$y^2 = x^3$, and so we might be tempted to take 1 for the Euler factor at 2 as well. However, this is wrong. When one defines $L(E, s)$, if there exists a $\mathbb{Q}$-linear change of variables that takes our equation E: $y^2 = x^3 + 16$ in $\mathbb{P}^2_{\mathbb{Q}}$ to a curve C whose reduction mod p is smooth, then we are obliged to say that E has good reduction at p and to form the corresponding Euler factor from the zeta-function of C over $\mathbb{F}_p$. In Problem 22 of §II.2, we saw that $y^2 = x^3 + 16$ is equivalent over $\mathbb{Q}$ to $y^2 + y = x^3$, a smooth curve over $\mathbb{F}_2$ whose zeta-function we computed. Show that the Euler factor at $p = 2$ is given by the same formula as in part (a).

(c) For $x \in \mathbb{Z}[\omega]$ prime to 3, let $\chi(x) = (-\omega)^j$ be the unique sixth root of 1 such that $x\chi(x) \equiv 1 \pmod 3$. Let $\chi(x) = 0$ for x in the ideal $(\sqrt{-3})$. Show that

$$L(E, s) = \frac{1}{6} \sum_{x \in \mathbb{Z}[\omega]} \frac{\chi(x)x}{(\mathbb{N}x)^s}.$$

(d) Let

$$\psi(x) \underset{\text{def}}{=} e^{(2\pi i/3)\,\mathrm{Tr}(x/i\sqrt{3})},$$

where $\mathrm{Tr}\, x = x + \bar{x} = 2\,\mathrm{Re}\, x$. Verify that $\psi(x)$ is an additive character of $\mathbb{Z}[\omega]/3$ satisfying the condition in Problem 9 of §II.2 (i.e., that it is nontrivial on any larger ideal than (3)). Find the value of $g(\chi, \psi) = \sum_{x \in \mathbb{Z}[\omega]/3} \chi(x)\psi(x)$, where χ is as in part (b).

8. (a) Let $w = (1, \omega)$, $u \in \mathbb{R}^2 - \mathbb{Z}^2$, and $t > 0$ be fixed. What is the Fourier transform of $g(x) = (x + u)\cdot w e^{-\pi t|(x+u)\cdot w|^2}$?

(b) Let $\theta_u(t) = \sum_{m \in \mathbb{Z}^2} g(m)$, where $g(x)$ is as in part (a). Find the Mellin transform $\phi(s)$ of

$$\sum_{\substack{u=(a/3,b/3)\\ 0 \le a,b < 3}} \chi(a + b\omega)\theta_u(t).$$

(c) Prove that $L(E, s)$ is an entire function, where E: $y^2 = x^3 + 16$ is the elliptic curve in Problem 7.

(d) Prove the functional equation $\Lambda(s) = \Lambda(2 - s)$ with

$$\Lambda(s) \underset{\text{def}}{=} \left(\frac{\sqrt{27}}{2\pi}\right)^s \Gamma(s) L(E, s).$$

§6. The critical value

The value at $s = 1$ of the Hasse–Weil L-function $L(E, s)$ of an elliptic curve E is called the "critical value". When we have a functional equation relating $L(E, s)$ to $L(E, 2 - s)$, the point $s = 1$ is the "center" of the functional equation, in the sense that it is the fixed point of the correspondence $s \leftrightarrow 2 - s$. The importance of this critical value comes from the following famous conjecture.

Conjecture (B. J. Birch and H. P. F. Swinnerton-Dyer). $L(E, 1) = 0$ *if and only if E has infinitely many rational points.*

In this conjecture E is any elliptic curve defined over $\mathbb{Q}$. In the general case it has not even been proved that it makes sense to speak of $L(E, 1)$, because no one has been able to prove analytic continuation of $L(E, s)$ to the left of the line Re $s = \frac{3}{2}$. However, analytic continuation and a functional equation have been proved for any elliptic curve with complex multiplication (see Problem 8 of §I.8), of which our E_n are special cases, and for a broader class of elliptic curves with a so-called "Weil parametrization" by modular curves. (It has been conjectured by Weil and Taniyama that the latter class actually consists of all elliptic curves defined over $\mathbb{Q}$.)

We shall call the above conjecture the "weak Birch–Swinnerton-Dyer conjecture", because Birch and Swinnerton-Dyer made a much more detailed conjecture about the behavior of $L(E, s)$ at $s = 1$. Namely, they conjectured that the *order* of zero is equal to the *rank* r of the group of rational points on E (see the beginning of §I.9). Moreover they gave a conjectural description of the coefficient of the first nonvanishing term in the Taylor expansion at $s = 1$ in terms of various subtle arithmetic properties of E. For a more detailed discussion of the conjecture of Birch and Swinnerton-Dyer, see [Birch 1963], [Birch and Swinnerton-Dyer 1963, 1965], [Cassels 1966], [Swinnerton-Dyer 1967], [Tate 1974].

There is a simple heuristic argument—far from a proof—which shows why the weak Birch–Swinnerton-Dyer conjecture might be true. Let us pretend that the Euler product for $L(E, s)$ (see (5.1) for the case $E = E_n$) is a convergent infinite product when $s = 1$ (which it isn't). In that case we would have:

$$L(E, 1) = \prod_p \frac{1}{1 - 2a_{E,p}p^{-s} + p^{1-2s}}\bigg|_{s=1} = \prod_p \frac{p}{p + 1 - 2a_{E,p}} = \prod_p \frac{p}{N_p},$$

where $N_p = N_{1,p} = p + 1 - 2a_{E,p}$ is the number of $\mathbb{F}_p$-points on the elliptic curve E considered modulo p. Now as p varies, the N_p "straddle" p at a distance bounded by $2\sqrt{p}$. This is because $2a_{E,p} = \alpha_p + \bar{\alpha}_p$, and the reciprocal roots α_p have absolute value $\sqrt{p}$ (see (2.7) for $E = E_n$, and the discussion of the Weil conjectures in §1 for the general case). Thus, roughly speaking, $N_p \approx p \pm \sqrt{p}$. If N_p spent an equal time on both sides of p as p varies, one could expect the infinite product of the p/N_p to converge to a nonzero limit. (See Problem 1 below.) If, on the other hand, the N_p had a tendency to be on the large side: $N_p \approx p + \sqrt{p}$, then we would obtain $L(E, 1) \approx \Pi_p p/(p + \sqrt{p}) = \Pi_p 1/(1 + p^{-1/2}) = 0$.

To conclude this heuristic argument, we point out that, if there are infinitely many rational points, one would expect that by reducing them modulo p (as in the proof of Proposition 17 in §I.9) we would obtain a large guaranteed contribution to N_p for all p, thereby ensuring this lopsided behavior $N_p \approx p + \sqrt{p}$. On the other hand, if there are only finitely many rational points, then their contribution to N_p would be negligible for large p, so that N_p would have the "random" behavior $N_p \approx p \pm \sqrt{p}$. Needless to say, this heuristic argument is not of much help in trying to prove the weak Birch–Swinnerton-Dyer conjecture.

But there is considerable evidence, both computational and theoretical to support the conjecture of Birch and Swinnerton-Dyer. The most dramatic partial result so far was the proof in 1977 by John Coates and Andrew Wiles that for a large class of elliptic curves, an infinite number of rational points implies that $L(E, 1) = 0$. Other major advances have been obtained in [Greenberg 1983] and [Gross and Zagier 1983].

Recall from Problem 8 of §I.8 that an elliptic curve is said to have complex multiplication if its lattice is taken to itself under multiplication by some complex numbers other than integers.

Theorem (J. Coates and A. Wiles). *Let E be an elliptic curve defined over $\mathbb{Q}$ and having complex multiplication. If E has infinitely many $\mathbb{Q}$-points, then* $L(E, 1) = 0$.

The proof of this theorem is rather difficult (see [Coates and Wiles 1977]), and it will not be given here. (The original proof further assumed that the quadratic imaginary field of complex multiplication has class number 1, but this turned out not to be necessary.)

Since our curves E_n have complex multiplication, the Coates–Wiles theorem applies, and, in view of Proposition 18 of Chapter I, tells us that if $L(E_n, 1) \neq 0$, then n is not a congruent number. Conversely, if we allow ourselves the weak Birch–Swinnerton-Dyer conjecture, then it follows that $L(E_n, 1) = 0$ implies that n is a congruent number.

There is one situation in which it is easy to know that $L(E_n, 1) = 0$. Recall that the "root number"—the plus or minus sign in the functional equation for $L(E_n, s)$—is equal to $(\frac{-2}{n})$ for n odd, and $(\frac{-1}{n_0})$ for $n = 2n_0$ even (see the theorem in §5).

Proposition 12. *If $n \equiv 5$, 6 or 7 (mod 8), and if the weak Birch–Swinnerton-Dyer conjecture holds for E_n, then n is a congruent number.*

Proof. According to the theorem in §5, if $n \equiv 5, 6, 7 \pmod 8$, then $\Lambda(s) = -\Lambda(2 - s)$, where $\Lambda(s)$ is given by (5.11). Substituting $s = 1$, we conclude that $\Lambda(1) = -\Lambda(1)$, i.e., $\Lambda(1) = 0$. But by (5.11), $\Lambda(1)$ differs from $L(E_n, 1)$ by a nonzero factor (namely, $\sqrt{N}/2\pi$). Thus, $L(E_n, 1) = 0$, and the weak Birch–Swinnerton-Dyer conjecture then tells us that E_n has infinitely many $\mathbb{Q}$-points, i.e., by Proposition 18 of Chapter I, n is a congruent number. □

In certain cases, the claim that all $n \equiv 5, 6, 7 \pmod 8$ are congruent numbers has been verified without assuming the weak Birch–Swinnerton-Dyer conjecture. A method due to Heegner (see [Birch 1975]) for constructing points on E_n enables one to prove this claim for n equal to a prime or twice a prime. That is, if n is a prime congruent to 5 or 7 modulo 8, or twice a prime congruent to 3 mod 4, then n is known to be a congruent number.

It is interesting to note that even in the cases when Heegner's method ensures us that n is a congruent number, the method does not give us an effective algorithm for constructing a nontrivial rational point on E_n, or equivalently, finding a right triangle with rational sides and area n.

Very recently, Gross and Zagier were able to improve greatly upon Heegner's method. As a special case of their results, they showed that for $n \equiv 5, 6, 7 \pmod 8$ the elliptic curve E_n has infinitely many rational points provided that $L(E_n, s)$ has only a simple zero at $s = 1$, i.e., $L'(E_n, 1) \neq 0$. This result represents substantial progress in making Proposition 12 unconditional. Moreover, their method is constructive, i.e., it gives you a rational point on the curve (equivalently, a right triangle with area n) when $L'(E_n, 1) \neq 0$. See [Gross and Zagier 1983].

In the cases when the root number is $+1$, we cannot be sure in advance whether $L(E_n, 1)$ is zero or nonzero. So in those cases it is useful to have an efficient algorithm for computing $L(E_n, 1)$, at least to enough accuracy to know for certain that it is nonzero. (It is harder to be sure of ourselves in cases when the critical value seems to be zero.) We cannot use the series (5.3) or (5.8) to evaluate $L(E_n, 1)$, since they only converge when Re $s > \frac{3}{2}$.

So we now turn our attention to finding a rapidly convergent expression for $L(E_n, 1)$.

Let us return to the functional equation for $L(E_n, s)$, and give a slightly different, more efficient proof. Recall that

$$L(E_n, s) = \frac{1}{4} \sum_{x \in \mathbb{Z}[i]} \tilde{\chi}_n(x)(\mathbb{N}x)^{-s}$$

with $\tilde{\chi}_n(x) = x\chi'_n(x)$, where χ'_n was defined in (3.3)–(3.4). Suppose we ask the question, "What function $F(E_n, t)$ has $\pi^{-s}\Gamma(s)L(E_n, s)$ as its Mellin transform?" By our usual method using (4.6), we see that the answer is

$$F(E_n, t) \underset{\text{def}}{=} \frac{1}{4} \sum_{x \in \mathbb{Z}[i]} \tilde{\chi}_n(x) e^{-\pi t |x|^2}. \tag{6.1}$$

We now proceed to find a functional equation for $F(E_n, t)$, which will then immediately give us once again our functional equation for the Mellin transform $L(E_n, s)$. The only difference with our earlier derivation is whether we take the character sum before or after applying the functional equation (compare with the two derivations in Problems 3 and 5 of §II.4 and in Problems 4 and 6 for the functional equation for a Dirichlet L-series).

Recall that $\chi'_n(x)$ is a primitive character of $(\mathbb{Z}[i]/n')^*$, where $n' = (2 + 2i)n$ for n odd, $n' = 2n$ for n even. Let $a + bi$ run through some set of coset representatives of $\mathbb{Z}[i]$ modulo n', and for each $a + bi$ define a corresponding pair (u_1, u_2) of rational numbers by: $u_1 + u_2 i = (a + bi)/n'$. Replacing x by $a + bi + n'(m \cdot (1, i))$ for $m \in \mathbb{Z}^2$, and setting

$$N' = |n'|^2 = \frac{N}{4} \tag{6.2}$$

(see (5.10)), we can rewrite $F(E_n, t)$ as follows:

$$F(E_n, t) = \frac{n'}{4} \sum_{a+bi \in \mathbb{Z}[i]/n'} \chi'_n(a + bi) \sum_{m \in \mathbb{Z}^2} (m + u) \cdot (1, i) e^{-\pi N' t |m+u|^2}.$$

If we replace t by $\frac{1}{N't}$, the summand in the inner sum becomes $\theta_u(\frac{1}{t})$ in the notation of (5.13). We then use the functional equation (5.16) for $\theta_u(\frac{i}{t})$. As a result we obtain:

$$F\left(E_n, \frac{1}{N't}\right) = \frac{n'}{4} \sum_{a+bi} \chi_n'(a+bi)(-it^2) \sum_m m\cdot(1, i) e^{2\pi i m\cdot u} e^{-\pi t|m|^2}$$
$$= -\frac{i}{4} t^2 n' \sum_m m\cdot(1, i) e^{-\pi t|m|^2} \sum_{a+bi} \chi_n'(a+bi) e^{2\pi i m\cdot u}.$$

Now $m \cdot u = \mathrm{Re}((m_1 - m_2 i)(u_1 + u_2 i)) = \mathrm{Re}((m_1 - m_2 i)(a+bi)/n')$. We now use Problem 2 of §II.2 to rewrite the last inner sum as

$$\bar{\chi}_n'(m_1 - m_2 i) \sum_{a+bi} \chi_n'(a+bi) e^{2\pi i\, \mathrm{Re}((a+bi)/n')}.$$

But $\bar{\chi}_n'(m_1 - m_2 i) = \chi_n'(m_1 + m_2 i)$, and the sum here is the Gauss sum $g(\chi_n')$ evaluated in Proposition 4 (see (3.9)). We finally obtain:

$$F\left(E_n, \frac{1}{N't}\right) = -\frac{i}{4} t^2 n'(\varepsilon n') \sum_{m\in\mathbb{Z}^2} \tilde{\chi}_n(m_1 + m_2 i) e^{-\pi t|m|^2},$$

where the ε is $(\frac{-2}{n})$ for n odd, $i(\frac{-1}{n_0})$ for $n = 2n_0$ even. Replacing $m_1 + m_2 i$ by $x \in \mathbb{Z}[i]$, we see that the sum is precisely $4F(E_n, t)$. Thus, we have

$$F\left(E_n, \frac{1}{N't}\right) = \begin{cases} \left(\dfrac{-2}{n}\right) N't^2 F(E_n, t), & n \text{ odd}; \\ \left(\dfrac{-1}{n_0}\right) N't^2 F(E_n, t), & n = 2n_0 \text{ even}. \end{cases} \tag{6.3}$$

We can easily derive the functional equation for $L(E_n, s)$ from (6.3). We shall write $\pm$ to denote $(\frac{-2}{n})$ for n odd, $(\frac{-1}{n_0})$ for $n = 2n_0$ even. We have

$$\pi^{-s}\Gamma(s)L(E_n, s) = \int_0^\infty t^s F(E_n, t)\frac{dt}{t} = \pm\frac{1}{N'}\int_0^\infty t^{s-2} F\left(E_n, \frac{1}{N't}\right)\frac{dt}{t}$$

by (6.3). Making the change of variables $u = \frac{1}{N't}$, we obtain:

$$\pi^{-s}\Gamma(s)L(E_n, s) = \pm N'^{1-s}\int_0^\infty u^{2-s} F(E_n, u)\frac{du}{u}$$
$$= \pm N'^{1-s}\pi^{s-2}\Gamma(2-s)L(E_n, 2-s).$$

Finally, replacing N'^{1-s} by $(\sqrt{N}/2)^{2-2s}$ and multiplying both sides by $(\sqrt{N}/2)^s$, we obtain the functional equation of (5.11)–(5.12).

We now use our function $F(E_n, t)$ in the case when the root number is $+1$, i.e., $n \equiv 1, 2, 3 \pmod 8$, in order to find a convenient expression for $L(E_n, 1)$. Thus, suppose that

$$F\left(E_n, \frac{1}{N't}\right) = N't^2 F(E_n, t). \tag{6.4}$$

We use this functional equation to break up the Mellin transform of $F(E_n, t)$

into two integrals from $\frac{1}{\sqrt{N'}}$ to ∞. The point $\frac{1}{\sqrt{N'}}$ is the "center" of the functional equation, i.e., the fixed point of the correspondence $t \leftrightarrow \frac{1}{N't}$.

We have:

$$\pi^{-s}\Gamma(s)L(E_n, s) = \int_0^\infty t^s F(E_n, t)\frac{dt}{t} = \int_{1/\sqrt{N'}}^\infty + \int_0^{1/\sqrt{N'}} t^s F(E_n, t)\frac{dt}{t}.$$

In the second integral we replace t by $\frac{1}{N't}$, and then use (6.4) to write $F(E_n, \frac{1}{N't})$ in terms of $F(E_n, t)$. The result is:

$$\pi^{-s}\Gamma(s)L(E_n, s) = \int_{1/\sqrt{N'}}^\infty (t^s F(E_n, t) + N'^{1-s}t^{2-s}F(E_n, t))\frac{dt}{t}.$$

Now set $s = 1$. Multiplying both sides by π, we immediately obtain:

$$L(E_n, 1) = 2\pi \int_{1/\sqrt{N'}}^\infty F(E_n, t)dt. \tag{6.5}$$

Recall that the Hasse–Weil L-function can be written as a Dirichlet series

$$L(E_n, s) = \sum_{m=1}^\infty b_{m,n}m^{-s}, \quad \text{where} \quad b_{m,n} = \frac{1}{4}\sum_{\substack{x\in\mathbb{Z}[i] \\ N x=m}} \tilde{\chi}_n(x). \tag{6.6}$$

Comparing with the definition (6.1) of $F(E_n, t)$, we see that

$$F(E_n, t) = \sum_{m=1}^\infty b_{m,n}e^{-\pi t m}. \tag{6.7}$$

We can now substitute the series (6.7) into (6.5) and integrate term by term. (Notice that the procedure below will work only because we have a *positive* lower limit of integration in (6.5); if we tried directly to use the Mellin transform, in which the lower limit of integration is 0, we would not have convergence.) Using the formula $\int_a^\infty e^{-ct}dt = \frac{1}{c}e^{-ac}$ with $a = N'^{-1/2}$, $c = \pi m$, we immediately obtain the following rapidly convergent infinite series for $L(E_n, 1)$.

Proposition 13. *The critical value of the Hasse–Weil L-function of the elliptic curve* E_n: $y^2 = x^3 - n^2x$ *for squarefree* $n \equiv 1, 2, 3 \pmod 8$ *is given by*:

$$L(E_n, 1) = 2\sum_{m=1}^\infty \frac{b_{m,n}}{m}e^{-\pi m/\sqrt{N'}}, \quad \textit{where} \quad \sqrt{N'} = \begin{cases} 2n\sqrt{2}, & n \textit{ odd;} \\ 2n, & n \textit{ even.}\end{cases} \tag{6.8}$$

Here the coefficients $b_{m,n}$ *are the Dirichlet series coefficients obtained by expanding*

$$L(E_n, s) = \prod_{p\nmid 2n}(1 - 2a_{E_n,p}p^{-s} + p^{1-2s})^{-1} = \sum_{m=1}^\infty b_{m,n}m^{-s}.$$

In addition, the absolute value of the coefficient $b_{m,n}$ *is bounded by* $\sigma_0(m)\sqrt{m}$, *where* $\sigma_0(m)$ *denotes the number of divisors of* m.

PROOF. We have already proved all except for the bound on $b_{m,n}$. If we write the Euler factor in the form $(1-\alpha_p p^{-s})^{-1}(1-\bar{\alpha}_p p^{-s})^{-1}$, expand each factor in a geometric series, and collect coefficients of p^{-es} for each positive integer e, we find that the coefficient of p^{-es} is $\alpha_p^e + \alpha_p^{e-1}\bar{\alpha}_p + \alpha_p^{e-2}\bar{\alpha}_p^2 + \cdots + \bar{\alpha}_p^e$. This means that, if m has prime factorization $m = p_1^{e_1}\cdots p_r^{e_r}$, then

$$b_{m,n} = \prod_{j=1}^{r} (\alpha_{p_j}^{e_j} + \alpha_{p_j}^{e_j-1}\bar{\alpha}_{p_j} + \cdots + \bar{\alpha}_{p_j}^{e_j}).$$

Since $|\alpha_p| = |\bar{\alpha}_p| = \sqrt{p}$ for all p, we immediately obtain the bound

$$|b_{m,n}| \le \prod_{j=1}^{r} (e_j+1)p_j^{e_j/2} = \sigma_0(m)\sqrt{m},$$

where we have used the easy fact from elementary number theory that $\sigma_0(m)$ is the product of the (e_j+1). This completes the proof. □

The bound for $b_{m,n}$ is useful in estimating the remainder after we compute the series in (6.8) out to the M-th place. In particular, if we find that the remainder is less than the value of that partial sum, we may conclude that $L(E_n, 1) \neq 0$.

As an example, we treat the case $n = 1$. The first few Dirichlet series coefficients b_m for $L(E_1, s)$ are given in (5.4). By (6.8), we have

$$\begin{aligned} L(E_1, 1) &\\ &= 2(e^{-\pi/2\sqrt{2}} - \tfrac{2}{5}e^{-5\pi/2\sqrt{2}} - \tfrac{1}{3}e^{-9\pi/2\sqrt{2}} + \tfrac{6}{13}e^{-13\pi/2\sqrt{2}} + \tfrac{2}{17}e^{-17\pi/2\sqrt{2}} + \cdots) \\ &= 0.6555143\ldots + R_{25}, \end{aligned}$$

where we have denoted $R_M = 2\sum_{m\ge M}\frac{b_m}{m}e^{-\pi m/2\sqrt{2}}$.

A very crude estimate for $\sigma_0(m)$ is $2\sqrt{m}$ (see the problems). Thus,

$$|R_M| \le 4\sum_{m\ge M} e^{-\pi m/2\sqrt{2}} = \frac{4}{1-e^{-\pi/2\sqrt{2}}}e^{-\pi M/2\sqrt{2}}.$$

So R_{25} is bounded by 5.2×10^{-12}. Actually, the convergence is so fast that we only needed to evaluate the first term to show that $L(E_1, 1) \neq 0$:

$$L(E_1, 1) = 0.6586\ldots + R_5, \quad \text{with} \quad |R_5| \le 0.023.$$

This computation, together with the Coates–Wiles theorem, then tells us that 1 is not a congruent number. In fact, this argument undoubtedly qualifies as the world's most roundabout proof of that fact, which was proved by Fermat more than three hundred years ago. (See [Weil 1973, p. 270 of Vol. III of Collected Papers]; see also Problem 3 of §I.1.)

The next topic we take up is the systematic study of functions such as theta-series which have certain types of functional equations under $t \mapsto \frac{1}{t}$ and similar changes of variable. Such functions are called "modular forms". Actually, modular forms are functions of the form $\sum b_m e^{2\pi i z}$ rather than

$\Sigma b_m e^{-\pi t}$, but the simple substitution $t = -2iz$ will transform our theta-series from this chapter into what turns out to be modular forms.

In studying modular forms, we will at the same time be approaching elliptic curves from another perspective. But these two aspects of elliptic curves—the congruence zeta-function and Hasse–Weil L-series, and the theory of modular forms—have combined in recent years to form a richly interlocking picture.

PROBLEMS

1. In the heuristic argument for the weak Birch–Swinnerton-Dyer conjecture, make the following ridiculous assumptions: (i) $|2a_{E,p} - 1| = \sqrt{p}$; and (ii) $(2a_{E,p} - 1)/\sqrt{p} = \pm 1$ is "evenly" distributed, and happens to coincide with the value at p of a fixed quadratic Dirichlet character $\chi(p) = (\frac{p}{N})$ for some fixed N. (One of the reasons why these assumptions are ridiculous is that $2a_{E,p}$ is an integer.) Show that then $L(E, 1)$ is equal to the value $L(\chi, \frac{1}{2})$ of the Dirichlet L-function at the center of symmetry of its functional equation.

2. Prove that if the root number in the functional equation for $L(E_n, s)$ is 1, then $L(E_n, s)$ has either a nonzero value or else an even-order zero at $s = 1$; and if the root number is -1, then $L(E_n, s)$ has an odd-order zero at $s = 1$.

3. In the notation of Proposition 13 (here we abbreviate $b_m = b_{m,n}$, $a_p = a_{E_n,p}$), prove that:
   (a) $b_p = 2a_p$ if $p \nmid 2n$; $b_p = 0$ if $p | 2n$;
   (b) $b_{m_1 m_2} = b_{m_1} b_{m_2}$ if m_1 and m_2 are relatively prime;
   (c) $b_{p^{e+1}} = 2a_p b_{p^e} - p b_{p^{e-1}}$ for $e \geq 0$ (here take $b_{1/p} = 0$ when $e = 0$).

4. Prove that $\sigma_0(m) < 2\sqrt{m}$ for all m, and that $m^{-\varepsilon}\sigma_0(m) \to 0$ as $m \to \infty$ for any positive ε.

5. Compute $L(E_2, 1)$ and $L(E_3, 1)$ to about three decimal places of accuracy, verifying that they are nonzero.

6. Prove that $L(E_{10}, 1) \neq 0$.

7. Suppose you knew a lower bound c for the absolute value of all nonzero $L(E_n, 1)$, $n = 1, 2, 3, \ldots$ squarefree. (No such c is known.) For n very large, what is the order of magnitude of M such that you could determine from the first M terms in (6.8) whether or not $L(E_n, 1) = 0$?

8. (a) Write a flow chart for a computer program that evaluates $L(E_n, 1)$ through the M-th term of (6.8) and estimates the remainder.
   (b) If you have a computer handy, use part (a) to find $L(E_{41}, 1)$ to three decimal places.