Proposition 7. *The theta-function satisfies the functional equation*

$$\theta(t) = \frac{1}{\sqrt{t}}\theta(1/t). \tag{4.10}$$

PROOF. We apply Poisson summation to $g(x) = e^{-\pi t x^2}$ for fixed $t > 0$. We write $g(x) = f(\sqrt{t}x)$ with $f(x) = e^{-\pi x^2}$. By Proposition 5 and property (3) of the Fourier transform (with $b = \sqrt{t}$) we have $\hat{g}(y) = t^{-1/2}e^{-\pi y^2/t}$. Then the left side of (4.8) is $\theta(t)$, and the right side is $t^{-1/2}\theta(1/t)$. This proves the proposition. □

We sometimes want to consider $\theta(t)$ for complex t, where we assume that $\operatorname{Re} t > 0$ in the definition (4.9). The functional equation (4.10) still holds for complex t, by the principle of analytic continuation of identities. That is, both sides of (4.10) are analytic functions of t on the right half-plane. Since they agree on the positive real axis, they must be equal everywhere for $\operatorname{Re} t > 0$.

Proposition 8. *As t approaches zero from above, we have*

$$|\theta(t) - t^{-1/2}| < e^{-C/t} \tag{4.11}$$

for some positive constant C.

PROOF. By (4.10) and (4.9), the left side is equal to $2t^{-1/2}\sum_{n=1}^{\infty} e^{-\pi n^2/t}$. Suppose t is small enough so that $\sqrt{t} > 4e^{-1/t}$ and also $e^{-3\pi/t} < \frac{1}{2}$. Then

$$\begin{aligned}|\theta(t) - t^{-1/2}| &< \tfrac{1}{2}e^{1/t}(e^{-\pi/t} + e^{-4\pi/t} + \cdots) < \tfrac{1}{2}e^{-(\pi-1)/t}(1 + \tfrac{1}{2} + \tfrac{1}{4} + \tfrac{1}{8} + \cdots)\\ &= e^{-(\pi-1)/t}.\end{aligned}$$

Thus, we can take $C = \pi - 1$. □

We now relate $\theta(t)$ to the Riemann zeta-function. Roughly speaking, $\zeta(s)$ is the Mellin transform of $\theta(t)$. The functional equation for $\theta(t)$ then leads us to the functional equation for $\zeta(s)$, and at the same time gives analytic continuation of $\zeta(s)$. We now show how this works.

Theorem. *The Riemann zeta-function $\zeta(s)$ defined by* (3.1) *for* $\operatorname{Re} s > 1$ *extends analytically onto the whole complex s-plane, except for a simple pole at $s = 1$ with residue* 1. *Let*

$$\Lambda(s) \underset{\text{def}}{=} \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s). \tag{4.12}$$

Then $\Lambda(s)$ is invariant under replacing s by $1 - s$:

$$\Lambda(s) = \Lambda(1 - s).$$

That is, $\zeta(s)$ satisfies the functional equation

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s). \tag{4.13}$$

Proof. Basically, what we want to do is consider the Mellin transform $\int_0^\infty \theta(t)t^s(\frac{dt}{t})$. However, for large t the theta-function is asymptotic to 1 (since all except the $n = 0$ term in (4.9) decrease rapidly); and for t near 0 it looks like $t^{-1/2}$, by Proposition 8. Hence, we must introduce correction terms if we want convergence at both ends. In addition, we replace s by $\frac{s}{2}$ (otherwise, we would end up with $\zeta(2s)$). So we define

$$\phi(s) \underset{\text{def}}{=} \int_1^\infty t^{s/2}(\theta(t) - 1)\frac{dt}{t} + \int_0^1 t^{s/2}\left(\theta(t) - \frac{1}{\sqrt{t}}\right)\frac{dt}{t}. \tag{4.14}$$

In the first integral, the expression $\theta(t) - 1 = 2\sum_{n=1}^\infty e^{-\pi n^2 t}$ approaches zero rapidly at infinity. So the integral converges, and can be evaluated term by term, for *any* s. Similarly, Proposition 8 implies that the second integral converges for any s. In any case, since $\theta(t)$ is bounded by a constant times $t^{-1/2}$ in the interval $(0, 1]$, if we take s with $\operatorname{Re} s > 1$ we can evaluate the second integral as

$$\int_0^1 t^{s/2}\theta(t)\frac{dt}{t} - \int_0^1 t^{(s-1)/2}\frac{dt}{t} = \int_0^1 t^{s/2}\theta(t)\frac{dt}{t} - \frac{2}{s-1}.$$

Thus, for s in the half-plane $\operatorname{Re} s > 1$, we obtain:

$$\begin{aligned}\phi(s) &= 2\sum_{n=1}^\infty \int_1^\infty e^{-\pi n^2 t}t^{s/2}\frac{dt}{t} + \left(\int_0^1 t^{s/2}\frac{dt}{t} + 2\sum_{n=1}^\infty \int_0^1 e^{-\pi n^2 t}t^{s/2}\frac{dt}{t} - \frac{2}{s-1}\right)\\ &= 2\sum_{n=1}^\infty \int_0^\infty e^{-\pi n^2 t}t^{s/2}\frac{dt}{t} + \frac{2}{s} + \frac{2}{1-s}.\end{aligned}$$

Using (4.6) with c replaced by πn^2 and s replaced by $\frac{s}{2}$, we have:

$$\begin{aligned}\frac{1}{2}\phi(s) &= \sum_{n=1}^\infty (\pi n^2)^{-s/2}\Gamma\left(\frac{s}{2}\right) + \frac{1}{s} + \frac{1}{1-s}\\ &= \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) + \frac{1}{s} + \frac{1}{1-s},\end{aligned} \tag{4.15}$$

where always here $\operatorname{Re} s > 1$.

Now $\phi(s)$ is an entire function of s, since the integrals in (4.13) converge so well for any s, as we saw. Thus, (4.14) shows us that there is a meromorphic function of s on the whole complex plane, namely

$$\frac{\pi^{s/2}}{\Gamma(s/2)}\left(\frac{1}{2}\phi(s) - \frac{1}{s} - \frac{1}{1-s}\right),$$

which is equal to $\zeta(s)$ for $\operatorname{Re} s > 1$. Moreover, since $\pi^{s/2}$, $1/\Gamma(\frac{s}{2})$, and $\phi(s)$ are all entire functions, it follows that the only possible poles are at $s = 0$ and at $s = 1$. But near $s = 0$ we can replace $s\Gamma(\frac{s}{2})$ in the denominator by $2(\frac{s}{2})\Gamma(\frac{s}{2}) = 2\Gamma(\frac{s}{2} + 1)$, which remains nonzero as $s \to 0$. H[illegible] the only pole is at $s = 1$, where we compute the residue

$$\lim_{s\to 1}(s-1)\frac{\pi^{s/2}}{\Gamma(s/2)}\left(\frac{1}{2}\phi(s) - \frac{1}{s} + \frac{1}{s-1}\right) = \frac{\pi^{1/2}}{\Gamma(1/2)} = 1.$$

It remains to prove the functional equation. Since, by (4.15), $\Lambda(s) = \frac{1}{2}\phi(s) - \frac{1}{s} - \frac{1}{(1-s)}$, and since $\frac{1}{s} + \frac{1}{(1-s)}$ is invariant under replacing s by $1-s$, it suffices to prove that $\phi(s) = \phi(1-s)$. This is where we use the functional equation (4.10) for the theta-function. Using (4.10) and replacing t by $\frac{1}{t}$ in (4.14), we obtain (note that $d(\frac{1}{t})/(\frac{1}{t}) = -\frac{dt}{t}$, and $\int_1^\infty$ becomes $\int_1^0 = -\int_0^1$ under the substitution):

$$\phi(s) = \int_0^1 t^{-s/2}\left(\theta\left(\frac{1}{t}\right) - 1\right)\frac{dt}{t} + \int_1^\infty t^{-s/2}\left(\theta\left(\frac{1}{t}\right) - \sqrt{t}\right)\frac{dt}{t}$$

$$\left(\text{replacing } t \text{ by } \frac{1}{t}\right)$$

$$= \int_0^1 t^{-s/2}(\sqrt{t}\theta(t) - 1)\frac{dt}{t} + \int_1^\infty t^{-s/2}(\sqrt{t}\theta(t) - \sqrt{t})\frac{dt}{t} \qquad \text{(by (4.10))}$$

$$= \int_0^1 t^{(1-s)/2}\left(\theta(t) - \frac{1}{\sqrt{t}}\right)\frac{dt}{t} + \int_1^\infty t^{(1-s)/2}(\theta(t) - 1)\frac{dt}{t}$$

$$= \phi(1-s).$$

This completes the proof of the theorem. □

In a similar way one can prove analytic continuation and a functional equation for the more general series obtained by inserting a Dirichlet character $\chi(n)$ before n^{-s} in (3.1), or, equivalently, inserting $\chi(p)$ before p^{-s} in the Euler product (see Problem 1 below). That is, for any character $\chi\colon (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$, one defines:

$$L(\chi, s) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}} \qquad (\text{where } \mathrm{Re}\, s > 1). \qquad (4.16)$$

The details of the proof of analytic continuation and the functional equation will be outlined in the form of problems below.

The Hasse–Weil L-function for our elliptic curve E_n, to be defined in the next section, will also turn out to be a series similar to (4.16), except that the summation will be over Gaussian integers x, the denominator will be the norm of x to the s-th power, and the numerator will be $\tilde{\chi}_n(x)$, where $\tilde{\chi}_n$ was defined in (3.3) in the last section. The techniques used in this section to treat the Riemann zeta-function can be modified to give analogous facts—analytic continuation and a functional equation—for the Hasse–Weil L-function for E_n. In the final section we shall use this information to investigate the "critical value" of the Hasse–Weil L-function, which is related to the congruent number problem.

(d) Let $s = k$ be a positive even integer. Show that for $a \in \mathbb{C}$, $\operatorname{Im} a > 0$:

$$\sum_{n=-\infty}^{\infty} \frac{1}{(a+n)^k} = \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n a}.$$

(e) Give a second derivation of the formula in part (d) by successively differentiating the formula

$$\pi \cot(\pi a) = \frac{1}{a} + \sum_{n=1}^{\infty} \frac{1}{a+n} + \frac{1}{a-n}.$$

§5. The Hasse–Weil L-function and its functional equation

Earlier in this chapter we studied the congruence zeta-function $Z(E/\mathbb{F}_p; T)$ for our elliptic curves E_n: $y^2 = x^3 - n^2 x$. That function was defined by a generating series made up from the number $N_r = N_{r,p}$ of $\mathbb{F}_{p^r}$-points on the elliptic curve reduced mod p. We now combine these functions for all p to obtain a function which incorporates the numbers $N_{r,p}$ for all possible prime powers p^r, i.e., the numbers of points on E_n over all finite fields.

Let s be a complex variable. We make the substitution $T = p^{-s}$ in $Z(E_n/\mathbb{F}_p; T)$, and define the Hasse–Weil L-function $L(E_n, s)$ as follows:

$$L(E_n, s) \underset{\text{def}}{=} \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E_n/\mathbb{F}_p; p^{-s})}$$

$$= \prod_{p \nmid 2n} \frac{1}{1 - 2a_{E_n,p} p^{-s} + p^{1-2s}} \tag{5.1}$$

$$= \prod_{P \nmid 2n} \frac{1}{1 - \alpha^{\deg P} (\mathbb{N}P)^{-s}}. \tag{5.2}$$

We must first explain the meaning of these products, why they are equivalent, and what restriction on $s \in \mathbb{C}$ will ensure convergence. In (5.1) we are using the form of the congruence zeta-function in the theorem in §II.2 (see the first equality in (2.7)), where the notation $a_{E_n,p}$ indicates that the coefficient a depends on E_n and also on the prime p. We put the term $\zeta(s)\zeta(s-1)$ in the definition so that the uninteresting part of the congruence zeta-function—its denominator—disappears, as we see immediately by replacing $\zeta(s)$ and $\zeta(s-1)$ by their Euler products (see (3.1)). Note that when $p|2n$, the denominator term is all there is (see Problem 10 of §II.1), so we only have a contribution of 1 to the product in that case; so those primes do not appear in the product in (5.1).

In (5.2) the product is over all prime ideals P of $\mathbb{Z}[i]$ which divide primes p of good reduction. Recall that those primes are of two types: $P = (p)$, $p \equiv 3 \pmod 4$, $\deg P = 2$, $\mathbb{N}P = p^2$; and $P = (a + bi)$, $a^2 + b^2 = p \equiv 1 \pmod 4$, $\deg P = 1$, $\mathbb{N}P = p$. The meaning of α_P and the equivalence of (5.1) and (5.2) are contained in Proposition 1 (see (3.2)).

As in the case of the Riemann zeta-function, we can expand the Euler product, writing each term as a geometric series and multiplying all of the geometric series corresponding to each prime. The result is a Dirichlet series, i.e., a series of the form

$$L(E_n, s) = \sum_{m=1}^{\infty} b_{m,n} m^{-s}. \tag{5.3}$$

Before discussing the "additive" form of $L(E_n, s)$ in detail, let us work out the values of the first few $b_{m,n}$ for the example of the elliptic curve $E_1 : y^2 = x^3 - x$. We first compute the first few values of $a_{E_1,p}$ in (5.1). If $p \equiv 3 \pmod 4$, then $a_{E_1,p} = 0$. If $p \equiv 1 \pmod 4$, there are two easy ways to compute $a = a_{E_1,p}$: (1) as the solution to $a^2 + b^2 = p$ for which $a + bi \equiv 1 \pmod{2 + 2i}$; (2) after counting the number N_1 of $\mathbb{F}_p$-points on E_1, we have $2a = p + 1 - N_1$ (see (1.5)). Here is the result:

$$\begin{aligned} L(E_1, s) &= \frac{1}{1 + 3\cdot 9^{-s}} \cdot \frac{1}{1 + 2\cdot 5^{-s} + 5\cdot 25^{-s}} \cdot \frac{1}{1 + 7\cdot 49^{-s}} \cdot \frac{1}{1 + 11\cdot 121^{-s}} \\ &\quad \cdot \frac{1}{1 - 6\cdot 13^{-s} + 13\cdot 169^{-s}} \cdot \frac{1}{1 - 2\cdot 17^{-s} + 17\cdot 289^{-s}} \cdots \\ &= 1 - 2\cdot 5^{-s} - 3\cdot 9^{-s} + 6\cdot 13^{-s} + 2\cdot 17^{-s} + \sum_{m \geq 25} b_{m,n} m^{-s}. \end{aligned} \tag{5.4}$$

We have not yet discussed convergence of the series or product for $L(E_n, s)$. Using (5.2) and the standard criterion for an infinite product to converge to a nonzero value, we are led to consider $\Sigma_P |\alpha_P|^{\deg P} (\mathbb{N}P)^{-s}$ for s real. By Proposition 1, we have $|\alpha_P|^{\deg P} = \mathbb{N}P^{1/2}$. In addition, $\mathbb{N}P^{1/2-s} \leq p^{1/2-s}$ for $s \geq \frac{1}{2}$ (where $P = (p)$ or else $P\bar{P} = (p)$). Since there are at most two P's for each p, it follows that the sum is bounded by $2\Sigma_p p^{1/2-s}$, which converges if $\operatorname{Re} s > \frac{3}{2}$. To summarize, the right half-plane of guaranteed convergence is 1/2 to the right of the right half-plane of convergence for the Riemann zeta-function, because we have a term of absolute value $\sqrt{p}$ in the Euler product which was absent in the case of $\zeta(s)$.

We now discuss the additive form of $L(E_n, s)$ in more detail. Using Proposition 2, we can rewrite (5.2) in terms of the map $\tilde{\chi}_n$ defined in (3.3)–(3.4):

$$L(E_n, s) = \prod_{P \nmid 2n} \left(1 - \frac{\tilde{\chi}_n(P)}{(\mathbb{N}P)^s}\right)^{-1}, \tag{5.5}$$

where we have used $\tilde{\chi}_n(P)$ to denote its value at any generator of the ideal P. Notice that, since $\tilde{\chi}_n$ is a multiplicative map taking the value 1 at all four units ± 1, $\pm i$, we may regard it equally well as a map on elements x of $\mathbb{Z}[i]$ or on ideals I.

We can now expand the product (5.5) in the same way one does for the Riemann zeta-function and for Dirichlet L-series (see Problem 1(a) in the last section). We use the two facts: (1) every ideal I has a unique factorization as a product of prime power ideals; and (2) both $\tilde{\chi}_n$ and $\mathbb{N}$ are multiplicative: $\tilde{\chi}_n(I_1 I_2) = \tilde{\chi}_n(I_1)\tilde{\chi}_n(I_2)$, $\mathbb{N}(I_1 I_2) = \mathbb{N}I_1 \cdot \mathbb{N}I_2$. Then, by multiplying out the geometric series, we obtain:

$$L(E_n, s) = \sum_I \tilde{\chi}_n(I)(\mathbb{N}I)^{-s}, \tag{5.6}$$

where the sum is over all nonzero ideals of $\mathbb{Z}[i]$.

A series of the form (5.6) is called a "Hecke L-series", and the map $\tilde{\chi}_n$ is an example of a "Hecke character". In a Hecke L-series, the sum on the right of (5.6) is taken over all nonzero ideals in some number ring. A multiplicative map χ on the ideals in that ring is said to be a Hecke character if the following condition holds. There is some fixed ideal $\mathfrak{f}$ and a fixed set of integers n_σ, one for each imbedding σ of the number field into $\mathbb{Q}^{\text{alg cl}}$, such that if I is a principal ideal generated by an element x which is congruent to 1 modulo the ideal $\mathfrak{f}$, then $\chi(I) = \Pi_\sigma \sigma(x)^{n_\sigma}$. In our example, the number ring is $\mathbb{Z}[i]$; there are two imbeddings $\sigma_1 =$ identity, $\sigma_2 =$ complex conjugation in $\text{Gal}(\mathbb{Q}[i]/\mathbb{Q})$; we take $n_{\sigma_1} = 1$, $n_{\sigma_2} = 0$; and we take $\mathfrak{f} = (n')$ ($n' = (2 + 2i)n$ if n is odd, $2n$ if n is even). Then the condition simply states that $\tilde{\chi}_n((x)) = x$ if $x \equiv 1 \pmod{n'}$.

It is very useful when the Hasse–Weil L-series of an elliptic curve turns out to be a Hecke L-series. In that case one can work with it much as with Dirichlet L-series, for example, proving analytic continuation and a functional equation. It can be shown that the Hasse–Weil L-series of an elliptic curve with complex multiplication (see Problem 8 of §I.8) is always a Hecke L-series.

The relation between the additive form (5.6) and the additive form (5.3) is quite simple. We obtain (5.3) by collecting all terms corresponding to ideals I with the same norm, i.e.,

$$b_{m,n} = \sum_{I \text{ with } \mathbb{N}I = m} \tilde{\chi}_n(I).$$

Notice that, since $\tilde{\chi}_n(I) = \tilde{\chi}_1(I) \cdot (\frac{n}{\mathbb{N}I})$ by (3.3), we have

$$b_{m,n} = \left(\frac{n}{m}\right) \sum_{I \text{ with } \mathbb{N}I = m} \tilde{\chi}_1(I) = \left(\frac{n}{m}\right) b_m,$$

where we have denoted $b_m = b_{m,1}$. Thus, if for fixed n we let χ_n denote the multiplicative map on $\mathbb{Z}$ given by $m \mapsto (\frac{n}{m})$ (for m prime to $2n$), we have

$$L(E_n, s) = \sum_{m=1}^{\infty} \chi_n(m) b_m m^{-s}$$
$$= 1 - 2\left(\frac{n}{5}\right)5^{-s} - 3\left(\frac{n}{3}\right)^2 9^{-s} + 6\left(\frac{n}{13}\right)13^{-s} + 2\left(\frac{n}{17}\right)17^{-s} + \cdots \tag{5.7}$$

(note: $(\frac{n}{3})^2$ is 1 if $3 \nmid n$ and 0 if $3 | n$); one says that $L(E_n, s)$ is a "twisting" of $L(E_1, s) = \Sigma\, b_m m^{-s}$ by the character χ_n. One can verify that for n square-free, the conductor of χ_n is n when $n \equiv 1 \pmod 4$ and is $4n$ when $n \equiv 2$ or 3

mod 4 (this follows from quadratic reciprocity). In other words, χ_n is a primitive Dirichlet character modulo n or $4n$.

To keep the notation clear in our minds, let us review the meaning of χ_n, χ'_n, and $\tilde{\chi}_n$. First, χ_n is a map from $\mathbb{Z}$ to $\{\pm 1, 0\}$ which is defined by the Legendre symbol on integers prime to $2n$. Second, χ'_n is a map from $\mathbb{Z}[i]$ to $\{\pm 1, \pm i, 0\}$ which takes elements x prime to $2n$ to the unique power of i such that $\chi'_n(x)x \equiv \chi_n(\mathbb{N}x)$ modulo $2+2i$ (see (3.3)–(3.4)). Thirdly, $\tilde{\chi}_n$ is a map from $\mathbb{Z}[i]$ to $\mathbb{Z}[i]$ which takes an element x to $x\chi'_n(x)$; also, $\tilde{\chi}_n$ can be regarded as a map from ideals of $\mathbb{Z}[i]$ to elements of $\mathbb{Z}[i]$ which takes an ideal I prime to $2n$ to the unique generator of I which is congruent to $\chi_n(\mathbb{N}I)$ modulo $2+2i$.

The character χ_n is intimately connected with the quadratic field $\mathbb{Q}(\sqrt{n})$. Namely, if $m = p \neq 2$ is a prime number, then the value of $\chi_n(p) = (\frac{n}{p})$ shows whether p splits into a product of two prime ideals $(p) = P_1P_2$ in $\mathbb{Q}(\sqrt{n})$ (this happens if $(\frac{n}{p}) = 1$), remains prime (if $(\frac{n}{p}) = -1$), or ramifies $(p) = P^2$ (if $(\frac{n}{p}) = 0$, i.e., $p|n$). (See [Borevich and Shafarevich 1966].) We say that χ_n is the quadratic character associated to the field $\mathbb{Q}(\sqrt{n})$.

It is not surprising that the character corresponding to the field $\mathbb{Q}(\sqrt{n})$ appears in the formula (5.7) which links $L(E_n, s)$ with $L(E_1, s)$. In fact, if we allow ourselves to make a linear change of variables *with coefficients in* $\mathbb{Q}(\sqrt{n})$, then we can transform $E_n\colon y^2 = x^3 - n^2x$ to $E_1\colon y'^2 = x'^3 - x'$ by setting $y = n\sqrt{n}y'$, $x = nx'$. One says that E_n and E_1 are isomorphic "over the field $\mathbb{Q}(\sqrt{n})$."

Returning now to the expression (5.6) for $L(E_n, s)$, we see that it can also be written as a sum over elements of $\mathbb{Z}[i]$ rather than ideals. We simply note that every nonzero ideal has four generators, and so appears four times if we list elements instead of ideals. Thus,

$$b_{m,n} = \frac{1}{4} \sum_{a+bi \text{ with } a^2+b^2=m} \tilde{\chi}_n(a+bi),$$

and

$$\begin{aligned} L(E_n, s) &= \frac{1}{4} \sum_{x \in \mathbb{Z}[i]} \tilde{\chi}_n(x)(\mathbb{N}x)^{-s} \\ &= \frac{1}{4} \sum_{a+bi \in \mathbb{Z}[i]} \frac{(a+bi)\chi'_n(a+bi)}{(a^2+b^2)^s}, \end{aligned} \tag{5.8}$$

where χ'_n was defined in (3.3)–(3.4). (The sums are over nonzero x, $a+bi$.)

Notice the analogy between the sum (5.8) and Dirichlet L-series. The only differences are that the number ring is $\mathbb{Z}[i]$ rather than $\mathbb{Z}$, and our Hecke character $\tilde{\chi}_n(x)$ includes an ordinary character $\chi'_n(x)$ (with values in the roots of unity) multiplied by x.

We now proceed to show that $L(E_n, s)$ can be analytically continued to the left of $\operatorname{Re} s = \frac{3}{2}$, in fact, to an entire function on the whole complex plane; and that it satisfies a functional equation relating $L(E_n, s)$ to $L(E_n, 2-s)$.

Since $L(E_n, s)$ is a "two-dimensional" sum over $\mathbb{Z}[i] \approx \mathbb{Z}^2$, i.e., over pairs of integers rather than integers, it follows that we shall need to look at Fourier transforms, the Poisson summation formula, and theta-functions in two variables. We shall give the necessary ingredients as a sequence of propositions whose proofs are no harder than the analogous results we proved in the last section for the case of one variable.

Since the definitions and properties we need in two dimensions are just as easy to state and prove in n dimensions, we shall consider functions on $\mathbb{R}^n$. For now, n will denote the number of variables (not to be confused with our use of n when writing E_n: $y^2 = x^3 - n^2x$, χ_n, etc.). We will use $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ to denote vectors in $\mathbb{R}^n$. As usual, we let $x \cdot y = x_1y_1 + \cdots + x_ny_n$, $|x| = \sqrt{x \cdot x}$. We shall also use the dot-product notation when the vectors are in $\mathbb{C}^n$; for example, if $n = 2$ we have $x \cdot (1, i) = x_1 + x_2 i$.

Let $\mathcal{S}$ be the vector space of functions f: $\mathbb{R}^n \to \mathbb{C}$ which are bounded, smooth (i.e., all partial derivatives exist and are continuous), and rapidly decreasing (i.e., $|x|^N f(x)$ approaches zero whenever $|x|$ approaches infinity for any N). For $f \in \mathcal{S}$ we define the Fourier transform $\hat{f}$: $\mathbb{R}^n \to \mathbb{C}$ as follows (where dx denotes $dx_1 dx_2 \cdots dx_n$):

$$\hat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi i x \cdot y} f(x) dx. \tag{5.9}$$

This integral converges for all $y \in \mathbb{R}^n$, and $\hat{f} \in \mathcal{S}$.

Proposition 9. *Let f: $\mathbb{R}^n \to \mathbb{C}$, g: $\mathbb{R}^n \to \mathbb{C}$ be functions in $\mathcal{S}$.*

(1) *If $a \in \mathbb{R}^n$ and $g(x) = f(x + a)$, then $\hat{g}(y) = e^{2\pi i a \cdot y} \hat{f}(y)$.*
(2) *If $a \in \mathbb{R}^n$ and $g(x) = e^{2\pi i a \cdot x} f(x)$, then $\hat{g}(y) = \hat{f}(y - a)$.*
(3) *If $b \in \mathbb{R}$, $b > 0$, and $g(x) = f(bx)$, then $\hat{g}(y) = b^{-n} \hat{f}(y/b)$.*
(4) *If $f(x) = e^{-\pi x \cdot x}$, then $\hat{f} = f$.*

Proposition 10 (Poisson Summation Formula). *If $g \in \mathcal{S}$, then*

$$\sum_{m \in \mathbb{Z}^n} g(m) = \sum_{m \in \mathbb{Z}^n} \hat{g}(m).$$

The proofs of Propositions 9 and 10 are completely similar to those of properties (1)–(3) of the Fourier transform in one variable and Propositions 5 and 6 of the last section. One simply has to proceed one variable at a time.

If $w \in \mathbb{C}^n$ and $f \in \mathcal{S}$, we let $w \cdot \frac{\partial}{\partial x} f \underset{\text{def}}{=} w_1 \frac{\partial f}{\partial x_1} + w_2 \frac{\partial f}{\partial x_2} + \cdots + w_n \frac{\partial f}{\partial x_n}$.

Proposition 11. *If $f \in \mathcal{S}$ and $g = w \cdot \frac{\partial}{\partial x} f$, then $\hat{g}(y) = 2\pi i w \cdot y \hat{f}(y)$.*

Proof. Since both sides of the equality are linear in w, it suffices to prove the proposition when w is the j-th standard basis vector, i.e., to prove that the Fourier transform of $\frac{\partial}{\partial x_j} f(x)$ is $2\pi i y_j \hat{f}(y)$. This is easily done by substituting $\frac{\partial}{\partial x_j}f(x)$ in place of $f(x)$ in (5.9) and integrating by parts with respect to the j-th variable (see Problem 5(a) in the last section). □

For the rest of this section, we take $n = 2$ in Propositions 9–11, and we return to our earlier use of the letter n in E_n, χ_n, etc.

Theorem. *The Hasse–Weil L-function $L(E_n, s)$ for the elliptic curve E_n: $y^2 = x^3 - n^2x$, which for* Re $s > \frac{3}{2}$ *is defined by* (5.1), *extends analytically to an entire function on the whole complex s-plane. In addition, let*

$$N = 4|n'|^2 = \begin{cases} 32n^2, & n \text{ odd;} \\ 16n^2, & n \text{ even.} \end{cases} \tag{5.10}$$

Let

$$\Lambda(s) \underset{\text{def}}{=} \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L(E_n, s). \tag{5.11}$$

Then $L(E_n, s)$ satisfies the functional equation

$$\Lambda(s) = \pm\Lambda(2 - s), \tag{5.12}$$

where the "root number" ± 1 is equal to 1 *if $n \equiv 1, 2, 3$* (mod 8) *and is equal to -1 if $n \equiv 5, 6, 7$* (mod 8).

Proof. The proof is closely parallel to the proof of analytic continuation and the functional equation for Dirichlet L-series with odd character, which was outlined in Problem 5 of the last section. Namely, we express $L(E_n, s)$, written in the form (5.8), in terms of the Mellin transform of a two-dimensional version of the theta-function $\theta_a(t)$ defined in Problem 5(c). We shall use the letter u rather than a to avoid confusion with the use of a in (5.8).

Thus, let $u = (u_1, u_2) \in \mathbb{R}^2$, where $u \notin \mathbb{Z}^2$, and let $t \in \mathbb{R}$ be positive. Let w be the fixed vector $(1, i) \in \mathbb{C}^2$, so that, for example, $m \cdot w = m_1 + m_2 i$ for $m \in \mathbb{Z}^2$. We define:

$$\theta_u(t) = \sum_{m \in \mathbb{Z}^2} (m + u) \cdot w e^{-\pi t |m+u|^2}; \tag{5.13}$$

$$\theta^u(t) = \sum_{m \in \mathbb{Z}^2} m \cdot w e^{2\pi i m \cdot u} e^{-\pi t |m|^2}. \tag{5.14}$$

Regarding u and t as fixed, we find a functional equation for $\theta_u(t)$ by means of the Poisson summation formula (Proposition 10); to obtain $\theta_u(t)$ on the left side of Proposition 10, we choose

$$g(x) = (x + u) \cdot w e^{-\pi t |x+u|^2}. \tag{5.15}$$

To find the Fourier transform of $g(x)$, and hence the right side of the Poisson summation formula, we proceed in several steps, writing $f(x) = e^{-\pi |x|^2}$, $g_1(x) = f(\sqrt{t}x)$, $g_2(x) = w \cdot \frac{\partial}{\partial x} g_1(x)$, and finally $g(x) = \frac{-1}{2\pi t} g_2(x + u)$. We have:

$\hat{f}(y) = e^{-\pi|y|^2}$ by Proposition 9, part (4);

$\hat{g}_1(y) = t^{-1}e^{-(\pi/t)|y|^2}$ by Proposition 9, part (3);

$\hat{g}_2(y) = 2\pi i t^{-1} w \cdot y\, e^{-(\pi/t)|y|^2}$ by Proposition 11;

$\hat{g}(y) = -it^{-2} w \cdot y\, e^{2\pi i u,y} e^{-(\pi/t)|y|^2}$ by Proposition 9, part (1).

If we now evaluate $\hat{g}(m)$ for $m \in \mathbb{Z}^2$, and sum over all m, we obtain the functional equation

$$\theta_u(t) = \frac{-i}{t^2}\theta^u\left(\frac{1}{t}\right). \tag{5.16}$$

We now consider the Mellin transform of $\theta_u(t)$: $\int_0^\infty t^s \theta_u(t)\frac{dt}{t}$, and show that the integral converges to an entire function of s. First, for large t it is easy to bound the integrand by something of the form e^{-ct}, using the fact that $|m+u|^2$ is bounded away from zero, since u is not in $\mathbb{Z}^2$. Next, for t near zero one uses the functional equation (5.16) and a bound for $\theta^u(\frac{1}{t})$ of the form $e^{-c/t}$, where we use the fact that the only term in (5.14) with $|m|^2 = 0$ vanishes because of the factor $m \cdot w$. These bounds make it a routine matter to show that the integral converges for all s, and that the Mellin transform is analytic in s.

If we now take $\mathrm{Re}\, s > \frac{3}{2}$, we can evaluate the Mellin transform integral term by term, obtaining a sum that begins to look like our L-function:

$$\int_0^\infty t^s \theta_u(t)\frac{dt}{t} = \sum_{m \in \mathbb{Z}^2} (m+u)\cdot w \int_0^\infty t^s e^{-\pi t|m+u|^2}\frac{dt}{t}$$

$$= \pi^{-s}\Gamma(s) \sum_{m \in \mathbb{Z}^2} \frac{(m+u)\cdot w}{|m+u|^{2s}} \qquad \text{(see (4.6))}.$$

Now for $\mathrm{Re}\, s > \frac{3}{2}$, we can rewrite $L(E_n, s)$ as a linear combination of these sums with various u.

We now suppose that n is odd. The case $n = 2n_0$ even is completely similar, and will be left as an exercise below. We take $w = (1, i)$. If we use (5.8) and recall that $\chi_n'(x)$ depends only on x modulo $n' = (2+2i)n$, and hence, *a fortiori*, only on x modulo $4n$, we obtain:

$$L(E_n, s) = \frac{1}{4}\sum_{0 \le a,b < 4n} \chi_n'(a+bi) \sum_{m \in \mathbb{Z}^2} \frac{a+bi+4nm\cdot w}{|(a,b)+4nm|^{2s}},$$

$$= \frac{1}{4}(4n)^{1-2s} \sum_{0 \le a,b < 4n} \chi_n'(a+bi) \sum_{m \in \mathbb{Z}^2} \frac{(m+(\frac{a}{4n}, \frac{b}{4n}))\cdot w}{|m+(\frac{a}{4n},\frac{b}{4n})|^{2s}}.$$

Thus

$$\pi^{-s}\Gamma(s)L(E_n, s) = \frac{1}{4}(4n)^{1-2s} \sum_{\substack{0 \le a,b < 4n \\ (a,b) \ne (0,0)}} \chi_n'(a+bi) \int_0^\infty t^s \theta_{a/4n,\, b/4n}(t)\frac{dt}{t}. \tag{5.17}$$

Since the integral inside the finite sum is an entire function of s, as are the functions $(4n)^{1-2s}$ and $\pi^s/\Gamma(s)$, we conclude that $L(E_n, s)$ has an analytic continuation to an entire function of s.

Moreover, we can transform this integral using the functional equation (5.16) and replacing t by $\frac{1}{t}$:

$$\int_0^\infty t^s\theta_{a/4n,b/4n}(t)\frac{dt}{t} = -i\int_0^\infty t^{s-2}\theta^{a/4n,b/4n}\left(\frac{1}{t}\right)\frac{dt}{t} = -i\int_0^\infty t^{2-s}\theta^{a/4n,b/4n}(t)\frac{dt}{t}.$$

In the entire function (5.17) we now suppose that $\operatorname{Re} 2 - s > \frac{3}{2}$ (i.e., $\operatorname{Re} s < \frac{1}{2}$) so that we can evaluate this last integral as an infinite sum. Using (4.6) again, inserting the definition (5.14), and interchanging summation and integration, we obtain

$$\int_0^\infty t^{2-s}\theta^{a/4n,b/4n}(t)\frac{dt}{t} = \pi^{s-2}\Gamma(2-s)\sum_{m\in\mathbb{Z}^2} m\cdot w\, e^{(2\pi i/4n)m\cdot(a,b)}|m|^{-2(2-s)}.$$

Thus, for $\operatorname{Re} 2 - s > \frac{3}{2}$, the right side of (5.17) is equal to

$$-i(4n)^{1-2s}\pi^{s-2}\Gamma(2-s)\frac{1}{4}\sum_{m\in\mathbb{Z}^2}\frac{m\cdot w}{|m|^{2(2-s)}}S_m \tag{5.18}$$

where for $m\in\mathbb{Z}^2$

$$S_m \underset{\text{def}}{=} \sum_{0\le a,b<4n}\chi_n'(a+bi)e^{(2\pi i/4n)m\cdot(a,b)}. \tag{5.19}$$

Lemma. *If $m_1 + m_2 i$ is not in the ideal $(1+i)$, then $S_m = 0$; whereas if $m_1 + m_2 i = (1+i)x$ with $x\in\mathbb{Z}[i]$, then $S_m = 2\chi_n'(x)g(\chi_n')$, where $g(\chi_n')$ is the Gauss sum defined in Proposition* 4 *of* §II.3 (*see* (3.9)).

Before proving the lemma, we show how the functional equation in the theorem follows immediately from it. Namely, if we make the substitution $m\cdot w = m_1 + m_2 i = (1+i)x$ in the sum in (5.18), the lemma gives us

$$\sum_{m\in\mathbb{Z}^2}\frac{m\cdot w}{|m|^{2(2-s)}}S_m = \sum_{x\in\mathbb{Z}[i]}\frac{2(1+i)x}{|(1+i)x|^{2(2-s)}}\chi_n'(x)g(\chi_n')$$
$$= (1+i)2^{s-1}\left(\frac{-2}{n}\right)(2+2i)n\sum_{x\in\mathbb{Z}[i]}\tilde{\chi}_n(x)(\mathbb{N}x)^{-(2-s)}$$

by Proposition 4. But this last sum is $4L(E_n, 2-s)$, by (5.8). Bringing this all together, we conclude that for $\operatorname{Re} 2 - s > \frac{3}{2}$ the right side of (5.17) is equal to

$$\begin{aligned}&-i(4n)^{1-2s}\pi^{s-2}\Gamma(2-s)(1+i)2^{s-1}\left(\frac{-2}{n}\right)(2+2i)nL(E_n, 2-s)\\ &= \left(\frac{-2}{n}\right)\pi^{s-2}\Gamma(2-s)(8n^2)^{1-s}L(E_n, 2-s).\end{aligned} \tag{5.20}$$

On the other hand, if we bring the term $(\sqrt{N}/2)^s$ over to the right in the functional equation (5.11)–(5.12) in the theorem, we find that what we want to prove is:

$$\pi^{-s}\Gamma(s)L(E_n, s) = \left(\frac{-2}{n}\right)(\sqrt{N}/2)^{-s}(2\pi)^{s-2}(\sqrt{N})^{2-s}\Gamma(2-s)L(E_n, 2-s)$$
$$= \left(\frac{-2}{n}\right)(N/4)^{1-s}\pi^{s-2}\Gamma(2-s)L(E_n, 2-s).$$

And this is precisely (5.20).

Thus, to finish the proof of the theorem for odd n, it remains to prove the lemma.

PROOF OF LEMMA. First suppose that $m_1 + m_2 i$ is not divisible by $1 + i$. This is equivalent to saying that m_1 and m_2 have opposite parity, i.e., their sum is odd. Now as a, b range from 0 to $4n$, the Gaussian integer $a + bi$ runs through each residue class modulo $(2 + 2i)n$ exactly twice. Each time gives the same value of $\chi_n'(a + bi)$, since $\chi_n'(a + bi)$ depends only on what $a + bi$ is modulo $n' = (2 + 2i)n$. But meanwhile, the exponential terms in the two summands have opposite sign, causing the two summands to cancel. To see this, we observe that if $a_1 + b_1 i$ and $a_2 + b_2 i$ are the two Gaussian integers in different residue classes modulo $4n$ but the same residue class modulo $(2 + 2i)n$, then $a_1 + b_1 i - (a_2 + b_2 i) \equiv (2 + 2i)n \pmod{4n}$, and so

$$e^{(2\pi i/4n)m\cdot((a_1,b_1)-(a_2,b_2))} = e^{(2\pi i/4n)m\cdot(2n,2n)} = e^{\pi i(m_1+m_2)} = -1.$$

This proves the first part of the lemma.

Now suppose that $m_1 + m_2 i = (1 + i)x$. Note that $m \cdot (a, b) = m_1 a + m_2 b = \mathrm{Re}((m_1 - m_2 i)(a + bi)) = \mathrm{Re}((1 - i)\bar{x}(a + bi))$. Hence, the exponential term in the summand in S_m is $\psi(\bar{x}(a + bi))$, where

$$\psi(x) \underset{\text{def}}{=} e^{2\pi i\,\mathrm{Re}(x/n')}$$

(with $n' = (2 + 2i)n$). Since χ_n' is a primitive character modulo $(2 + 2i)n$ (see Proposition 3), we can apply Problem 9(a)–(b) of §II.2. Since the summation in (5.19) goes through each residue class modulo $(2 + 2i)n$ twice, we have

$$S_m = 2 \sum_{a+bi\in\mathbb{Z}[i]/(2+2i)n} \chi_n'(a + bi)\psi(\bar{x}(a + bi))$$
$$= 2\bar{\chi}_n'(\bar{x})g(\chi_n') = 2\chi_n'(x)g(\chi_n').$$

This proves the lemma, and hence the theorem (except for some slight modifications in the case of even n, which will be left as an exercise). □

In the problems we shall outline a proof of the analogous theorem in the case of an elliptic curve, namely $y^2 = x^3 + 16$, which has complex multiplication by another quadratic imaginary integer ring, namely $\mathbb{Z}[\omega]$, where $\omega = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}$. There is one additional feature which is needed because we end up summing not over $\mathbb{Z}[i]$, which can be thought of as $\mathbb{Z}^2$, but rather over a lattice which is the image of $\mathbb{Z}^2$ under a certain 2×2-matrix.

So we have to apply Poisson summation to a function much like the function in this section, but involving this matrix.

We conclude this section by mentioning two references for a more general treatment of the theory of which we have only treated a few special cases. First, in C. L. Siegel's Tata notes [Siegel 1961] (see especially pp. 60–72) one finds L-functions whose summand has the form

$$e^{2\pi i m\cdot u}\frac{P(m+v)}{(Q[m+v])^{s+g/2}},$$

where $m\in\mathbb{Z}^n$, u, $v\in\mathbb{R}^n$, Q is the matrix of a positive definite quadratic form, and P is a "spherical polynomial with respect to Q of degree g". The case we needed for $L(E_n, s)$ was: $n=2$, $Q=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $P(x_1, x_2)=x_1+ix_2$, $g=1$. In Problem 8 below we have the case $Q=\left(\begin{smallmatrix}1&1/2\\1/2&1\end{smallmatrix}\right)$, $P(x_1, x_2)=(\omega+1/2)x_1+(\omega/2+1)x_2$ (where $\omega=-1/2+i\sqrt{3}/2$), $g=1$.

In [Lang 1970, Chapters XIII and XIV], two approaches are given to this topic. In Ch. XIII, the approach we have used (originally due to Hecke) is applied to obtain the functional equation for the Dedekind zeta-function of an arbitrary number field. This is a generalization of Problems 2 and 6 below. However, the case of more general Hecke L-series is not included in that chapter. A quite different approach due to J. Tate—using Fourier analysis on p-adic fields—is given in Ch. XIV of Lang's book.

Problems

1. Finish the proof of the theorem for n even.

2. (a) Find a functional equation for $\theta(t) \underset{\text{def}}{=} \sum_{m\in\mathbb{Z}^2} e^{-\pi t|m|^2}$, $t>0$.
   (b) The Dedekind zeta-function of a number field K is defined as follows:

$$\zeta_K(s) \underset{\text{def}}{=} \sum (\mathbb{N}I)^{-s},$$

   where the sum is over all nonzero ideals I of the ring of integers of K. This sum converges for $\operatorname{Re} s>1$ (see [Borevich and Shafarevich 1966, Ch. 5, §1]). Let $K=\mathbb{Q}(i)$. Prove that $\zeta_K(s)$ is an entire function except for a simple pole at $s=1$ with residue $\pi/4$, and find a functional equation relating $\zeta_K(s)$ to $\zeta_K(1-s)$.

3. For u and v in $\mathbb{R}^2$, let

$$\theta_u^v(t) \underset{\text{def}}{=} \sum_{m\in\mathbb{Z}^2} e^{2\pi i m\cdot v}e^{-\pi t|m+u|^2}, \qquad t>0.$$

   Find a functional equation relating $\theta_u^v(t)$ to $\theta_{-v}^u(\frac{1}{t})$.

4. (a) In the situation of Proposition 11, express the Fourier transform of $(w\cdot\frac{\partial}{\partial x})^k f(x)$ in terms of $\hat{f}(y)$ for any nonnegative integer k.
   (b) Suppose that k is a nonnegative integer, $u\in\mathbb{R}^2$ is fixed with $u\notin\mathbb{Z}^2$, $t>0$ is fixed, and $w=(1, i)\in\mathbb{C}^2$. What is the Fourier transform of

$$g(x)=((x+u)\cdot w)^k e^{-\pi t|x+u|^2}?$$

   (c) With k, u, t, w as in part (b), define: