L-Series of Elliptic Curves, the Birch–Swinnerton-Dyer Conjecture, and the Class Number Problem of Gauss

by D. Zagier

1. Elliptic curves over Q. Consider a Diophantine equation in two variables, i.e., a polynomial equation $f(x,y)=0$ with rational coefficients which we want to solve in rational numbers. Already in the works of Diophantus it is clear that the level of difficulty of this problem is very different for different classes of polynomials f. If f is quadratic, then, given one solution (x_0, y_0), one can find all solutions in terms of a rational parameter t by solving the linear equation $(1/u)f(x_0+u,\ y_0+tu)=0$ (this method was used sporadically long before, and systematically by, Diophantus). For cubic and certain quartic f, there are methods in Diophantus' works—and later much more extensively in Fermat's—for studying the rational solutions of $f=0$ and, particularly, for constructing new solutions out of known ones. For higher degree f no general method for getting solutions has ever been found. Poincaré realized that this division into three classes depends on the topology of the set of complex points of the curve X defined by the equation $f(x,y)=0$ (or rather by its projective version $f(x,y,z)=0$), i.e., on the genus g of the Riemann surface $X(\mathbf{C})$. If $g=0$ the set of rational points $X(\mathbf{Q})$, if nonempty, is isomorphic to $\mathbf{P}^1(\mathbf{Q})$. If $g=1$ then $X(\mathbf{Q})$, if nonempty, has the structure of an abelian group. (In this case the curve can always be put into the standard Weierstrass form

$$(1)\qquad y^2=4x^3-ax-b\qquad (a,b\in\mathbf{Z}),$$

and the group structure is $0=$ point at infinity, $-P=(x,-y)$ if $P=(x,y)$, $P+Q+R=0$ if $P,Q,R\in X(\mathbf{Q})$ are collinear.) If $g\geq 2$ then we know by Faltings' recent work that $X(\mathbf{Q})$ is a finite set ("Mordell conjecture"); no further structure is known. The most interesting case from a Diophantine point of view is thus $g=1$, in which case we call X an elliptic curve and write E instead of X. Here Poincaré conjectured, and Mordell proved, that the abelian group $E(\mathbf{Q})$ is finitely generated; the structure theorem for such groups then gives

$$(2)\qquad E(\mathbf{Q})\cong\mathbf{Z}^r\oplus\mathcal{F}$$

for some integer $r\geq 0$ and some finite abelian group $\mathcal{F}$. For a given curve E one can find $\mathcal{F}$ by a finite algorithm, while for r we can get upper bounds by descent (Fermat) and lower bounds by exhibiting independent solutions; if we are lucky, these agree. It is known exactly what groups $\mathcal{F}$ can occur: $\mathcal{F}$ has the structure $\mathbf{Z}/(2n-1)\mathbf{Z}$, $\mathbf{Z}/2n\mathbf{Z}$, or $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2n\mathbf{Z}$ for some $n\in\mathbf{N}$, depending on whether $4x^3-ax-b$ in (1) has $0,1$, or 3 rational roots (this is elementary), and a deep theorem of Mazur (1977) says that n is then ≤ 5, ≤ 6, or ≤ 4, respectively, all fifteen cases occurring infinitely often. As for r, it is known by recent examples of Mestre (1983, 1984) that values as large as 14 occur, and it is conjectured that all values can occur.

By (2) the number of rational solutions of $f(x,y)=0$ is finite or infinite according to whether $r=0$ or $r>0$. In fact, we can even get an asymptotic estimate for the number $\mathcal{N}(A)$ of rational solutions $P=(x,y)$ for which the numerator and denominator of x are less than A in absolute value, namely

$$(3)\qquad \mathcal{N}(A)\sim C(\log A)^{r/2}\qquad (A\to\infty)$$

with the same r as in (2) and some $C>0$. Indeed, part of the proof of (2) consists of showing that there is a positive definite quadratic form ("*height*") $h: E(\mathbf{Q})\otimes\mathbf{R}\to\mathbf{R}$ with $h(P)-\log\max\{|\mathrm{num}\ x(P)|, |\mathrm{den}\ x(P)|\}$ bounded (such an h is clearly unique). Equation (3) follows by counting points in an r-dimensional ellipsoid of diameter $\approx(\log A)^{1/2}$, the constant C being given by

$$(4)\qquad C=\frac{\pi^{r/2}}{(r/2)!}\frac{|\mathcal{F}|}{\sqrt{R}},$$

where R (the *regulator*) is the determinant of the symmetric $r\times r$ matrix defining h w.r.t. a $\mathbf{Z}$-basis of $E(\mathbf{Q})/\mathcal{F}$ (so $R=1$ if $r=0$, $R=h(P_0)$ if $r=1$ and P_0 is a generator of $E(\mathbf{Q})/\mathcal{F}$). Note that (3) yields an elementary definition of both r and the ratio $R/|\mathcal{F}|^2$ which does not refer at all to the group structure on $E(\mathbf{Q})$. As examples, we have

(a) Fermat's equation $a^3+b^3=c^3$ (which can be put into Weierstrass form $y^2=4x^3-27$ by $a=y-9$, $b=6x$, $c=y+9$); here $r=0$, $C=|\mathcal{F}|=3$;

(b) $y^2-y=x^3-x$; here $r=1$, $|\mathcal{F}|=1$, $C=8.8464916\ldots$;

(c) $y^2=4x^3-28x+25$; here $r=3$, $|\mathcal{F}|=1$, $C=6.48553546\ldots$ (cf. [2]).

2. The conjecture of Birch and Swinnerton-Dyer. Around 1960, Birch and Swinnerton-Dyer formulated a conjecture which determines r, and to some extent C, in (3). The idea is that a curve with a large value of r (or, given r, with a large value of C) has an especially large number of rational points and should therefore have a relatively large number of solutions modulo a prime p on the average as p varies. More precisely, let $N(p)$ be the number of pairs of integers $x, y \,(\mathrm{mod}\ p)$ satisfying (1) as a congruence (mod p); then the BSD conjecture in its crudest form says that we should have an asymptotic formula

$$(5) \qquad \prod_{p<x} \frac{N(p)+1}{p} \sim C_1(\log p)^r \qquad (x \to \infty)$$

analogous to (3) with the *same* r and a constant $C_1 > 0$ related to C. (The "Riemann hypothesis for elliptic curves", proved by Hasse in 1933, says that $|N(p)-p| < 2\sqrt{p}$, so at least we know that $(N(p)+1)/p \to 1$ in (5).) For a more precise formulation it is convenient to introduce the *L-series* of E. This is a Dirichlet series defined by an Euler product

$$(6) \quad L_E(s) = \prod_p{}^{*} \frac{1}{1+(N(p)-p)/p^s+p/p^{2s}} \qquad (\mathrm{Re}(s) > 3/2),$$

where * means that the Euler factor must be modified for the finitely many "bad" primes dividing $2(a^3-27b^2)$, for which (1) becomes singular modulo p. It is conjectured that $L_E(s)$ has an analytic continuation to all s. If this is so, then L_E has a Taylor expansion $L_E(s) = C_0(s-1)^m + \cdots$ for some integer $m \geq 0$ and constant $C_0 \neq 0$, and the BSD conjecture says that the order of vanishing m should equal the rank r and the constant C_0 should be given by [5]

$$(7) \qquad C_0 := \lim_{s\to 1} \frac{L_E(s)}{(s-1)^m} = \frac{R}{|\mathcal{F}|^2}\cdot\Omega\cdot S,$$

where R and $\mathcal{F}$ are as before, $\Omega > 0$ is a simple rational multiple (depending on the "bad" primes) of the elliptic integral

$$\int_\gamma^\infty \frac{dx}{\sqrt{4x^3-ax-b}}$$

($\gamma =$ largest real root of $4x^3-ax-b=0$), and S is an integer square which is supposed to be the order of a certain group Ш, the Tate–Shafarevich group of E (however, Ш is not even known to be finite!).

We are still very far from a proof of the BSD conjecture, although there are many numerical calculations supporting it (see [2] for an example and a description of the algorithms used to compute the various terms in (7)). The following partial results are known:

1. If E is a Weil curve (cf. §3), as is conjecturally always the case and verifiable in any particular case, then $L_E(1)$ is a rational multiple of Ω (note that this is compatible with (7), since if $L_E(1) \neq 0$ we should have $r = 0$, $R = 1$); in certain cases one can show that it is a rational *square* multiple.

2. If E has complex multiplication (for elliptic curves over $\mathbf{Q}$ this happens if and only if the j-invariant $1728a^3/(a^3-27b^2)$ takes on one of thirteen integral values 0, 1728, $-3375, \ldots, -262537412640768000$), then $m = 0 \Rightarrow r = 0$, i.e., if $L_E(1) \neq 0$ then (1) has only finitely many rational solutions.

3. If E is a Weil curve, then $m = 1 \Rightarrow r \geq 1$, i.e., if $L_E(1) = 0$ and $L_E'(1) \neq 0$ then (1) has infinitely many rational solutions.

4. If E is a Weil curve with $L_E(1) = 0$ and $r = 1$, then $L_E'(1)$ is a rational multiple of ΩR, and this multiple can sometimes be shown to be a square.

5. There exist curves E with $m = r = 3$, e.g., the curve $-139y^2 = x^3+10x^2-20x+8$.

Result **1** is elementary except for the statement about squares, which follows from a result of Waldspurger. Result **2** is a theorem of Coates and Wiles (1977). Results **3–5** follow from a theorem of Benedict Gross and myself, announced in [3], whose statement will be explained in the next section.

3. Heegner points. We call E a *Weil curve* if for some integer N there is a nontrivial map $\phi : X_0(N) \to E(\mathbf{C})$ defined over $\mathbf{Q}$; here $X_0(N) = \mathfrak{H}/\Gamma_0(N) \cup \{\text{cusps}\}$, where $\mathfrak{H}$ is the complex upper half-plane and $\Gamma_0(N)$ is the modular group

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \,\middle|\, c \equiv 0 \,(\mathrm{mod}\ N)\right\}.$$

Such a map exists if and only if the function

$$f(z) = \sum_{n=1}^{\infty} a(n)\, e^{2\pi i n z},$$

where $a(n)$ are the coefficients of the Dirichlet series $L_E(s)$, is a modular form of weight 2 on $\Gamma_0(N)$, i.e.,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z) \qquad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

These curves are called Weil curves because Weil (1967) proved that the standard conjectures on the analytic continuation and functional equation of the L-series of E and its twists by Dirichlet characters imply the existence of ϕ; the possibility that all elliptic curves over $\mathbf{Q}$ might arise as quotients of Jacobians of modular curves $X_0(N)$ had already been raised some years earlier by Taniyama. That a given elliptic curve is a Weil curve can be checked by a finite algorithm (this has been done in hundreds of cases), and we will assume from now on that our curves are Weil curves, since otherwise the analytic continuation of L_E is not known and the BSD conjecture makes no sense. In particular, $L_E(s)$ is entire and the *parity* of its order m at $s = 1$ is known: m is even or odd according to whether the sign of the functional equation of L_E is $+1$ or -1, and this in turn depends on whether f satisfies $f(-1/Nz) = -Nz^2 f(z)$ or $f(-1/Nz) = +Nz^2 f(z)$.

Assuming, then, the existence of ϕ, we have the following construction of points on E, due essentially to Heegner. Let $d < 0$ be the discriminant of an imaginary quadratic field K, and assume that $(d, n) = 1$ and $d \equiv \beta^2 \pmod{4N}$ for some integer β. Then the set of $z \in \mathfrak{H}$ satisfying a quadratic equation $az^2 + bz + c = 0$ with $a \equiv 0 \pmod{N}$, $b \equiv \beta \pmod{2N}$, $c \in \mathbf{Z}$, $b^2 - 4ac = d$ is $\Gamma_0(N)$-invariant and has finitely many orbits modulo $\Gamma_0(N)$. If $z_1, \ldots, z_h$ are representatives for these (h will in fact be the class number of K), then the points $\phi(z_1), \ldots, \phi(z_h) \in E(\mathbf{C})$ are defined over a certain extension (the "Hilbert class field") of K, but their sum P_d is defined over K. Moreover, under complex conjugation P_d goes to $-\epsilon P_d$, where ϵ is the sign of the functional equation of $L_E(s)$. Thus, if $\epsilon = -1$, so that by the BSD conjecture we expect $E(\mathbf{Q})$ to have odd, and hence positive, rank, then $2P_d \in E(\mathbf{Q})$, while if $\epsilon = +1$ then $2P_d$ has the form $(x, y\sqrt{d})$, with x and y rational, and therefore gives a rational point on the "twisted" curve

$$(8) \qquad E^{(d)}: dy^2 = 4x^3 - ax - b.$$

Changing the choice of β with $\beta^2 \equiv d \pmod{4N}$ changes P_d at most by sign; we will suppress this dependence in our notation. Then the result of Gross and myself mentioned in §2 says—in the case that the sign of the functional equation is -1, so that $L_E(1) = 0$ and $2P_d \in E(\mathbf{Q})$—

$$(9) \qquad L_{E^{(d)}}(1)L'_E(1) = c \cdot \Omega_{E^{(d)}} \cdot \Omega_E \cdot h(2P_d),$$

where $\Omega_{E^{(d)}}$ and Ω_E are the periods occurring in the BSD conjecture for $E^{(d)}$ and E, h is the height function on $E(\mathbf{Q})$ defined in §1, and c is a simple nonzero rational number. The number $\Omega_{E^{(d)}}\sqrt{|d|}$ is independent of d. If the sign of the functional equation of L_E is $+1$, the formula becomes

$$(10) \qquad L_E(1)L'_{E^{(d)}}(1) = c \cdot \Omega_{E^{(d)}} \cdot \Omega_E \cdot h_{E^{(d)}}(2P_d),$$

where $h_{E^{(d)}}$ is the height function on $E^{(d)}(\mathbf{Q})$. Actually, the result proved is more general in two respects: the heights are computed already on the Jacobian of $X_0(N)$, rather than on its quotient E, and the heights of the individual z_j (rather than only their sums P_d) are computed; however, since $X_0(N)$ is not, in general, elliptic, nor z_j rational over $\mathbf{Q}$, the full statement cannot be given without explaining height theory for curves of arbitrary genus and over arbitrary number fields.

Notice that (9) implies statements **3** and **4** at the end of §2. Indeed, if E is a Weil curve with $m = 1$, then the sign of the functional equation is -1 and $L'_E(1) \neq 0$; the same theorem of Waldspurger mentioned at the end of §2 implies that we can find a d such that $L_{E^{(d)}}(1) \neq 0$, and then (9) implies that P_d has nonzero height and, hence, infinite order in $E(\mathbf{Q})$. Moreover, by **1** we know that $L_{E^{(d)}}(1)/\Omega_{E^{(d)}}$ is rational, so (9) also gives the rationality of $L'_E(1)/\Omega_E h(P_d)$ in this case; if $E(\mathbf{Q})$ has rank 1, then $h(P_d)$ is a (square) integral multiple of the regulator R, and **4** follows, the statement about squares being a consequence of the corresponding statement in **1** applied to $E^{(d)}$. Note that the mysterious factor $S = |Ш|$ in (7) has disappeared and is replaced by something like the square of the index of the subgroup of $E(\mathbf{Q})$ generated by all Heegner points P_d. Finally, **5** also follows by applying (10) to the curve $E: y^2 = x^3 + 10x^2 - 20x + 8$ (which is a Weil curve with $N = 37$) and $d = -139$; here $L_E(1) \neq 0$ and $P_d = 0$, as we will prove in §4, so (10) shows that $L'_{E^{(d)}}(1)$ vanishes; since $L_{E^{(d)}}(s)$ has a functional equation with sign -1 and $L'''_{E^{(d)}}(1) \neq 0$, it follows that $m = 3$ for the curve $E^{(d)}$ (that $r = 3$ is elementary). Observe, by the way, that **5** is elementary if 3 is replaced by a smaller number: take a Weil curve with rank $r = 0$, 1, or 2; then, if $r = 0$, the number $L_E(1)$ must be nonzero (or we would have a counterexample to BSD), and this can be checked numerically; if $r = 1$ we need only check that the sign of the functional equation of L_E is -1 and that $L'_E(1)$ is nonzero; and if $r = 2$ we can prove $L_E(1) = 0$ by calculating the rational number $L_E(1)/\Omega$ in **1** and then prove $m = 2$ by verifying that the sign of the functional equation is $+1$ and $L''_E(1) \neq 0$. (For E a Weil curve, L_E and its derivatives at $s = 1$ can be computed by rapidly convergent series; cf. [2].) However, to get **5** we must show that $L'_E(1) = 0$, and this can only be done by using some such formula as (9), since the verification that a number is zero, unlike the verification that a number is nonzero, can never be carried out by numerical computation alone.

We should also say a word about the history of the above formulas. The Heegner points P_d were defined by Birch and studied extensively by Birch and Stephens from a numerical point of view; they formulated conjectures equivalent to (9) and (10) (cf. [1]). Gross was led by other considerations coming from the theory of descent to conjecture more general formulas of the same type, and he also saw that there might be some possibility of proving them by using local height theory on the modular curves $X_0(N)$ to compute the heights of Heegner points and by using the theory of modular forms (in particular, "Rankin's method") to compute the derivative of $L_E(s)L_{E^{(d)}}(s)$ at $s = 1$. He then suggested to me a systematic attack on the problem from both sides, and the collaboration took the following rather amusing course: one of us would find a method to compute one piece of the formula, on either the height or the L-series side of the formula (usually the L-series side succumbed first), and communicate it to the other, and then the form of the result would suggest the method by which a piece of the expression on the other side could be evaluated. At the end of this process, both sides of the purported equality had been calculated explicitly as a sum of about a dozen terms, some of them quite complicated; these matched perfectly, and this provided the proof—without, however, giving the least inkling of *why* the height of the Heegner point and the derivative of the L-series should have anything to do with one another. It is to be hoped that this rather unsatisfactory state of affairs will eventually change.

4. Application to the class number problem of Gauss. Of the three consequences of (9) and (10) given in §2, the last one—the assertion of the existence of a single elliptic curve with $m = 3$—appears to be the most special and least interesting. Yet it is this result which leads to the most dramatic application, the final solution of a problem stated by Gauss nearly 200 years ago. The problem concerns class numbers of binary quadratic forms and appears at first sight very remote from questions about the Diophantine analysis of cubic equations; that there is a connection is a beautiful discovery made by Goldfeld a few years ago. We review the history briefly.

In Article 303 of the *Disquisitiones* Gauss describes extensive computations of class numbers of imaginary quadratic fields (or, rather, of positive definite binary quadratic forms, an equivalent problem) and observes that the sequence of discriminants with a given class number h seems to end for each value h. Thus, the last d with $h(d) = 1$ is apparently 163, the last with $h = 2$, 427, and the last with $h = 3$, 907 (Gauss uses a different normalization, so his values look different from these). The proof of this remained an entirely open problem for over a hundred years. Around 1916, Hecke showed that

$$h(d) > C\frac{\sqrt{|d|}}{\log |d|}$$

with an effective constant C if the L-series $L_d(s) = \sum(d/n)n^{-s}$ has no zeros near $s = 1$, thus solving Gauss's problem under the assumption of the generalized Riemann hypothesis. Then, in 1933, Deuring showed that the *falseness* of the (ordinary) Riemann hypothesis would imply $h(d) > 1$ for $|d|$ large enough. This was a decisive step, for, soon after, Mordell showed that $h(d)$ goes to infinity with $|d|$ if the Riemann hypothesis is false, and Heilbronn (1934) proved the same if the generalized Riemann hypothesis is false; together with Hecke's result, this provided an unconditional proof of Gauss's claim on the finiteness of the set of d with a given value of $h(d)$. A year later Siegel proved the definitive result of this type by showing that $h(d) > C(\epsilon)|d|^{1/2-\epsilon}$ as $d \to -\infty$ for any $\epsilon > 0$. But his result, like those of Deuring, Mordell, and Heilbronn, was ineffective in a very basic sense, since it said something like this: if no L-series has a zero in the interval $[1-\epsilon/10, 1]$, then $h(d) > C_0(\epsilon)|d|^{1/2-\epsilon}$ with an effectively computable constant $C_0(\epsilon)$ by Hecke's theorem; if $L_{d_0}(s)$ has such a zero for some discriminant d_0, then $h(d) > C_1(\epsilon)|d|^{1/2-\epsilon}$ for all d, where $C_1(\epsilon)$ is given explicitly but depends on d_0. Thus, to decide, say, whether there is a $d < -907$ with $h(d) = 3$, we must either know that the generalized Riemann hypothesis is true, or else have our hands on a particular counterexample; until we have this, the problem is in some sense just as unsolved as if Siegel's result were unknown.

No further progress was made on the problem for general values of h for the next forty years, although the special (and most interesting) case of class number 1 was solved by important work of Heegner (1952) and Baker and Stark (1969); the last two authors also settled the case $h = 2$, but the methods failed for larger class numbers. The final breakthrough came in 1975, when Dorian Goldfeld proved a deep and entirely unexpected theorem to the effect that the existence of a single L-function with appropriate analytic properties and a zero of sufficiently high order at the symmetry point of its functional equation could be used to give an effective lower bound for $h(d)$ which goes to infinity as $d \to -\infty$. What Gross and I did was to produce such a function.

Goldfeld's argument is a long and difficult piece of analytic number theory. A simplification and very clear exposition of it was given in a recent Bourbaki talk by Joseph Oesterlé [4], which we recommend to the interested reader (this paper also contains references to Goldfeld's work and to previous work on the class number problem). Here we give only a brief indication of the way that the L-series with a triple zero is used to obtain analytic information. Suppose we have a discriminant d with $|d|$ very large; we want to show that $h = h(d)$ is also large. We may assume that the Legendre symbol $(d/37)$ is 0 or -1, because if $(d/37) = 1$ then 37 is the norm of a prime ideal $\mathfrak{p}$ in $\mathbf{Q}(\sqrt{d})$ and 37^h is the norm of the principal ideal $\mathfrak{p}^h$ and, hence, the norm of an integer $(x + y\sqrt{d})/2$ ($x, y \in \mathbf{Z}$, $y \neq 0$), so

$$37^h = \frac{x^2 + y^2|d|}{4} > \frac{|d|}{4},$$

and we already have the desired effective lower bound for h. From $(d/37) = 0$ or -1 it follows that the L-series of $E^{(d)}$, where E is the particular elliptic curve mentioned in 5 of §2, has a minus sign in its functional equation and, hence, the product $L(s) = L_E(s)L_{E^{(d)}}(s)$ has a functional equation with a plus sign (say $\gamma(s)L(s) = +\gamma(2-s)L(2-s)$ with an appropriate Γ-factor $\gamma(s)$) and a zero of order at least 4 at $s = 1$. On the other hand, the same argument which gave $(d/37) \neq 1$ shows that $(d/p) = -1$ for all small primes $p \nmid d$ (namely all $p < |d/4|^{1/h}$; in fact, with an argument given in [4, p. 10], one can extend this to all $p < |d/4|^{1/(\sqrt{2h}+1)}$ with at most one exception). This means that $(d/n) = \lambda(n)$ for most small integers n, where $\lambda(n)$ is the Liouville function, defined by $\lambda(p_1 \cdots p_r) = (-1)^r$ for any primes $p_1, \ldots, p_r$. But $L_{E^{(d)}}(s)$ is the twist of $L_E(s)$ by $(d/\cdot)$ (i.e., if $L_E(s) = \sum a(n)n^{-s}$, then $L_{E^{(d)}}(s) = \sum \tilde{a}(n)n^{-s}$ with $\tilde{a}(n) = (d/n)a(n)$ for all n prime to d), so this means that the function $\mathcal{L}(s)$ should not differ too much from the function $\mathcal{R}(s) = L_E(s)L_{E,\lambda}(s)$, where $L_{E,\lambda}(s) = \sum \lambda(n)a(n)n^{-s}$ ("not too much" can be made precise by an analysis of the Dedekind zeta-function of $\mathbf{Q}(\sqrt{d})$). The function $\mathcal{R}(s)$ is nothing other than the Rankin zeta-function of the modular form $\sum a(n)e^{2\pi i n z}$ associated to the elliptic curve E and has been extensively studied in the theory of modular forms. In particular, it is known to have a meromorphic continuation with all poles to the left of the line $\mathrm{Re}(s) = 1$ and a simple zero at $s = 1$. Since $\mathcal{L}(s)$ has at least a quadruple zero at $s = 1$, the functions $\mathcal{L}(s)$ and $\mathcal{R}(s)$ do *not* have the same qualitative behavior, and this contradicts the above assertion that $\mathcal{L}(s)$ and $\mathcal{R}(s)$ are close to one another if h is very small compared to $|d|$. The actual contradiction is obtained by comparing the two integrals

$$\int_{C-i\infty}^{C+i\infty} \frac{\gamma(s)\mathcal{L}(s)}{(s-1)^3}\,ds \quad \text{and} \quad \int_{C-i\infty}^{C+i\infty} \frac{\gamma(s)\mathcal{R}(s)}{(s-1)^3}\,ds$$

(C any constant > 1). The first is identically zero because the fact that $\mathrm{ord}_{s=1}\,\mathcal{L}(s) \geq 3$ permits us to move the path of integration from $\mathrm{Re}(s) = C > 1$ to $\mathrm{Re}(s) = 2 - C < 1$, and then the oddness of the integrand under $s \to 2 - s$ implies that the integral is minus itself. The second integral is nonzero because it is dominated by the nontrivial residue at $s = 1$; this residue has the form $A \log |d| + B$, because $\mathcal{R}(s)$ is independent of d and $\gamma(s)$ has the form $|d|^s \gamma_0(s)$, with $\gamma_0(s)$ independent of d. On the other hand, by estimating the difference of $\mathcal{L}(s)$ and $\mathcal{R}(s)$, one can show that the difference of the two integrals is $O(h)$, and together this leads to the desired contradiction if $|d|$ is large enough. Actually, we have somewhat oversimplified the picture, and the analytic details are more complicated if d is composite. The final result obtained in [4] is the estimate

$$h(d) > C \cdot \prod_{p|d}\left(1 - \frac{2}{\sqrt{p}}\right) \cdot \log |d|$$

for all d, where C is an absolute and effectively computable constant (Goldfeld's original result was somewhat weaker), and, in particular, $h(-p) > C' \log p$ for p prime. Good numerical values for C and C' have not yet been obtained, but this should soon be done.

Finally, we give the proof—postponed in §3—that the Heegner point P_{-139} vanishes on an elliptic curve of conductor 37. One can check whether $P_d = 0$ on any Weil curve and for any d by a finite computation, but here there is a pretty argument, found by Gross, which requires essentially no calculation. The class number of -139 is 3, and for the three points z_j defined in §2 (with $N = 37$ and $\beta = 3$) we can choose

$$\frac{-3 + i\sqrt{139}}{2 \cdot 37}, \frac{71 + i\sqrt{139}}{10 \cdot 37} \text{ and } \frac{-151 + i\sqrt{139}}{10 \cdot 37}.$$

These satisfy $37z = (az + b)/(cz + d)$ with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} -3 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -77 & -31 \\ 5 & 2 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 34 & -7 \\ 5 & -1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$, respectively, the value of $(cz + d)^{-1}$ in each case being $(3 + i\sqrt{139})/2$. From the well-known transformation equation

$$\Delta\left(\frac{az + b}{cz + d}\right) = (cz + d)^{12}\Delta(z)$$

of the "discriminant" function

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} \qquad (q = e^{2\pi i z},\ z \in \mathfrak{H}),$$

it now follows that the function

$$\begin{aligned} g(z) &= \sqrt[12]{\frac{\Delta(z)}{\Delta(37z)}} - \frac{3 + i\sqrt{139}}{2} \\ &= q^{-3} \prod_{n=1}^{\infty} \left(\frac{1 - q^n}{1 - q^{37n}}\right)^2 - \frac{3 + i\sqrt{139}}{2} \end{aligned}$$

vanishes at z_1, z_2, and z_3. On the other hand, $g(z)$ is $\Gamma_0(37)$-invariant, has a triple pole at $z = \infty$, and has no other poles (since $\Delta \neq 0$ in $\mathfrak{H}$), so these are the only three zeros. Therefore, $(z_1) + (z_2) + (z_3) - 3(\infty)$ is a principal divisor on $X_0(37)$, so $\phi(z_1) + \phi(z_2) + \phi(z_2) = 0 \in E(\mathbf{C})$ for any map ϕ from $X_0(37)$ to an elliptic curve E with $\phi(\infty) = 0$.

Suggested Reading

1. B. Birch and N. Stephens, *Heegner's construction of points on the curve $y^2 = x^3 - 1728e^3$* (Séminaire de Théorie des Nombres, Paris, 1981-1982), Progress in Math., Vol. **38**, Birkhäuser, Boston-Basel-Stuttgart, 1983, pp. 1–19.

2. J. Buhler, B. Gross and D. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3*, Math. Comp. (to appear).

3. B. Gross and D. Zagier, *Points de Heegner et dérivées de fonctions L*, C. R. Acad. Sci. Paris **297** (1983), 85–87.

4. J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Séminaire Nicolas Bourbaki 1983-1984, Exposé 631, Astérisque (to appear).

5. J. Tate, *Arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.