working on the arithmetic of elliptic curves when comparatively little was known, but when new tools were just becoming available, and when forgotten theories such as the theory of automorphic function were being rediscovered. At that time, one could still obtain exciting new results without too much sophisticated apparatus: one was learning exciting new mathematics all the time, but it seemed to be less difficult!

To set the stage for Heegner points, one may compare the state of the theory of elliptic curves over the rationals, E/Q for short, in the 1960's and in the 1970's; Serre [15] has already done this, but never mind! Lest I forget, I should stress that when I say "elliptic curve" I will always mean "elliptic curve defined over the rationals".

In the 1960's, we were primarily interested in the problem of determining the Mordell-Weil group $E(Q)$, though there was much other interesting apparatus waiting to be investigated (cf Cassels' report [7]). There was a good theory of descent, Selmer and Tate-Shafarevich groups, and so forth: plenty of algebra. But there was hardly any useful analytic theory, unless the elliptic curve had complex multiplication; $E(C)$ was a complex torus, beautiful maybe, but smooth and featureless, with nothing to get hold of. One could define the L-function

$$L_S(E,s) \sim \prod_{p \notin S} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

(where S is a set of "bad" primes), and Hasse had conjectured that this is an analytic function with a good functional equation; but most of us could only prove this when the curve had complex multiplication.

By the 1970's, everything had changed. Shimura showed that for *modular* elliptic curves (that is, elliptic curves parametrised by functions on $X_0(N)$) the L-function automatically has a good functional equation. For Peter Swinnerton-Dyer and myself, the turning point came when Weil wrote to Peter [A], stressing the importance of the functional equation, which (Weil said) *is of the form*

$$\Lambda(s) = (2\pi)^{-s}\Gamma(s)L(s) = C.N^{1-s}\Lambda(2-s)$$

in all known cases (and, conjecturally, also in all unknown cases). Here, N is the analytic conductor of the curve, conjecturally the same as the algebraic conductor defined by Serre and Tate. Weil went on to point out that this conjecture of Hasse's was known for modular elliptic curves (Weil actually called them Eichler-Shimura curves) as well as for curves with complex multiplication. Though Weil didn't actually say it explicitly, we knew that he was advising us to concentrate on *modular* elliptic curves. The next year, Weil [20] proved that the functional equations conjectured by Hasse for an elliptic curve over Q were valid *only* if the curve was modular. From then on, it was clear that in all work that needed $L_E(s)$ to be well behaved, one might as well assume that the elliptic curve E/Q under consideration was modular. We referred (for instance, in letters [B] between Peter and John Tate) to the hypothesis, implicit in Weil's letter and paper, that every elliptic curve over Q really was modular, as the "Weil conjecture"; years later we learnt that this had been suggested much earlier, by Taniyama [18]. (I hope these remarks, and the slightly earlier references, are a helpful amplification of the very accurate account of the history of this conjecture given by Serre [15].)

Almost on cue, Heegner points came along, specifically on modular curves! Suddenly, instead of being a featureless homogeneous space, $E(C)$ was a highly structured object, studded all over with canonically defined families of points, with coordinates in known number fields. In studying $E(Q)$, instead of searching for structure, one had the much more hopeful task of analysing a situation where there was almost too much of it.

And sure enough, the theorems rolled in, though not immediately. There was about a ten year gap between the repopularisation of Heegner points and anyone making proper use of them! That will be what Dick talks about. My job is to tell you where these points came from.

2. Prehistory

In this context, "prehistory" means the latter half of the nineteenth century; and it is summarised in Weber's *Algebra* [19], one of the great books of mathematics. I believe that Weber remained the most up-to-date book on the arithmetic of modular functions until Shimura's book [16] was published in 1971; certainly it was the best I could find in 1966.

The story starts with the modular function, $j(z)$, characterised by its values at i and ρ, its pole at ∞ and its functional equation $j(M(z)) = j(z)$ for any

unimodular integral transformation $z \to M(z) := (az+b)/(cz+d)$; that is, j is invariant by the modular group $\Gamma(1)$. So j may be regarded as a function of similarity classes of lattices: if $\Lambda = \Lambda(\omega_1, \omega_2)$ is a lattice with basis (ω_1, ω_2) then $j(\Lambda) := j(\omega_1/\omega_2)$ does not depend on the choice of basis. If $f(z)$ is another function invariant by the modular group then f is a rational function of j, and if f is invariant by a group commensurable with $\Gamma(1)$ then $f(z), j(z)$ are algebraically dependent. In particular, if N is any natural number, the function $j_N(z) := j(Nz)$ is invariant by the conjugate $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma(1)\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$ of $\Gamma(1)$, the intersection $\Gamma_0(N)$ of these two conjugate subgroups has finite index in both, and so j, j_N are related by a polynomial equation $F_N(j(z), j_N(z)) = 0$ with $F_N(X,Y) \in \mathbb{Z}[X,Y]$. We recognise $F_N(X,Y) = 0$ as the modular curve $Y_0(N)$, the quotient of the upper half plane by $\Gamma_0(N)$. Functions invariant by $\Gamma_0(N)$ are rational functions of j and j_N. If p is a prime, we have Kronecker's congruence

$$F_p(X,Y) \equiv (X^p - Y)(X - Y^p) \pmod{p}.$$

A beautiful discovery was the theory of "complex multiplication". Suppose that ω is a complex quadratic surd satisfying a primitive equation $A\omega^2 + B\omega + C = 0$ with A, B, C integers; the discriminant of ω is $D(\omega) := B^2 - 4AC < 0$. Then $j(\omega)$ is an algebraic integer: the reason is that we can find ω' in the lattice $\Lambda(1,\omega)$ so that the lattices $\Lambda(1,\omega')$ and $\Lambda(1, N\omega')$ are the same for some N. Further, the field $K(D) := Q(\omega, j(\omega))$ in which $j(\omega)$ lives depends only on $D(\omega)$, not on ω, and the degree $[K(D) : Q(\omega)]$ is equal to the class number of the ring $R(D) := Z\left[\frac{D+D^{1/2}}{2}\right]$. In fact, one may regard the ideals A of this ring as lattices, so it makes sense to evaluate j at an ideal class A, and then when A runs through the classes of $R(D)$ the values of $j(A)$ are all conjugate. The field $K(D)$ is called the *ring class field* corresponding to the ring $R(D)$; in particular, if Δ is a field discriminant (discriminant of the ring of integers of $Q(\Delta^{1/2})$) then $K(\Delta)$ is simply the class field of $Q(\Delta^{1/2})$, and the fields $K(s^2\Delta)$ are extensions of $K(\Delta)$ of predictable degrees.

Complex multiplication was the beginning of class field theory, and nowadays it is often treated as a particular case of the general theory. But that is really the wrong way round: the theory presents us with the explicit field $K(D)$ constructively, at the very start, and the beautiful "class field" properties of $K(D)$ are more easily obtained directly; it is the subject of Weber's book. (The language in Weber is now unfamiliar, so that the arguments seem more complicated than they actually are. I should perhaps add that until the Brighton conference in 1965, published as [8], the apparatus of class field theory was much more forbidding than was Weber's *Algebra*.)

The theory of complex multiplication as developed by Weber tells us about the field $j(A)$ lives in when A is an ideal of a given complex quadratic ring. When one reads Weber, one sees that he aims to work in rather greater generality. He considers other modular functions, invariant by various subgroups of $\Gamma(1)$;

for instance, he defines particular functions $\gamma_2, \gamma_3, \sigma(x)$ which satisfy $\gamma_2^3 = j$, $\gamma_3^2 = j - 1728$, $\sigma^{24} - 16 = \sigma^8\gamma_2$ and $(\sigma^{24} - 64)(\sigma^{24} + 8)^2 = (\gamma_3\sigma^{12})^2$ (I use Heegner's later notation for these functions); and he proves by various contortions that if $D(\omega)$ satisfies various congruence conditions then evaluating these functions at ω gives values in the ring class field $K(D)$, not as one might expect in some proper extension. For instance, if $(3, D) = 1$ then $\gamma_2(\omega) \in K(D)$, so $j(\omega)$ is a cube — e.g, $j(\sqrt{-2}) = 8000$, and $j\left(\frac{1+\sqrt{-163}}{2}\right) = -640320^3$; if D is odd then $\gamma_3(\omega) \in K(D)$ and if $D \equiv 5 (\mathrm{mod} 8)$ then $\sigma^6(\omega) \in K(D)$. Unhappily, though Weber was aiming for a more general theory, he seemed only to succeed in constructing a plethora of other special cases. Many beautiful numbers were calculated, but everything was far too particular, and the theory too complicated: it was too far ahead of the rest of mathematics. New mathematical concepts were needed before a civilised theory of automorphic functions could be developed.

Quite abruptly, the theory of modular functions dropped completely out of fashion; Hecke did important work and so did Rankin (hence the title of this workshop), but it is hardly an exaggeration to say that for half a century most mathematicians hardly knew that the theory of modular functions had ever existed.

3. Heegner

So we may jump directly to Heegner's paper [11] of 1952. Heegner was a fine mathematician, with a rather low-grade post in a gymnasium in East Berlin; he clearly knew Weber's book well. He was interested in the congruence number problem: recollect that m is a congruence number if it is the area of a rightangled triangle with rational sides (most people call this a Pythagorean triangle; Heegner called it a Harpedonapten triangle). In his famous, very eccentrically written, paper he begins with a historical introduction concerning the congruence number problem, then he quotes various things from Weber and proves some highly surprising theorems showing that the congruence number problem is soluble for certain families of m; and then he suddenly (correctly but over succinctly) solves the classical class number one problem (see also [1] and [17]). Unhappily, in 1952 there was noone left who was sufficiently expert in Weber's *Algebra* to appreciate Heegner's achievement.

Heegner proved that if p is a prime congruent to 5 or 7 modulo 8 then p is a congruence number, and if p is congruent to 3 or 7 modulo 8 then $2p$ is a congruence number. The proofs are similar, I will sketch his proof that $2p$ is congruence when $p \equiv 3 (\mathrm{mod}\ 8)$, since it is the simplest. A typical Pythagorean triangle has sides $2rst, r(s^2 - t^2)$ with rational r, s, t, so $2p$ is a congruence number if there are rational r, s, t with $2p = r^2st(s^2 - t^2)$. For this it is clearly enough that the elliptic curve

$$E \ : \ -py^2 = x(x^2 - 64) \tag{1}$$

should have a nontrivial rational point, and for this it is enough that the Diophantine equation

$$-pu^2 = v^4 - 64 \tag{2}$$

is soluble in rational u, v. Referring to Weber, we see that if $p \equiv 3 (\mathrm{mod}\ 8)$ there is a solution of (2) with $(u, v) \in K(-p)$ given by $\sqrt{-p}u = \gamma_3\sigma^{12}/(\sigma^{24} + 8)$, $v = \sigma^6$, with the functions evaluated at $\omega = \frac{-3+\sqrt{-p}}{2}$; and it is easy to check that u, v are real. If now p is prime, the class number is odd, so the classfield $K(-p) \cap \mathbb{R}$ has odd degree over the rationals. So to prove Heegner's theorem that twice every prime congruent to 3 modulo 8 is a congruence number, it is enough to show that if (2) has a point in an extension of odd degree then it has a rational point. Nowadays, this would be done by saying that a solution of (2) gives a point of E in the nontrivial coset C of $E(\mathbb{R})/2E(\mathbb{R})$, and adding up an odd number of points of C gives a point in C, which has to be nontrivial. Heegner uses a characteristically offbeat method; it is hardly known and has the advantage of being good for explicit computation over Q, so I quote it:

HEEGNER'S LEMMA. *Suppose that $f(X)$ is a quartic over a field L whose leading coefficient is not a square in L, and that $Y^2 = f(X)$ has a solution in a field M with M/L an extension of odd degree d. Then $Y^2 = f(X)$ has a solution in L.*

If not, we may suppose that M is the extension of least odd degree in which there exist x, y satisfying $y^2 = f(x)$. We may suppose that $y \in L(x)$, else it would need an extension of even degree, so $L(x) = M$, so x is a root of $g(X) = 0$ where g is a polynomial over L of degree $d \geq 3$; and $y = h(x)$ where h is a polynomial over L of degree $s \leq d - 1$. We see that $h^2 - f$ is of degree $\max(4, 2d - 2)$ since the leading coefficients cannot cancel; and $h^2 - f$ is divisible by g, so $h^2 - f = gk$ where k is a polynomial over L of degree $\max(4 - d, d - 2)$ which is certainly odd and less than d. But now if θ is a root of $k(X) = 0$, we see that $x = \theta, y = h(\theta)$ gives a point of $y^2 = f(x)$ in a smaller extension than M.

Heegner's paper was written in an amateurish and rather mystical style, so perhaps it was not surprising that at the time noone tried very hard to understand it. It was thought that his solution of the class number problem contained a gap, and though his work on the congruence number problem was clearly correct, noone realised that it contined the germs of a valuable new method. Sadly, he died in obscurity.

4. Simplification and Generalisation

Looking back at old diaries and suchlike, I find that I first saw Heegner's paper in 1966 (a little later than Stark, he tells me); I had been told it was wrong, but so far as I could see, it followed from results in Weber's *Algebra*; and his results on points on elliptic curves were exciting. It took a while to decide he was right (one had to read Weber first, and I hadn't even got good German) but

this was achieved by the end of 1967 (see [2] and [3]). It took very much longer to understand it properly, maybe until 1973; it was necessary to both simplify and generalise. One needed to replace Heegner's rather miraculous construction of rational points on certain elliptic curves by a theorem that modular elliptic curves, indeed modular curves, are born with natural points on them, defined over certain classfields.

One also wanted to relate these points to something else – maybe to L_E. I persuaded Nelson Stephens (while he held an Atlas Fellowship) to compute the functions γ_2, γ_3 for discriminants D up to 1580, prime to 6. (He computed for even D too, but for the sake of exposition let us restrict to odd D.) We know that for such discriminants $D^{1/2}\gamma_3$ and γ_2 are in the class field $K(D)$, so we get points $P(\omega)$ on the curve

$$y^2 = x^3 - 1728.$$

(It was exceptionally easy to compute the points $P(\omega)$ as complex points, as one simply integrated the differential $\eta^4(6z)$.) Summing over the ideal class group of $R(D)$, we get a rational point $u(D,1)$ of the curve

$$E_D: \ Dy^2 = x^3 - 1728.$$

More generally, if we take χ as a genus character of the classgroup, then the sum $\sum \chi(\omega)P(\omega)$ gives a point $u(e,f)$ of the curve

$$E_e: \ ey^2 = x^3 - 1728,$$

where the factorisation $D = ef$ depends on χ. The computations were consistent with a formula

$$\hat{h}(u(e,f)) = 2^A 3^B L(E_f,1)L'(E_e,1)/\sqrt{-3/ef}\,\Omega^2$$

where the exponents A, B were explicit and not very interesting (but we did not understand them at the time); note that $u(e,f)$ was trivial when $E_e(Q(\sqrt{D}))$ had rank more than 1. We told people, the above formula is quoted from a 1973 Harvard seminar [C] (unfortunately Dick Gross was away in Oxford that term), but as we did not understand what we were doing, we did not publish these computations till years later [5]. Nowadays, we know that $ey^2 = x^3 - 1728$ is the "wrong" model, which explains the unwanted factors $2^A 3^B$.

Meanwhile, we realised what one should be doing in a general case. One wants points on a modular curve, with coordinates in smaller fields than one would expect, and in the first instance one finds points on $X_0(N)$ itself rather than on the elliptic curves it covers. Once one realises this, the problem becomes fairly simple. $X_0(N)$ is the completion of the upper half plane factored by $\Gamma_0(N)$, it is parametrised by $j(z)$ and $j_N(z) = j(Nz)$, so we may take a typical point of $X_0(N)$ as $P(z) := (j(z), j(Nz))$. If we take ω as a quadratic surd with discriminant D, then $j(\omega) \in K(D)$ and usually $N\omega$ will have discriminant N^2D and $j(N\omega) \in K(N^2D)$ so that $P(\omega)$ is defined over the field $K(N^2D)$ which is

big and useless; but it is actually easy to persuade ω and $N\omega$ to have the same discriminant. Simply take ω as a root of an equation of shape

$$NA\omega^2 + B\omega + C = 0,$$

then ω and $N\omega$ both have the discriminant $D = B^2 - 4NAC$, and $P(\omega) \in X_0(N)(K(D))$. Note that there is enormous freedom in choosing D.

It is inelegant to evaluate functions at complex numbers, when really they depend only on ideal classes. Fix N as a conductor, choose D as a negative discriminant so that $D = B^2 - 4NAC$ is soluble, and write $R(D)$ for the corresponding quadratic ring $Z\left[\frac{D+\sqrt{D}}{2}\right]$; then there is a primitive ideal n of $R(D)$ with norm N, fix such an ideal. Then for every ideal a of R, $P(n,a) := (j(a), j(\overline{n}a))$ is a *Heegner point* of $X_0(N)(K(D))$; we can go to and fro between the notations $P(n,a)$ and $P(\omega)$ — to every pair of ideal classes $(a, \overline{n}a)$ there corresponds a coset (ω) modulo $\Gamma_0(N)$.

Suppose now that E is an elliptic curve over Q, covered by $X_0(N)$; write $\phi : X_0(N) \to E$ for the covering map. Then $\phi(P(n,a))$ is a point of $E(K(D))$, and taking $u(D,1) := \sum_{(a)} P(n,a)$ as the $K(D)/Q(\sqrt{(}D)$ trace, we obtain a point of $E(Q(\sqrt{D}))$. More generally, if χ is a genus character, $u(e,f) := \sum \chi(a)\phi(P(n,a))$ is a point of $E(Q(\sqrt{e}))$, where e, f are determined by χ with $D = ef$; we may call the $u(e,f)$ Heegner points too. The elliptic curve E will correspond to a differential $f(z)\,dz$ on $X_0(N)$, and then the period lattice $\Lambda(E)$ of E is easily calculable as $\int_{H_1(X_0(N))} f(z)\,dz$, and $\phi(P(\omega))$ can be calculated as $\int_\omega^{i\infty} f(z)\,dz \in E(C) = C/\Lambda(E)$. So we are in good shape for actually computing the Heegner points $u(e,f)$, at least their elliptic parameters.

This is essentially the point that had been reached in 1973–75. I lectured in Rome, Paris, Kyoto, Moscow and Harvard; and the Rome talk was summarised as a short note [4]; but there was very little immediate feedback (I missed Kurčanov's paper [13]). With hindsight, I should have realised that the theory of Heegner points was a natural extension of Weber's theory of complex multiplication, worth developing for its own sake (and indeed the functorial properties of Heegner points have turned out to be immensely valuable, in particular for Kolyvagin's Euler systems [12]); but I didn't, and indeed was discouraged. There was undue concentration on the original application of Heegner points, the construction of rational points on elliptic curves and (harder) proving that the points one had constructed were non-trivial. I gave another method on these lines, Barry Mazur (in [14]) gave one which worked beautifully for quadratic twists of $X_0(11)$, and Dick Gross (in II of [9]; [9] was not published until after the discovery of the Gross-Zagier theorem, but I think the ideas of II came a year or so earlier) gave a third. Nowadays, people tend to say that there is an adequate criterion for the nontriviality of the rational Heegner point using Gross-Zagier, "one just has to check that $L'(E,1) \neq 0$"; but I've never understood why computing $L'(E,1)$ should be considered easier than the direct computation of the Heegner point as

a point of $E(C) = C/\Lambda$ (of course, Gross-Zagier shows that if one Heegner point of a given curve is non-trivial then they almost all are).

The involvement of Dick Gross marked the turning point: at last someone young enough and bright enough was thinking seriously about Heegner points! It is the logical point at which to end this lecture, and hand over to him. But it is happier to end with a bang rather than a whimper, so I need a final paragraph.

5. 1982

In 1981 and 1982, Nelson Stephens arranged a sabbatical year, and we planned a massive computation of the Heegner points of modular curves, to see what they would tell us. We actually did those computations [6], and very illuminating the results would have been — but they were anticipated by far more exciting developments.

In 1982, I got several letters from Dick (to which I replied with increasing delight).

March 1st. Dick's first letter [D] begins "I recently found an amusing method to study Heegner points on $J_0(N)$."

This included the method in II of [9]; it was exciting, because for the first time it related the index of the Heegner point in $E(Q)$ to the order of the Tate-Shafarevich group. He conjectures a not-quite-correct form of Gross Zagier and proves a tiny bit of it. This letter was only a foretaste of what was to come.

My reply [E] included "you seem to be opening so many doors that I'm almost afraid to push", which Dick correctly translated from British to American as "Get shoving, you lucky so-and-so".

May 14th. Dick's second letter [F]; it was wonderful. "I noticed some really amazing things, like the following:

1) The product $L'(E^{(\chi)}, 1)L(E^{(\chi')}, 1)$ is just the derivative at $s = 1$ of the L-series $L(E \otimes \mathrm{Ind}_F^Q \chi, s)$ ...

2) The L-series $L(E \otimes \mathrm{Ind}\, \chi, s)$ has a beautiful integral expression by Rankin's method..."

and so on for four beautiful pages, culminating with "So all one has to do is prove the formula

$$L'(f \otimes \mathrm{Ind}\, \chi, s) = \langle y_\chi, y_{\chi^{-1}} \rangle_f . \int_\chi \omega_f \wedge \overline{\omega}_f / \sqrt{D_F} . \text{"}^1$$

After that there was no going back! I replied, and got a third letter dated September 17 asking for more data; could Nelson Stephens and I supply concrete

[1] Readers of the September 6 letter printed on page 17 of this volume will see that it does not comment directly on the ideas of May 14th; instead it describes the results of relevant computations (cf. [4]), and also makes detailed comments on a preliminary version of [9].

evidence supporting the Gross-Zagier theorem-to-be? By that time, we had plenty, so I supplied it.

On December 9th, I got the news "Dear Bryan, Working with Don Zagier, I think I've assembled a proof ...." And the rest is in print.

References

[1] Alan Baker, "Linear forms in the logarithms of algebraic numbers", *Mathematika* **13** (1966), 204–216.

[2] B. J. Birch, *Diophantine analysis and modular functions*, Conference on Algebraic Geometry, Tata Institute, Bombay, 1968.

[3] B. J. Birch, "Elliptic curves and modular functions", pp. 27–32 in *Symposia Mathematica* **4**, Istituto Nazionale di Alta Matematica, New York, Academic Press, 1970.

[4] B. J. Birch, "Heegner points of elliptic curves", pp. 441–445 in *Symposia Mathematica* **15**, Istituto Nazionale di Alta Matematica, New York, Academic Press, 1975.

[5] B. J. Birch and N. M. Stephens, "Heegner's construction of points on the curve $y^2 = x^3 - 1728e^3$", in *Séminaire de Théorie des Nombres*, Paris 1981–2, edited by Marie-José Bertin, *Progress in mathematics* **38**, Boston, Birkhäuser, 1983.

[6] B. J. Birch and N. M. Stephens, "Computation of Heegner points", pp. 13–41 in *Modular forms*, edited by R. A. Rankin, Chichester, Ellis Horwood, 1984.

[7] J. W. S. Cassels, "Diophantine equations with special reference to elliptic curves", *J. London Math. Soc.* **41** (1966), 193–291.

[8] J. W. S. Cassels and A. Fröhlich (editors), *Algebraic number theory* (Brighton, 1965), London, Academic Press, 1967.

[9] B. H. Gross, "Heegner points on $X_0(N)$", pp. 87–105 in *Modular forms*, edited by R. A. Rankin, Chichester, Ellis Horwood, 1984.

[10] B. H. Gross and D. Zagier, "Heegner points and derivatives of L-series", *Invent. Math.* **84** (1986), 225–320.

[11] Kurt Heegner, "Diophantische Analysis und Modulfunktionen", *Math. Zeitschrift* **56** (1952), 227–253.

[12] V. A. Kolyvagin, "Finiteness of $E(Q)$ and Ш(E/Q) for a class of Weil curves", *Izv. Akad. Nauk SSSR* **52** (1988).

[13] P. K. Kurčanov, "The zeta-function of elliptic curves over certain abelian extensions of imaginary quadratic fields", *Mat. Sbornik* (N.S.) **102** (**144**) (1977), 56–70.

[14] Barry Mazur, "On the arithmetic of special values of L-functions", *Invent. Math.* **55** (1979), 207–240.

[15] J.-P. Serre, "Lettre à David Goss, 30 mars 2000", pp. 537–9 in *Wolf Prize in Mathematics*, vol. 2, edited by S.-S. Chern and F. Hirzebruch, River Edge, NJ, 2001.

[16] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Tokyo, Iwanami Shoten and Princeton, University Press, 1971.

[17] H. M. Stark, "A complete determination of the complex quadratic fields with class-number one", *Michigan Math. J.* **14** (1967), 1–27.

[18] Yutaka Taniyama, Problem 12 in the Japanese version of the *Proceedings of the International Symposium on Algebraic Number Theory*, Tokyo and Nikko, 1955; see also p. 399 in J.-P. Serre, *Collected papers*, v. 3, New York, Springer, 1983.

[19] H. Weber, *Lehrbuch der Algebra*, Braunschweig, Vieweg, 1908 (especially volume III).

[20] André Weil, "Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen", *Math. Annalen* **168** (1967), 149–156.

Letters and Manuscripts

[A] Letter from André Weil to Peter Swinnerton-Dyer, dated July 24, 1965.

[B] Letter from John Tate to Peter Swinnerton-Dyer, dated November 5, 1965, and reply from Peter Swinnerton-Dyer to John Tate in December.

[C] Harvard Seminar ("Mazur-Birch seminar"), Fall 1973.

[D] Letter from Dick Gross to Bryan Birch, dated March 1, 1982 (page 11 of this volume).

[E] Letter from Birch to Gross, dated May 6, 1982 (page 13 of this volume).

[F] Letter from Gross to Birch, dated May 14, 1982 (page 14 of this volume).

[G] Letter from Gross to Birch, dated Sept 17, 1982 (page 21 of this volume).

[H] Letter from Gross to Birch, dated December 1, 1982 (page 22 of this volume).

Bryan Birch
Mathematical Institute
24-29 St Giles'
Oxford OX1 3LB
United Kingdom
birch@maths.ox.ac.uk