Cusp Forms Associated with Elliptic Curves

8.1. The Hasse-Weil L-function

An elliptic curve E is an algebraic curve (a projective algebraic variety of dimension 1) of genus 1 over a field K. If $\mathrm{char}(K) \neq 2, 3$, then E is given by the Weierstrass equation

$$y^2 = x^3 + Ax + B \tag{8.1}$$

with $A, B \in K$. The discriminant of E is the discriminant of the cubic polynomial

$$g(x) = x^3 + Ax + B, \tag{8.2}$$

and it is equal to

$$\Delta = -16(4A^3 + 27B^2). \tag{8.3}$$

It turns out that (see Figure 9)

$$\begin{aligned} &E \text{ is non-singular } \Leftrightarrow \Delta \neq 0, \\ &E \text{ has node } \Leftrightarrow \Delta = 0, A \neq 0, \\ &E \text{ has cusp } \Leftrightarrow \Delta = 0, A = 0. \end{aligned}$$

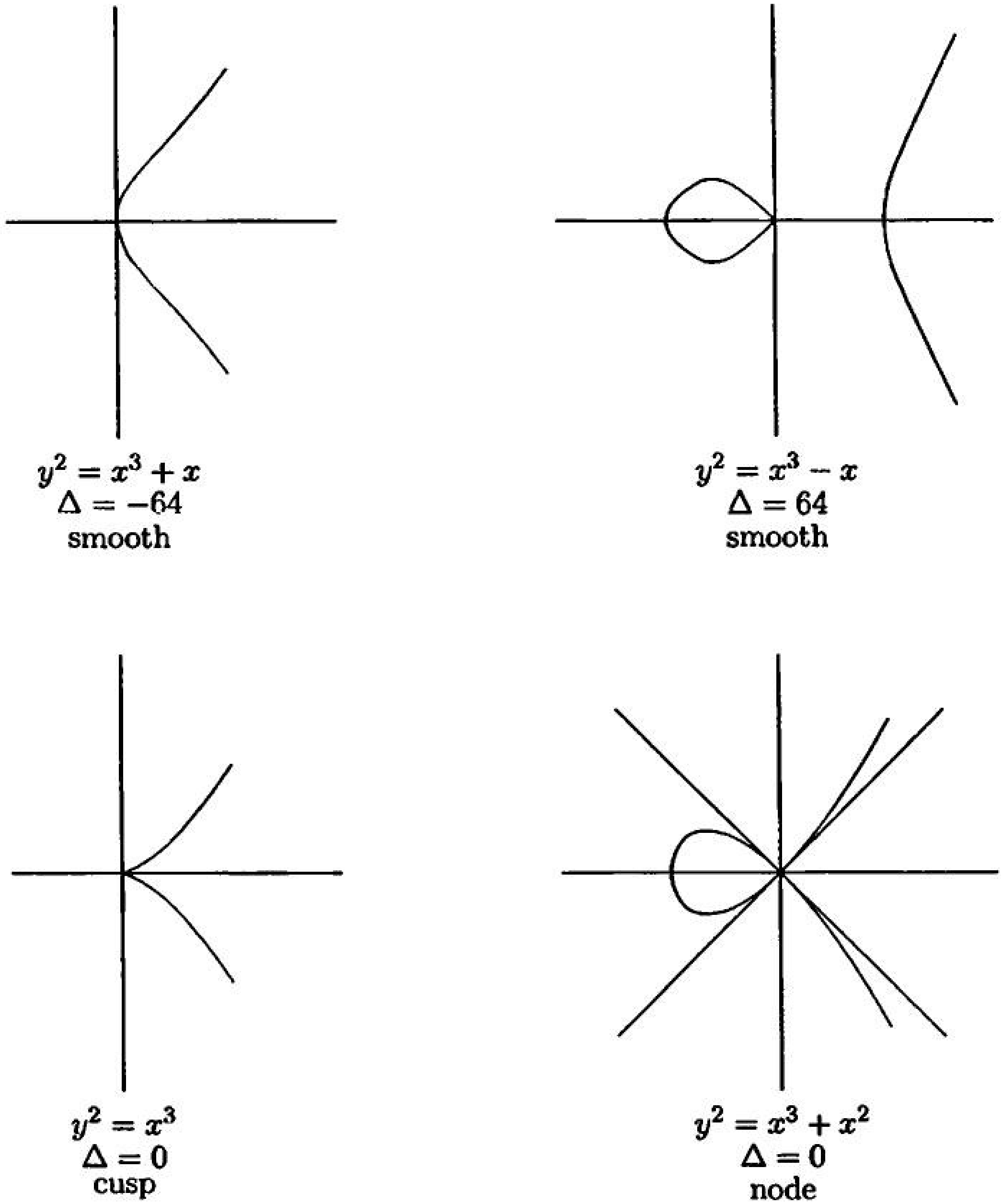

Figure 9. **Elliptic curves**

If $\text{char}(K) = 2$ or 3, the Weierstrass equation and the description of singularities are slightly different.

Suppose E is given by the Weierstrass equation (8.1) with $A, B \in \mathbb{Z}$ and $\Delta \neq 0$. For each prime p consider the reduced curve $E/\mathbb{F}_p$ over the field $\mathbb{F}_p$ of p elements. Let $\nu(p)$ denote the number of points on $E/\mathbb{F}_p$, i.e. the number of solutions to the congruence

$$y^2 \equiv g(x) \pmod{p}.$$

We do not count the point at infinity. It turns out that $\nu(p)$ is well approximated by p; more precisely, the difference

$$\lambda(p) = p - \nu(p) \tag{8.4}$$

satisfies

$$|\lambda(p)| < 2\sqrt{p}. \tag{8.5}$$

This estimate is due to H. Hasse and is essentially best possible. In order to understand how the $\lambda(p)$ vary with p, Hasse began and Weil continued to investigate the L-function for E defined by the following Euler product:

$$L_E(s) = \prod_{p|\Delta}(1 - \lambda(p)p^{-s})^{-1} \prod_{p\nmid\Delta}(1 - \lambda(p)p^{-s} + p^{1-2s})^{-1}. \tag{8.6}$$

Remarks. Although we assumed that $E/\mathbb{Q}$ is smooth (since $\Delta \neq 0$), the reduced curve $E/\mathbb{F}_p$ is singular if $p|\Delta$, and E is said to have bad reduction at such primes. One can show that for primes of bad reduction

$$\lambda(p) = 0, 1, -1$$

according to a type of singularity which occurs, namely a cusp, a node with rational slopes for the tangents, or a node with quadratic irrational slopes for the tangents. If $p \nmid \Delta$ then the reduced curve $E/\mathbb{F}_p$ remains smooth, so E is said to have good reduction at p. In this case the local factor

$$1 - \lambda(p)p^{-s} + p^{1-2s}$$

appears naturally in the so-called congruence zeta-function of E defined by

$$\zeta_{E/\mathbb{F}_p}(s) = \exp\left(\sum_{m=1}^{\infty} m^{-1}\nu(p^m)p^{-ms}\right)$$

where $\nu(q)$ denotes the number of points on E over the finite field $\mathbb{F}_q$ (it is not the same as the number of points modulo q). We have

$$\zeta_{E/\mathbb{F}_p}(s) = (1 - p^{1-s})^{-1}(1 - \lambda(p)p^{-s} + p^{1-2s}).$$

The estimate of Hasse (8.5) can be interpreted as the Riemann hypothesis for $\zeta_{E/\mathbb{F}_p}(s)$, which asserts that the roots are on the line Re $s = 1/2$.

Write $L_E(s)$ as the Dirichlet series

$$L_E(s) = \sum_{1}^{\infty} \lambda(n)n^{-s}. \tag{8.7}$$

Note that the Euler product (8.6) and the Dirichlet series (8.7) converge absolutely for Re $s > 3/2$.

Conjecture (Hasse). *$L_E(s)$ has analytic continuation to an entire function, and it satisfies the functional equation*

$$\left(\frac{\sqrt{q}}{2\pi}\right)^s \Gamma(s)L_E(s) = \eta\left(\frac{\sqrt{q}}{2\pi}\right)^{2-s} \Gamma(2-s)L_E(2-s) \tag{8.8}$$

where q is a positive integer composed of prime factors of Δ, the so-called conductor of E, and $\eta = \pm 1$ is called the root number.

Conjecture (Shimura-Taniyama). *The Fourier series*

$$f(z) = \sum_1^\infty \lambda(n)e(nz) \tag{8.9}$$

is a cusp form of weight 2 for $\Gamma_0(q)$ and the principal character; it is a newform with

$$T_n f = \lambda(n)f \tag{8.10}$$

$$Wf = \eta f. \tag{8.11}$$

Recently these conjectures were proved by A. Wiles (at least if q is squarefree). We shall give a simple proof for special curves, the so-called congruent number curves.

8.2. Elliptic curves E_r

In this chapter we shall examine a family of elliptic curves E_r given by the equation

$$y^2 = x^3 - r^2x \tag{8.12}$$

where r is a positive, squarefree integer. These curves were studied by J. Tunnell in connection with the ancient problem of the so-called "congruent numbers." A positive rational number r is called a congruent number if it is the area of some right triangle with rational sides. Equivalently, there exists x such that all three number $x-r, x, x+r$ are squares of rationals. This also means there are infinitely many rational points on E_r. Multiplying by suitable squares, we may require r to be a positive, squarefree integer. Tunnell used the curve E_r to establish an effective method of checking if r is a congruent number. The smallest congruent numbers are $r = 5, 6, 7$.

Note that the discriminant of E_r is $\Delta_r = 64r^6$, and if $p|\Delta_r$ then $\nu_r(p) = p$, so $\lambda_r(p) = 0$. In this case the Hasse-Weil L-function reduces to

$$L_{E_r}(s) = \prod_{p\nmid 2r}(1 - \lambda_r(p)p^{-s} + p^{1-2s})^{-1} = \sum_{(n,2r)=1} \lambda_r(n)n^{-s}. \tag{8.13}$$

In general if a curve E is given by

$$y^2 = g(x) \quad \text{with } g \in \mathbb{Z}[x],$$

then the number of points of $E/\mathbb{F}_p$ is equal to

$$\nu(p) = \sum_{x \pmod p} \left(1 + \left(\frac{g(x)}{p}\right)\right)$$

where $\left(\frac{x}{p}\right)$ is the quadratic residue symbol (the Legendre symbol). Hence

$$\lambda(p) = -\sum_{x \pmod p} \left(\frac{g(x)}{p}\right). \tag{8.14}$$

In particular, if $p \nmid 2r$, then

$$\lambda_r(p) = -\sum_{x \pmod p} \left(\frac{x^3 - r^2 x}{p}\right) = -\left(\frac{r}{p}\right) \sum_{x \pmod p} \left(\frac{x^3 - x}{p}\right) = \left(\frac{r}{p}\right) \lambda_1(p)$$

by changing $x \to rx$. Hence for all n

$$\lambda_r(n) = \chi_r(n)\lambda_1(n) \tag{8.15}$$

where $\chi_r(n)$ is the Jacobi symbol,

$$\chi_r(n) = \left(\frac{r}{n}\right). \tag{8.16}$$

This shows that the L-function for E_r is obtained from that for E_1 by twisting with the character χ_r,

$$\begin{aligned} L_{E_r}(s) &= \prod_{p \neq 2} (1 - \chi_r(p)\lambda_1(p)p^{-s} + \chi_r^2(p)p^{1-2s})^{-1} \\ &= \sum_{2 \nmid n} \chi_r(n)\lambda_1(n)n^{-s}. \end{aligned} \tag{8.17}$$

By virtue of the above connection it will be sufficient to prove the Hasse and the Shimura-Taniyama conjectures for E_1. In this case we simplify notation by omitting the subscript $r = 1$, so we write $E = E_1, \lambda = \lambda_1$ and

$$L_E(s) = \prod_{p \neq 2} (1 - \lambda(p)p^{-s} + p^{1-2s})^{-1} = \sum_{2 \nmid n} \lambda(n)n^{-s}. \tag{8.18}$$

After establishing the conjectures for the curve E, one can extend the results for E_r by an appeal to a general principle about twisting automorphic forms with characters (see Section 7.3, Theorem 7.4 and the formulas (7.32), (7.33)).

8.3. Computing $\lambda(p)$

The curve E given by the equation

$$y^2 = x^3 - x \tag{8.19}$$

has many automorphisms; for example, if (y, x) is on E then so are the points $(-y, x)$ and $(iy, -x)$. We do not dwell on explaining what really happens here, but only say that this observation is tacitly used in the course of computing $\lambda(p)$.

The discriminant of E is $\Delta = 64$. For $p = 2$ we have $\nu(2) = 2$, so

$$\lambda(2) = 0. \tag{8.20}$$

For $p \equiv -1 \pmod 4$, since $\left(\frac{-1}{p}\right) = -1$ and $g(-x) = -g(x)$, we derive by (8.14) that $\lambda(p) = -\lambda(p)$, and so

$$\lambda(p) = 0 \quad \text{if } p \equiv -1 \pmod 4. \tag{8.21}$$

In the remaining case $p \equiv 1 \pmod 4$ we shall carry out computations by passing to another curve E' given by the equation

$$Y^2 = X^4 + 4. \tag{8.22}$$

There is a map from $E - (0,0)$ to E' given by

$$(y, x) \to (2x - y^2x^{-2},\ yx^{-1}).$$

This has the inverse from E' to $E - (0,0)$ given by

$$(Y, X) \to \left(\frac{1}{2}X(Y + X^2), \frac{1}{2}(Y + X^2)\right).$$

Therefore the number of points on $E/\mathbb{F}_p$ and $E'/\mathbb{F}_p$ are related by $\nu(p) - 1 = \nu'(p)$. The key advantage of dealing with E' is that E' has a diagonal equation.

Let $p \equiv 1 \pmod 4$. The multiplicative group $\mathbb{F}_p^*$ is cyclic of order $p-1 \equiv 0 \pmod 4$, and so is the character group $\hat{\mathbb{F}}_p^*$. For any $z \in \mathbb{F}_p^*$ we have

$$\#\{x \in \mathbb{F}_p^* : x^4 = z\} = \sum_{\chi^4=1} \chi(z).$$

Hence

$$\nu'(p) = 2 + \sum_{\chi^4=1} \mathcal{J}(\chi)$$

where

$$\mathcal{J}(\chi) = \sum_{Y \pmod p} \chi(Y^2 - 4).$$

There are four characters of exponent 4, all given by $\chi = 1, \eta, \eta^2, \eta^3$, where η is a fixed character of order 4. For $\chi = 1$ we get

$$\mathcal{J}(1) = p - 2.$$

For $\chi = \eta^2$ (it is the Legendre symbol) we get

$$\begin{aligned}\mathcal{J}(\eta^2) &= \sum_Y \chi((Y-2)(Y+2)) \\ &= \sum_Y \chi((Y-4)Y) = \sum_{Y\neq 0} \chi\left(\frac{Y-4}{Y}\right) \\ &= \sum_{Y\neq 0} \chi(1-4Y) = -1 + \sum_Y \chi(Y),\end{aligned}$$

whence

$$\mathcal{J}(\eta^2) = -1.$$

For $\chi = \eta^3$ we get $\mathcal{J}(\eta^3) = \mathcal{J}(\bar\eta) = \bar{\mathcal{J}}(\eta)$. From the above evaluations we infer that

$$\nu'(p) = p - 1 + \mathcal{J}(\eta) + \bar{\mathcal{J}}(\eta),$$

whence

$$\nu(p) = p + \mathcal{J}(\eta) + \bar{\mathcal{J}}(\eta),$$

and

$$\lambda(p) = -\mathcal{J}(\eta) - \bar{\mathcal{J}}(\eta). \tag{8.23}$$

Now we proceed to compute $\mathcal{J}(\eta)$ (the Jacobi sum). First we establish that

$$|\mathcal{J}(\eta)| = p^{\frac{1}{2}}. \tag{8.24}$$

Indeed, by squaring, factoring $Y^2 - 4 = (Y-2)(Y+2)$ and changing the variables several times we derive the following expressions:

$$
\begin{aligned}
|\mathcal{J}(\eta)|^2 &= \left|\sum_x \eta((x-4)x)\right|^2 = \sum\sum_{x,y\neq 0,4} \eta\left(\frac{(x-4)x}{(y-4)y}\right) \\
&= \sum_z \eta(z) \sum_{y\neq 0,4} \eta\left(\frac{yz-4}{y-4}\right) = \sum_z \eta(z) \sum_{y\neq 0,4} \eta\left(z + \frac{4(z-1)}{y-4}\right) \\
&= p - 2 + \sum_{z\neq 1} \eta(z) \sum_{v\neq 0,-1} \eta(z + (z-1)v) \\
&= p - 2 - \sum_{z\neq 1} \eta(z)(\eta(z)+1) \\
&= p - \sum_z \eta^2(z) - \sum_z \eta(z) = p.
\end{aligned}
$$

Next we determine the argument of $\mathcal{J}(\eta)$. There are not many possibilities to choose from. Since $\eta^4 = 1$ the terms of $\mathcal{J}(\eta)$ take values $0, \pm 1, \pm i$; therefore $\mathcal{J}(\eta)$ is a Gaussian integer, $\mathcal{J}(\eta) \in \mathbb{Z}[i]$. On the other hand, $p \equiv 1 \pmod 4$ factors in $\mathbb{Z}[i]$ into

$$p = \pi\bar{\pi}$$

where π is determined up to complex conjugation (π is not distinguished from $\bar{\pi}$) and a unit $\varepsilon = \pm 1, \pm i$ (by the unique factorization in the ring $\mathbb{Z}[i]$). Combining the above facts, we deduce that

$$\mathcal{J}(\eta) = \pi \tag{8.25}$$

for some prime factor of p in $\mathbb{Z}[i]$.

To determine which factor (out of eight possibilities) is correct, we test the equation (8.25) modulo the ideal

$$\mathfrak{a} = ((1+i)^3) = 2(1+i), \quad N\mathfrak{a} = 8.$$

Since the character η takes values $0, \pm 1, \pm i$, each of which except for 0 is congruent to 1 (mod $(1+i)$), we infer that

$$
\begin{aligned}
\mathcal{J}(\eta) &= \sum_{Y \pmod p} \eta(Y^2 - 4) = 1 + 2 \sum_{\substack{0<Y\leqslant \frac{p-1}{2} \\ Y\neq 2}} \eta(Y^2-4) \\
&\equiv 1 + 2\left(\frac{p-1}{2} - 1\right) \equiv p - 2 \pmod{\mathfrak{a}}.
\end{aligned}
$$

Hence for $p \equiv 1 \pmod 4$

$$\mathcal{J}(\eta) \equiv -1 \pmod{\mathfrak{a}}. \tag{8.26}$$

The above congruence together with (8.25) determines $\mathcal{J}(\eta)$ up to complex conjugation (surely one cannot be more exact as long as η is not distinguished from $\bar{\eta}$).

We say that a Gaussian integer α is primary if $\alpha \equiv 1 \pmod{\mathfrak{a}}$. Every odd α (i.e. coprime with $\mathfrak{a}$) is conjugate to exactly one primary integer. The only primary unit of $\mathbb{Z}[i]$ is 1. The product of primary numbers is primary, and every primary number factors uniquely (up to permutation) as a product of primary numbers which are Gaussian primes. By (8.25) and (8.26) it follows that $-\mathcal{J}(\eta)$ is a primary prime.

Finally by (8.23), (8.25) and (8.26) we conclude that

$$\lambda(p) = \pi + \bar{\pi} \quad \text{if } p \equiv 1 \pmod 4 \tag{8.27}$$

where $\pi\bar{\pi} = p$ and π is determined up to conjugation by the congruence

$$\pi \equiv 1 \pmod{\mathfrak{a}}, \tag{8.28}$$

i.e. π is a primary factor of p.

8.4. A Hecke Grossencharacter

Consider the multiplicative group $(\mathbb{Z}[i]/\mathfrak{a})^*$ of residue classes in $\mathbb{Z}[i]$ to modulus $\mathfrak{a}$ and prime to $\mathfrak{a}$; it is a cyclic group of 4 elements represented by the units. For α odd we define $\rho(\alpha)$ to be the unit which makes $\rho(\alpha)\alpha$ primary, i.e. $\rho(\alpha) = 1, i, i^2, i^3$ is such that

$$\rho(\alpha)\alpha \equiv 1 \pmod{\mathfrak{a}} \quad \text{if } (\alpha, \mathfrak{a}) = 1. \tag{8.29}$$

If $(\alpha, \mathfrak{a}) \neq 1$ we set $\rho(\alpha) = 0$. Thus ρ is a character on $\mathbb{Z}[i]$ to modulus $\mathfrak{a}$. Then we put

$$\chi(\alpha) = \rho(\alpha)\alpha. \tag{8.30}$$

The function χ is one of many kinds of Grossencharacters which have been invented by E. Hecke. This can be regarded as a character on ideals $\mathfrak{r} \subset \mathbb{Z}[i]$. Every ideal is a principal ideal, say $\mathfrak{r} = (a)$, with generator determined up to a unit. If $(\mathfrak{r}, \mathfrak{a}) = 1$ we can fix a by requiring $a \equiv 1 \pmod{\mathfrak{a}}$, and we set

$$\chi(\mathfrak{r}) = a. \tag{8.31}$$

If $(\mathfrak{r}, \mathfrak{a}) \neq 1$ we put $\chi(\mathfrak{r}) = 0$.

With the character χ Hecke associated the L-function defined by the Euler product (see Chapter 12)

$$L(s, \chi) = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s})^{-1}. \tag{8.32}$$