CHAPTER II

The Hasse–Weil L-Function of an Elliptic Curve

At the end of the last chapter, we used reduction modulo p to find some useful information about the elliptic curves $E_n: y^2 = x^3 - n^2x$ and the congruent number problem. We considered E_n as a curve over the prime field $\mathbb{F}_p$ where $p \nmid 2n$; used the easily proved equality $\#E_n(\mathbb{F}_p) = p + 1$ when $p \equiv 3 \pmod 4$; and, by making use of infinitely many such p, were able to conclude that the only rational points of finite order on E_n are the four obvious points of order two. This then reduced the congruent number problem to the determination of whether r, the rank of $E_n(\mathbb{Q})$, is zero or greater than zero.

Determining r is much more difficult than finding the torsion group. Some progress can be made using the number of $\mathbb{F}_q$-points. But the progress does not come cheaply. First of all, we will derive a formula for $\#E_n(\mathbb{F}_q)$ for any prime power $q = p^r$. Next, we will combine these numbers $N_r = N_{r,p} = \#E_n(\mathbb{F}_{p^r})$ into a function which is analogous to the Riemann zeta-function (but more complicated). The behavior of this complex-analytic function near the point 1 is intimately related to the group of rational points.

Before introducing this complex-analytic function, which is defined using all of the $N_{r,p}$, we introduce a much simpler function, called the "congruence zeta-function", which is built up from the $N_r = N_{r,p}$ for a fixed prime p.

§1. The congruence zeta-function

Given any sequence N_r, $r = 1, 2, 3, \ldots$, we define the corresponding "zeta-function" by the formal power series

$$Z(T) \underset{\text{def}}{=} \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right), \qquad \text{where} \quad \exp(u) \underset{\text{def}}{=} \sum_{k=0}^{\infty} \frac{u^k}{k!}. \tag{1.1}$$

At first glance, it might seem simpler to define $Z(T)$ as $\Sigma N_r T^r$; however, the above definition has crucial properties which make it the most useful one (see the problems below).

Let K be a field. Let $\mathbb{A}_K^m$ denote the set of m-tuples of elements of K. By an "affine algebraic variety in m-dimensional space over K" we mean a system of polynomial equations of the form $f_j(x_1, \ldots, x_m) = 0$, where $f_j \in K[x_1, \ldots, x_m]$. For example, a conic section is a system of two equations

$$f_1(x, y, z) = x^2 + y^2 - z^2 = 0; \qquad f_2(x, y, z) = ax + by + cz + d = 0$$

in 3-dimensional space over $\mathbb{R}$. If L is any field extension of K, the "L-points" of the variety are the m-tuples $(x_1, \ldots, x_m) \in \mathbb{A}_L^m$ for which all of the polynomials f_j vanish.

By a "projective variety in m-dimensional space over K" we mean a system of *homogeneous* polynomial equations $f_j(x_0, x_1, \ldots, x_m)$ in $m + 1$ variables. If L is a field extension of K, the "L-points" of the projective variety are the points in $\mathbb{P}_L^m$ (i.e., equivalence classes of $m + 1$-tuples $(x_0, \ldots, x_m)$, where $(x_0, \ldots, x_m) \sim (\lambda x_0, \ldots, \lambda x_m)$, $\lambda \in L^*$) at which all of the f_j vanish. For example, in the last chapter we studied the $\mathbb{F}_q$-points of the elliptic curve defined in $\mathbb{P}_{\mathbb{F}_p}^2$ by the single equation $f(x, y, z) = y^2 z - x^3 + n^2 x z^2 = 0$. (Note: Here $x_0 = z$, $x_1 = x$, $x_2 = y$ are variables for a projective variety in $\mathbb{P}_K^2$, while in the last paragraph $x_1 = x$, $x_2 = y$, $x_3 = z$ were variables for an affine variety in $\mathbb{A}_K^3$.)

If we have a projective variety, by setting $x_0 = 1$ in the f_j we obtain an affine variety whose L-points correspond to the $m + 1$-tuples with nonzero first coordinate. The remaining L-points of the projective variety will be the projective variety in $\mathbb{P}_K^{m-1}$ obtained by setting $x_0 = 0$ in all of the equations and considering the equivalence classes of m-tuples $(x_1, \ldots, x_m)$ which satisfy the resulting equations. For example, the elliptic curve with equation $y^2 z - x^3 + n^2 x z^2$ consists of the affine points—the solutions of $y^2 = x^3 - n^2 x$—and the points (x, y) of $\mathbb{P}_K^1$ for which $-x^3 = 0$, i.e., the single point $(0, 1)$ on the line at infinity $z = 0$.

Let V be an affine or projective variety defined over $\mathbb{F}_q$. For any field $K \supset \mathbb{F}_q$, we let $V(K)$ denote the set of K-points of V. By the "congruence zeta-function of V over $\mathbb{F}_q$" we mean the zeta-function corresponding to the sequence $N_r = \# V(\mathbb{F}_{q^r})$. That is, we define

$$Z(V/\mathbb{F}_q; T) \underset{\text{def}}{=} \exp\left(\sum_{r=1}^{\infty} \# V(\mathbb{F}_{q^r}) T^r / r\right). \tag{1.2}$$

Of course, N_r is finite, in fact, less than the total number of points in $\mathbb{A}_{\mathbb{F}_{q^r}}^m$ (in the affine case) or $\mathbb{P}_{\mathbb{F}_{q^r}}^m$ (in the projective case).

We shall be especially interested in the situation when V is an elliptic curve defined over $\mathbb{F}_q$. This is a special case of a smooth projective plane curve. A projective plane curve defined over a field K is a projective variety given in $\mathbb{P}_K^2$ by one homogeneous equation $f(x, y, z) = 0$. Such a curve is said to be "smooth" if there is no $K^{\text{alg cl}}$-point at which all partial derivatives

vanish. This agrees with the usual definition when $K = \mathbb{C}$ ("has a tangent line at every point").

It turns out that the congruence zeta-function of *any* elliptic curve E defined over $\mathbb{F}_q$ has the form

$$Z(E/\mathbb{F}_q; T) = \frac{1 - 2a_E T + qT^2}{(1 - T)(1 - qT)}, \tag{1.3}$$

where only the integer $2a_E$ depends on E. We shall soon prove this in the case of the elliptic curve $E_n: y^2 = x^3 - n^2x$. Let α be a reciprocal root of the numerator; then $1 - 2a_E T + qT^2 = (1 - \alpha T)(1 - \frac{q}{\alpha}T)$. If one takes the logarithmic derivative of both sides of (1.3) and uses the definition (1.1), one easily finds (see problems below) that the equality (1.3) is equivalent to the following formula for $N_r = \#E(\mathbb{F}_{q^r})$:

$$N_r = q^r + 1 - \alpha^r - (q/\alpha)^r. \tag{1.4}$$

As a special case of (1.4) we have

$$N_1 = \#E(\mathbb{F}_q) = q + 1 - \alpha - \frac{q}{\alpha} = q + 1 - 2a_E. \tag{1.5}$$

Thus, if we know that $Z(E/\mathbb{F}_q; T)$ must have the form (1.3), then we can determine a_E merely by counting the number of $\mathbb{F}_q$-points. This will give us $Z(E/\mathbb{F}_q; T)$, the value of α, and all of the values $N_r = \#E(\mathbb{F}_{q^r})$ by (1.4). In other words, in the case of an elliptic curve, the number of $\mathbb{F}_q$-points determines the number of $\mathbb{F}_{q^r}$-points for all r. This is an important property of elliptic curves defined over finite fields. We shall prove it in the special case $y^2 = x^3 - n^2x$.

It will also turn out that α is a quadratic imaginary algebraic integer whose complex absolute value is $\sqrt{q}$. In the case $y^2 = x^3 - n^2x$, it will turn out that α is a square root of $-q$ if $q \equiv 3 \pmod 4$, and is of the form $a + bi$, $a, b \in \mathbb{Z}$, $a^2 + b^2 = q$, if $q \equiv 1 \pmod 4$.

This situation is a special case of a much more general fact concerning smooth projective algebraic varieties over finite fields. The general result was conjectured by Andre Weil in [Weil 1949], and the last and most difficult part was proved by Pierre Deligne in 1973. (For a survey of Deligne's proof, see [Katz 1976a].) We shall not discuss it, except to state what it says in the case of a smooth projective *curve* (one-dimensional variety):

(i) $Z(V/\mathbb{F}_q; T)$ is a rational function of T (this is true for any variety without the smoothness assumption) which for a smooth curve has the form $P(T)/(1 - T)(1 - qT)$. Here $P(T)$ has coefficients in $\mathbb{Z}$ and constant term 1 (equivalently, its reciprocal roots are algebraic integers).

(ii) If V was obtained by reducing modulo p a variety $\tilde{V}$ defined over $\mathbb{Q}$, then $\deg P = 2g$ is twice the genus ("Betti number") of the complex analytic manifold $\tilde{V}$. Intuitively, g is the "number of handles" in the corresponding Riemann surface. An elliptic curve has $g = 1$, and the Riemann surface in Fig. II.1 has $g = 3$.

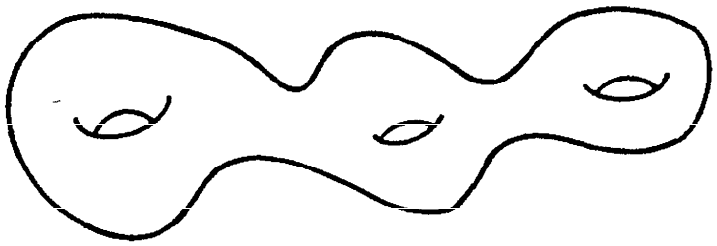

Figure II.1

(iii) If α is a reciprocal root of the numerator, then so is q/α.
(iv) All reciprocal roots of the numerator have complex absolute value $\sqrt{q}$.

One reason for the elegance of the Weil conjectures is the intriguing indirect connection between the "physical" properties of a curve (e.g., its number of handles as a Riemann surface when considered over $\mathbb{C}$) and the number theoretic properties (its number of points when considered over $\mathbb{F}_{q^r}$). Roughly speaking, it says that the more complicated the curve is (the higher its genus), the more N_r's you need to know before the remaining ones can be determined. In the simplest interesting case, that of elliptic curves, where $g = 1$, all of the N_r's are determined once you know N_1.

Problems

1. Show that if $N_r = N_r^* + N_r^{**}$ and $Z(T)$, $Z^*(T)$, $Z^{**}(T)$ are the corresponding zeta-functions, then $Z(T) = Z^*(T) \cdot Z^{**}(T)$; and if $N_r = N_r^* - N_r^{**}$, then $Z(T) = Z^*(T)/Z^{**}(T)$.

2. Show that if there exists a fixed set $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t$ such that for all r we have $N_r = \beta_1^r + \cdots + \beta_t^r - \alpha_1^r - \cdots - \alpha_s^r$, then

$$Z(T) = \frac{(1-\alpha_1 T)(1-\alpha_2 T)\cdots(1-\alpha_s T)}{(1-\beta_1 T)(1-\beta_2 T)\cdots(1-\beta_t T)}.$$

3. Prove that if $N_r < CA^r$ for some constants C and A, then the power series $Z(T)$ converges in the open disc of radius $1/A$ in the complex plane.

4. Show that if $N_r = \begin{cases} 1, & r \text{ even}; \\ 0, & r \text{ odd}, \end{cases}$ then $Z(T)$ is *not* a rational function; but if $N_r = \begin{cases} 2, & r \text{ even}; \\ 0, & r \text{ odd}, \end{cases}$ then $Z(T)$ is rational. In the latter case, interpret N_r as the number of $\mathbb{F}_{p^r}$-solutions of some equation.

5. The Bernoulli polynomials $B_r(x) \in \mathbb{Q}[x]$ have the properties: (i) $\deg B_r = r$; (ii) for all M, $B_r(M) - B_r(0) = r(1^{r-1} + 2^{r-1} + \cdots + (M-1)^{r-1})$. Now for fixed M let $N_{r-1} = \frac{1}{r}(B_r(M) - B_r(0))$. Find the corresponding $Z(T)$. (Cultural note: $B_1(x) = x - \frac{1}{2}$, $B_2(x) = x^2 - x + \frac{1}{6}$, etc.; they are uniquely determined by properties (i) and (ii) along with the normalization requirement that $\int_0^1 B_r(x)dx = 0$ for $r \geq 1$. One way to define them is by equating terms in the relation: $te^{tx}/(e^t - 1) = \sum_{r=0}^{\infty} B_r(x)t^r/r!$.)

(the residue fields of P and P', respectively) which takes a_i to a_i'. Thus, the maximal ideal $m(P)$ corresponds to d different $K^{\text{alg cl}}$-points P on V, where $d = [R(V)/m(P): K]$ is the residue degree of any of the points P.

15. In the situation of Problem 14, let $K = \mathbb{F}_q$. For a given $K^{\text{alg cl}}$-point P, the residue field is $\mathbb{F}_{q^d}$ for some d. Then P contributes 1 to each N_r for which r is a multiple of d. That is, the contribution of P to the exponent in the definition of the zeta-function is $\Sigma_{k=1}^{\infty} T^{kd}/kd$. Then $Z(V/\mathbb{F}_q; T)$ is exp of the sum of all contributions from the different $K^{\text{alg cl}}$-points P. Group together all points corresponding to a given maximal ideal, and express $Z(V/\mathbb{F}_q; T)$ as the product over all maximal ideals $\mathbf{m}$ of $(1 - T^{\deg \mathbf{m}})^{-1}$. Then show that the zeta-function belongs to $1 + T\mathbb{Z}[[T]]$. (Cultural note: If we make the change of variables $T = q^{-s}$, and define $\text{Norm}(\mathbf{m})$ to be the number of elements in the residue field, i.e., $\text{Norm}(\mathbf{m}) = q^{\deg \mathbf{m}}$, then we have $Z(V/\mathbb{F}_q; q^{-s}) = \Pi_{\mathbf{m}}(1 - \text{Norm}(\mathbf{m})^{-s})^{-1}$, which is closely analogous to the Euler product for the Dedekind zeta-function of a number field: $\zeta_K(s) = \Pi_{\mathfrak{p}}(1 - \text{Norm}(\mathfrak{p})^{-s})^{-1}$, in which the product is over all nonzero prime ideals of the ring of integers in the field K. In a number ring, a nonzero prime ideal is the same as a maximal ideal.)

16. Prove that if $Z(V/\mathbb{F}_q; T) \in \mathbb{Q}(T)$, then the numerator and denominator are in $1 + T\mathbb{Z}[T]$ (equivalently, the α's and β's in Problem 2 are algebraic integers).

§2. The zeta-function of E_n

We now return to our elliptic curve E_n, which is the curve $y^2 = x^3 - n^2x$, where n is a squarefree positive integer. More precisely, E_n is the projective completion of this curve, i.e., we also include the point at infinity. E_n is an elliptic curve over any field K whose characteristic does not divide $2n$, and, as we have seen, it is sometimes useful to take $K = \mathbb{F}_p$, or more generally $K = \mathbb{F}_q$. The purpose of this section is to express the number of $\mathbb{F}_q$-points on E_n in terms of "Jacobi sums".

To do this, we first transform the equation of E_n to a "diagonal form". We say that a hypersurface $f(x_1, \ldots, x_n) = 0$ in $\mathbb{A}_K^m$ is "diagonal" if each monomial in f involves at most one of the variables, and each variable occurs in at most one monomial. For example, the "Fermat curve" $x^d + y^d = 1$ is diagonal. It turns out that diagonal hypersurfaces lend themselves to easy computation of the N_r (much in the same way that multiple integrals are much easier to evaluate when the variables separate). We shall not treat the general case, but only the one we need to evaluate $N_r = \#E_n(\mathbb{F}_{q^r})$. (For a general treatment of diagonal hypersurfaces, see [Weil 1949] or [Ireland and Rosen 1982, Chapter II].)

We first show a relation between points on E_n: $y^2 = x^3 - n^2x$ and points on the curve E_n': $u^2 = v^4 + 4n^2$. As usual, we suppose that $p \nmid 2n$. First suppose that (u, v) is on E_n'. Then it is easy to check that the point $(x, y) = (\frac{1}{2}(u + v^2); \frac{1}{2}v(u + v^2))$ is on E_n. Conversely, if (x, y) is on E_n and its x-coordinate is nonzero, then we check that the point $(u, v) = (2x - y^2/x^2, y/x)$ is on E_n'.

Moreover, these two maps are inverse to one another. In other words, we have a one-to-one correspondence between points on E_n' and points on $E_n - \{(0, 0)\}$. Let N' be the number of $\mathbb{F}_q$-solutions (u, v) to $u^2 = v^4 + 4n^2$. Then the points on our elliptic curve consist of $(0, 0)$, the point at infinity, and the N' points corresponding to the pairs (u, v). In other words, $N_1 = \#E_n(\mathbb{F}_q)$ is equal to $N' + 2$. So it remains to compute N'. The advantage of the equation $u^2 = v^4 + 4n^2$ is that it is diagonal.

The basic ingredients in determining the number of points on a diagonal hypersurface are the Gauss and Jacobi sums over finite fields. We shall now define them and give their elementary properties.

Let $\psi: \mathbb{F}_q \to \mathbb{C}^*$ be a nontrivial additive character, i.e., a nontrivial homomorphism from the additive group of the finite field to the multiplicative group of complex numbers. (Since $\mathbb{F}_q$ is finite, the image must consist of roots of unity.) In what follows, we shall always define $\psi(x) = \xi^{\mathrm{Tr}\, x}$, where $\xi = e^{2\pi i/p}$, and Tr is the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. Since the trace is a nontrivial additive map, and its image is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, we obtain in this way a nontrivial additive character.

Now let $\chi: \mathbb{F}_q^* \to \mathbb{C}^*$ be any multiplicative character, i.e., a group homomorphism from the multiplicative group of the finite field to the multiplicative group of nonzero complex numbers. In what follows, the additive character ψ will be fixed, as defined above, but χ can vary.

We define the Gauss sum (depending on the variable χ) by the formula

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x)$$

(where we agree to take $\chi(0) = 0$ for *all* χ, even the trivial multiplicative character). We define the Jacobi sum (depending on two variable multiplicative characters) by the formula

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1 - x).$$

The proofs of the following elementary properties of Gauss and Jacobi sums are straightforward, and will be left as exercises. (Here χ_{triv} denotes the trivial character, which takes all nonzero elements of $\mathbb{F}_q$ to 1; χ, χ_1, and χ_2 denote nontrivial characters; and $\bar{\chi}$ denotes the complex conjugate (also called "inverse") character of χ, whose value at x is the complex conjugate of $\chi(x)$.)

(1) $g(\chi_{\mathrm{triv}}) = -1$; $J(\chi_{\mathrm{triv}}, \chi_{\mathrm{triv}}) = q - 2$; $J(\chi_{\mathrm{triv}}, \chi) = -1$;
$J(\chi, \bar{\chi}) = -\chi(-1)$; $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$;
(2) $g(\chi) \cdot g(\bar{\chi}) = \chi(-1)q$; $|g(\chi)| = \sqrt{q}$;
(3) $J(\chi_1, \chi_2) = g(\chi_1)g(\chi_2)/g(\chi_1\chi_2)$ if $\chi_2 \neq \bar{\chi}_1$.

We now proceed to the computation of the number N' of $u, v \in \mathbb{F}_q$ satisfying $u^2 = v^4 + 4n^2$. The key observation in computing N' is that for any $a \neq 0$ in $\mathbb{F}_q$ and any m dividing $q - 1$, the number of solutions $x \in \mathbb{F}_q$ to the equation $x^m = a$ is given by:

$$\#\{x^m = a\} = \sum_{\chi^m = 1} \chi(a), \tag{2.1}$$

where the sum is over all multiplicative characters whose m-th power is the trivial character. Namely, both sides of (2.1) equal m if a is an m-th power in $\mathbb{F}_q$ and equal 0 otherwise; the detailed proof will be left as a problem below.

By Proposition 16 of the last chapter, we know that $N_1 = q + 1$ if $q \equiv 3 \pmod 4$. In what follows, we shall suppose that $q \equiv 1 \pmod 4$.

In counting the pairs (u, v), we count separately the pairs where either u or v is zero. Thus, we write

$$\begin{aligned} N' = {} & \#\{u \in \mathbb{F}_q | u^2 = 4n^2\} + \#\{v \in \mathbb{F}_q | 0 = v^4 + 4n^2\} \\ & + \#\{u, v \in \mathbb{F}_q^* | u^2 = v^4 + 4n^2\}. \end{aligned} \tag{2.2}$$

The first term in (2.2) is obviously 2 (recall that we are assuming that $p \nmid 2n$). We use (2.1) to evaluate the second term. Let χ_4 be one of the characters of $\mathbb{F}_q^*$ having exact order 4, i.e., $\chi_4(g) = i$ for some generator g of the cyclic group $\mathbb{F}_q^*$. Then, by (2.1), the second term in (2.2) equals

$$\sum_{j=1}^{4} \chi_4^j(-4n^2) = 2 + 2\chi_4(-4n^2) \tag{2.3}$$

(where we use the fact that $-4n^2$ is a square in $\mathbb{F}_q^*$). Finally, we evaluate the third term in (2.2). Let χ_2 denote the nontrivial character of order 2 (i.e., $\chi_2 = \chi_4^2$). Using (2.1) again, we can write the third term in (2.2) as

$$\sum_{\substack{a,b \in \mathbb{F}_q^* \\ a = b + 4n^2}} \#\{u^2 = a\} \cdot \#\{v^4 = b\} = \sum_{a \in \mathbb{F}_q^*, a - 4n^2 \neq 0} \sum_{\substack{j=1,2,3,4 \\ k=1,2}} \chi_2^k(a)\chi_4^j(a - 4n^2).$$

Note that since $\chi_4^j(0) = 0$, we can drop the condition $a - 4n^2 \neq 0$ on the right. We now make the change of variable $x = a/4n^2$ in the first summation on the right. As a result, after we reverse the order of summation, the right side becomes

$$\sum_{\substack{j=1,2,3,4 \\ k=1,2}} \chi_4^j(-4n^2) \sum_{x \in \mathbb{F}_q^*} \chi_2^k(x)\chi_4^j(1 - x) = \sum_{\substack{j=1,2,3,4 \\ k=1,2}} \chi_4^j(-4n^2) J(\chi_2^k, \chi_4^j).$$

Finally, bringing together the three terms in (2.2) and using property (1) of Jacobi sums when χ_2^k or χ_4^j is trivial or they are conjugate to one another, we obtain:

$$\begin{aligned} N' &= 4 + 2\chi_4(-4n^2) + \sum_{j=1,3} \chi_4^j(-4n^2) J(\chi_2, \chi_4^j) + q - 2 + 3 \cdot (-1) \\ &\quad + 2\chi_4(-4n^2) \cdot (-1) \\ &= q - 1 + \chi_4(-4n^2)(J(\chi_2, \chi_4) + J(\chi_2, \bar{\chi}_4)). \end{aligned} \tag{2.4}$$

In the problems we show that $\chi_4(-4) = 1$. Hence, $\chi_4(-4n^2) = \chi_2(n)$. Thus, if we set

$$\alpha = \alpha_{n,q} \underset{\text{def}}{=} -\chi_2(n) \tag{2.5}$$

we conclude that

$$N_1 = \#E_n(\mathbb{F}_q) = q + 1 - \alpha - \bar{\alpha}. \tag{2.6}$$

Notice that α is an algebraic integer in $\mathbb{Q}(i)$, since the values of χ_2 and χ_4 in the definition of $J(\chi_2, \chi_4)$ are all ± 1, $\pm i$. We now pin down the Gaussian integer $\alpha = a + bi$, at least in the case when $q = p$ is a prime congruent to 1 mod 4 or $q = p^2$ is the square of a prime congruent to 3 mod 4. By property (3) relating Jacobi to Gauss sums, we have

$$\alpha = -\chi_2(n)g(\chi_2)g(\chi_4)/g(\bar{\chi}_4),$$

and hence, by property (2), we have $|\alpha|^2 = a^2 + b^2 = q$. In the two cases $q = p \equiv 1 \pmod 4$ and $q = p^2$, $p \equiv 3 \pmod 4$, there are very few possibilities for such an α. Namely, in the former case there are eight choices of the form $\pm a \pm bi$, $\pm b \pm ai$; and in the latter case there are the four possibilities $\pm p$, $\pm pi$. The following lemma enables us to determine which it is.

Lemma 1. *Let $q \equiv 1 \pmod 4$, and let χ_2 and χ_4 be characters of $\mathbb{F}_q^*$ of exact order 2 and 4, respectively. Then $1 + J(\chi_2, \chi_4)$ is divisible by $2 + 2i$ in the ring $\mathbb{Z}[i]$.*

PROOF. We first relate $J(\chi_2, \chi_4)$ to $J(\chi_4, \chi_4)$ by expressing both in terms of Gauss sums. By property (3), we have: $J(\chi_2, \chi_4) = J(\chi_4, \chi_4)g(\chi_2)^2/g(\chi_4)g(\bar{\chi}_4)$ $= \chi_4(-1)J(\chi_4, \chi_4)$ by property (2). Next, we write

$$J(\chi_4, \chi_4) = \sum \chi_4(x)\chi_4(1-x) = \chi_4^2\left(\tfrac{p+1}{2}\right) + 2\sum{}' \chi_4(x)\chi_4(1-x),$$

where Σ' is a sum over $(q-3)/2$ elements, one from each pair x, $1-x$, with the pair $\frac{(p+1)}{2}$, $\frac{(p+1)}{2}$ omitted. Notice that $\chi_4(x)$ is a power of i, and so is congruent to 1 modulo $1 + i$ in $\mathbb{Z}[i]$; thus, $2\chi_4(x)\chi_4(1-x) \equiv 2 (\mathrm{mod}\, 2 + 2i)$. As a result, working modulo $2 + 2i$, we have $J(\chi_4, \chi_4) \equiv q - 3 + \chi_4^2(\frac{(p+1)}{2}) \equiv$ $2 + \chi_4(4)$ (since $q \equiv 1 \pmod 4$). Returning to $J(\chi_2, \chi_4)$, we obtain:

$$1 + J(\chi_2, \chi_4) = 1 + \chi_4(-1)J(\chi_4, \chi_4) \equiv 1 + \chi_4(-4) + 2\chi_4(-1)$$

$$(\mathrm{mod}\ 2 + 2i).$$

Since $\chi_4(-4) = 1$, as mentioned above (and proved in the problems below), and since $2(1 + \chi_4(-1)) = 0$ or 4, it follows that $1 + J(\chi_2, \chi_4)$ is divisible by $2 + 2i$, as claimed. □

We now have the basic ingredients to prove a formula for $Z(E_n/\mathbb{F}_p; T)$.

Theorem. *Let E_n be the elliptic curve $y^2 = x^3 - n^2x$ defined over $\mathbb{F}_p$, where $p \nmid 2n$. Then*

$$Z(E_n/\mathbb{F}_p; T) = \frac{1 - 2aT + pT^2}{(1-T)(1-pT)} = \frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-pT)}, \tag{2.7}$$

where e α; $\alpha = i\sqrt{p}$ if $p \equiv 3 \pmod 4$; and if $p \equiv 1 \pmod 4$, then α is an elem $i]$ of norm p which is congruent to $(\frac{n}{p})$ modulo $2 + 2i$.

Before proving the theorem, we note that in the case $p \equiv 1 \pmod 4$ it says we choose $\alpha = a + bi$ with a odd (and b even), where the sign of a is determined by the congruence condition modulo $2 + 2i$. There are two possible choices $a + bi$ and $a - bi$; and of course the formula (2.7) does not change if we replace α by its conjugate.

PROOF. In order to obtain $Z(E_n/\mathbb{F}_p; T)$, we must let the power of p vary, and determine $N_r = \#E_n(\mathbb{F}_{p^r})$ for $p \equiv 1 \pmod 4$ and $N_{2r} = \#E_n(\mathbb{F}_{q^r})$ for $p \equiv 3 \pmod 4$, $q = p^2$ (since we know that $N_r = p^r + 1$ for odd r in that case). So we fix q equal to p in the first case and equal to p^2 in the second case (in either case $q \equiv 1 \pmod 4$), and we replace q by q^r throughout the work we did earlier to find a formula for $\#E_n(\mathbb{F}_q)$, $q \equiv 1 \pmod 4$.

Because the r is varying, we need a notation to indicate which χ_2 and χ_4 we are talking about, i.e., to indicate for which finite field they are multiplicative characters. Let $\chi_{2,1} = \chi_2$ denote the unique nontrivial character of $\mathbb{F}_q^*$ of order 2, and let $\chi_{4,1} = \chi_4$ denote a fixed character of $\mathbb{F}_q^*$ of exact order 4 (there are two, the other one being $\bar{\chi}_4$). Then by composing χ_2 or χ_4 with the norm from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$, we obtain a character of $\mathbb{F}_{q^r}^*$ of exact order 2 or 4, respectively. We denote these characters $\chi_{2,r}$ and $\chi_{4,r}$. For example, if g is a generator of $\mathbb{F}_q^*$ such that $\chi_4(g) = i$, and if g_r is a generator of $\mathbb{F}_{q^r}^*$ whose norm is g, i.e., $(g_r)^{1+q+\cdots+q^{r-1}} = g$, then we have $\chi_{4,r}(g_r) = i$. If $\mathbb{N}_r$ denotes the norm from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$, we can write our definitions:

$$\chi_{4,r} = \chi_4 \circ \mathbb{N}_r, \qquad \chi_{2,r} = \chi_2 \circ \mathbb{N}_r. \tag{2.8}$$

With these definitions, using (2.5) and (2.6), we can write:

$$\begin{aligned} &\#E_n(\mathbb{F}_{q^r}) = q^r + 1 - \alpha_{n,q^r} - \bar{\alpha}_{n,q^r}, \\ &\text{where} \quad \alpha_{n,q^r} = -\chi_{2,r}(n)\frac{g(\chi_{2,r})g(\chi_{4,r})}{g(\bar{\chi}_{4,r})}. \end{aligned} \tag{2.9}$$

We now use a basic relationship, called the Hasse–Davenport relation, for Gauss sums over extensions of finite fields. The Hasse–Davenport formula is:

$$-g(\chi \circ \mathbb{N}_r) = (-g(\chi))^r. \tag{2.10}$$

The proof of this fact will be given in a series of exercises below. Applying (2.10) to the three Gauss sums in (2.9), and observing that $\chi_{2,r}(n) = \chi_2(n^r) = \chi_2(n)^r$, we conclude the following basic relationship:

$$\alpha_{n,q^r} = \alpha_{n,q}^r. \tag{2.11}$$

The theorem now follows quickly. First suppose $p \equiv 1 \pmod 4$, in which case $q = p$. Then $\chi_2(n)$ is the Legendre symbol $(\frac{n}{p})$. Using (2.5) and Lemma 1, we find that $\alpha = \alpha_{n,p}$ is a Gaussian integer of norm p which is congruent to $(\frac{n}{p})$ modulo $2 + 2i$; and, by (2.9) and (2.11),

$$N_r = p^r + 1 - \alpha^r - \bar{\alpha}^r.$$

This proves the theorem when $p \equiv 1 \pmod 4$ (see Problem 2 of §II.1).

Now suppose that $p \equiv 3 \pmod 4$, $q = p^2$. Then $\chi_2(n) = 1$, since all elements of $\mathbb{F}_p$ are squares in $\mathbb{F}_{p^2}$. Then Lemma 1 tells us that $\alpha_{n,q}$ is a Gaussian integer of norm q which is congruent to 1 mod $2 + 2i$. Of the four Gaussian integers $i^j p$, $j = 0, 1, 2, 3$, having norm q, only $\alpha_{n,q} = -p$ satisfies the congruence condition. Then, by (2.6) and (2.11), we conclude that for r even we have

$$N_r = \#E_n(\mathbb{F}_{q^{r/2}}) = p^r + 1 - (-p)^{r/2} - (-p)^{r/2}.$$

Since $N_r = p^r + 1$ for odd r, we have for any r:

$$N_r = p^r + 1 - (i\sqrt{p})^r - (-i\sqrt{p})^r.$$

This completes the proof of the theorem. □

We conclude this section by calling attention to the role Lemma 1 has played in pinning down the reciprocal roots α and $\bar{\alpha}$ in (2.7). The congruence condition in Lemma 1 will again be needed when we start working with the Hasse–Weil L-function of the elliptic curve E_n, which combines the α's for different primes p. In that context, Lemma 1 is a special case of a general fact about how Jacobi sums vary as we vary the prime p. The general case is treated in [Weil 1952].

Problems

1. Prove properties (1)–(3) of Gauss and Jacobi sums that were given in the text.

2. Let G be a finite group, and let $\check{G}$ denote the group of characters χ (i.e., of homomorphisms $\chi: G \to \mathbb{C}^*$). Recall that for any nontrivial $\chi \in \check{G}$, $\Sigma_{g \in G} \chi(g) = 0$. Notice that any fixed $g \in G$ gives a character $g: \chi \mapsto \chi(g)$ on the group $\check{G}$, and also on any subgroup $S \subset \check{G}$. Apply these general considerations to the case when $G = \mathbb{F}_q^*$ and S is the subgroup of characters χ such that $\chi^m = 1$. In that way prove the relation (2.1) in the text.

3. Let $q \equiv 1 \pmod 4$, and let χ_4 have exact order 4. Show that $\chi_4(4)$ and $\chi_4(-1)$ are both equal to 1 if $q \equiv 1 \pmod 8$ and equal to -1 if $q \equiv 5 \pmod 8$. Conclude that $\chi_4(-4) = 1$ in all cases.

4. Show that $g(\chi_2)^2 = (-1)^{(q-1)/2} q$. It is somewhat harder to determine which square root to take to get $g(\chi_2)$ (see [Borevich and Shafarevich 1966, pp. 349–353]). Compute $g(\chi_2)$ when $q = 3, 5, 7, 9$.

5. For $q \equiv 1 \pmod 4$, again let χ_2 be the nontrivial quadratic character, and let χ_4 and $\bar{\chi}_4$ be the two characters of exact order 4. Compute $J(\chi_2, \chi_4)$ and $J(\chi_2, \bar{\chi}_4)$ directly from the definition when $q = 5, 9, 13, 17$.

6. Show that if χ_2 is the nontrivial quadratic character of $\mathbb{F}_q^*$ and χ is any nontrivial character, then $J(\chi_2, \chi) = \chi(4) J(\chi, \chi)$.

7. Let χ_3 and $\bar{\chi}_3$ be the two characters of $\mathbb{F}_q^*$ of order 3, where $q \equiv 1 \pmod 3$. Compute $J(\chi_3, \chi_3)$ and $J(\bar{\chi}_3, \bar{\chi}_3)$ directly from the definition when $q = 7, 13$.

Therefore

$$\prod_{i=1}^{n}(p-r_i)\prod_{j=1}^{m}s_j \equiv (\frac{p-1}{2})! \pmod{p}$$

Simplifying, we have

$$(-1)^n\prod_{i=1}^{n}r_i\prod_{j=1}^{m}s_j \equiv (\frac{p-1}{2})! \pmod{p}$$

In addition, however, we have

$$\prod_{i=1}^{n}r_i\prod_{j=1}^{m}s_j \equiv \prod_{k=1}^{\frac{p-1}{2}}ka \equiv a^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}k \equiv a^{\frac{p-1}{2}}(\frac{p-1}{2})! \pmod{p}$$

Therefore

$$(-1)^n a^{\frac{p-1}{2}}(\frac{p-1}{2})! \equiv (\frac{p-1}{2})! \pmod{p}$$

which implies that

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$$

The conclusion now follows from Euler's Criterion (Theorem 7.2) and Lemma 7.1. ■

For example, let us use Gauss' Lemma to evaluate $(\frac{3}{11})$. Since $\frac{1}{2}(11-1)=5$, we look at the first 5 multiples of 3, namely, 3, 6, 9, 12, 15. The least positive residues (mod 11) are 3, 6, 9, 1, 4. Exactly 2 of these least positive residues exceed $\frac{11}{2}$, namely, 6 and 9. Therefore $\frac{3}{11}=(-1)^2=1$.

Next, let us evaluate $(\frac{7}{13})$ via Gauss' Lemma. Since $\frac{1}{2}(13-1)=6$, we look at the first 6 multiples of 7, namely, 7, 14, 21, 28, 35, 42. The least positive residues (mod 13) are, 7, 1, 8, 2, 9, 3. exactly 3 of these least positive residues exceed $\frac{13}{2}$, namely, 7, 8, and 9. Therefore $(\frac{7}{13})=(-1)^3=-1$.

If we apply Gauss' Lemma to the case $a=2$, we obtain an explicit formula for $(\frac{2}{p})$, which is given by Theorem 7.5.

Theorem 7.5 If p is an odd prime, then

$$\left(\frac{2}{p}\right)=\begin{cases}1 & \text{if } p\equiv\pm1 \pmod 8\\ -1 & \text{if } p\equiv\pm3 \pmod 8\end{cases}$$

Proof: Applying Gauss' Lemma, we look at the first $\frac{p-1}{2}$ multiples of 2, namely, at $\{2, 4, 6, \ldots, p-1\}$. These positive integers are all less than p, so they are their own least positive residues (mod p). Let S_p denote the set of least positive residues (mod p) that exceed $\frac{p}{2}$. If $p = 8k+1$, so that $\frac{p}{2} = 4k + \frac{1}{2}$, then $S_p = \{4k+2, 4k+4, \ldots, 8k\}$. If $p = 8k-1$, so that $\frac{p}{2} = 4k - \frac{1}{2}$, then $S_p = \{4k, 4k+2, \ldots, 8k-2\}$. In either case, these residues are $2k$ in number, so $(\frac{2}{p}) = (-1)^{2k} = 1$.

If $p = 8k+3$, so that $\frac{p}{2} = 4k+\frac{3}{2}$, then $S_p = \{4k+2, 4k+4, \ldots, 8k+2\}$. Finally, if $p = 8k+5$, so that $\frac{p}{2} = 4k + \frac{5}{2}$, then

$$S_p = \{4k+4, 4k+6, \ldots, 8k+4\}.$$

In either case, these residues are $2k+1$ in number, so $(\frac{2}{p}) = (-1)^{2k+1} = -1$. ■

For example, since $13 \equiv -3 \pmod 8$, it follows that $(\frac{2}{13}) = -1$. Also, since $17 \equiv 1 \pmod 8$, it follows that $(\frac{2}{17}) = 1$.

A more compact formulation of Theorem 7.5 is the following:

Theorem 7.5A If p is an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Recall that a Mersenne prime is a prime of the form $2^p - 1$, where p itself is prime. By virtue of Theorem 7.5, we can prove that $2^p - 1$ is composite for certain primes, p.

Theorem 7.6 If the prime $p > 3$, $p \equiv 3 \pmod 4$, and $q = 2p+1$ is prime, then $2^p - 1$ is composite.

Proof: Since $p \equiv 3 \pmod 4$ and $q = 2p+1$ by hypothesis, it follows that $q \equiv 7 \pmod 8$. Therefore Theorem 7.5 implies $(\frac{2}{q}) = 1$. Now Euler's Criterion implies $2^{\frac{q-1}{2}} \equiv 1 \pmod q$, that is, $q \mid (2^p - 1)$. If $n > 3$, one can prove by induction that $2^n - 1 > 2n + 1$. Since $p > 3$ by hypothesis, we have $2^p - 1 > q$. Therefore $2^p - 1$ is composite, having q as a factor. ■

Remarks

If $2p+1$ is prime, then $3 \nmid (2p+1)$, so $p \equiv 2 \pmod 3$. If also $p \equiv 3 \pmod 4$, then $p \equiv 11 \pmod{12}$. The five smallest primes for which Theorem 7.6 holds are 11, 23, 83, 131, 179.

■