PARABOLIC POINTS AND ZETA-FUNCTIONS OF MODULAR CURVES

UDC 511

Ju. I. MANIN

Abstract. In this paper we obtain explicit formulas for the values at the center of the critical strip of Dirichlet series connected with weight 2 parabolic forms of the group $\Gamma_0(N)$. In particular, these formulas allow us to verify the Birch–Swinnerton-Dyer conjecture on the order of a zero for uniformizable elliptic curves over certain Γ-extensions. We also give applications to noncommutative reciprocity laws.

Introduction

Let X be an elliptic curve over the field $\mathbb{Q}$, N its conductor, ω a Néron differential, and $L(X, s)$ the canonical Dirichlet series. Further, let X_N be the standard modular curve over $\mathbb{Q}$ parametrized by the group $\Gamma_0(N)$. Weil [16] conjectured that there exists a morphism $\psi : X_N \to X$ over $\mathbb{Q}$ such that the differential $\psi^*(\omega)$ lifted to the uppper halfplane H has the same Fourier coefficients as the Dirichlet series $L(X, s)$ (see the precise formulation in §5.2 of this paper). We call such a morphism ψ a *Weil uniformization* of the curve X.

In this paper we show that the existence of a Weil uniformization for the curve X allows us to give explicit formulas for the values of $L(X, 1)$, and also $L(X \otimes K, 1)$, for all possible abelian extensions $K \supset \mathbb{Q}$. These explicit formulas have the structure predicted by the Birch–Swinnerton-Dyer conjectures. Comparison with Mazur's theory [10] of elliptic curves over Γ-extensions of $\mathbb{Q}$ also shows a good agreement with the Birch–Swinnerton-Dyer conjecture. In particular, Mazur's "anomalous prime numbers" appear in an analytic context.

The general idea for obtaining explicit formulas for $L(X \otimes K, 1)$ consists in the following. Let $\Phi(z)dz$ be the preimage of ω on H, and let $\{0, i\infty\}$ be the path on $X_N(\mathbb{C})$ which is the image of the imaginaty semiaxis on H. From the classical integral representation for $L(X, s)$, we find, after a suitable normalization of ψ, that

$$L(X, 1) = \int_0^{i\infty} \Phi(z)dz = \int_{\{0, i\infty\}} \psi^*(\omega) = \int_{\psi_*\{0, i\infty\}} \omega.$$

Since $\psi_*(i\infty)$ is the zero point on $X(\mathbb{C})$, it follows that $L(X, 1)$ is the Abel-Jacobi

---

AMS (MOS) subject classifications (1970). Primary 14G10; Secondary 14H99.

)

:gument of the image of $0 \in H$, i. e. of some parabolic point on X_N. If the images of
and $i\infty$ coincided, then to compute $L(X, 1)$ we would have to integrate ω over some
losed path in $X(\mathbf{C})$ (and even $X(\mathbf{R})$), so that the number $L(X, 1)$ would be an integral
ultiple of the minimal real period of the differential ω. In general this is not the case.
revertheless, we were able to find a technical device which allows us to reduce to in-
egration over closed paths in $X(\mathbf{C})$. Hecke operators are used to do this in the case of
round field $\mathbf{Q}$, and in the case of an abelian extension $K \supset \mathbf{Q}$ we use the expansion of
ne series $L(X \otimes K, s)$ with respect to the characters χ of the Galois group and the
lecke-Weil lemma on Mellin tranforms of the series $L_\chi(X, s)$. This device and the
esulting formulas make up the conceptual center of the paper; they are presented in
§3–5.

The homology classes in the group $H_1(X_N(\mathbf{C}), \mathbf{Z})$ over which we must integrate
$\phi^*(\omega)$ to compute $L(X \otimes K, s)$ are fundamental arithmetic invariants of the curves X
and X_N. Hence the paper begins by studying them: in §1 we prove a new theorem on
he structure of the first homology group of a curve uniformized by any subgroup G of
the modular group, and in §2 we specialize this theorem to the case $G = \Gamma_0(N)$.

§§6 and 7 contain applications of these results. Namely, §6 is devoted to com-
paring them with the Birch–Swinnerton-Dyer conjecture. To make this comparison, we
nust have independent information about the rank of $X(K)$ and the order of the Tate-
Šafarevič group of the curve $X \otimes K$. Mazur's theory [10], [11] (see also [9]) obtains
several results of this type, and they actually lend themselves to detailed comparison
with our formulas.

In §7 we give new exact formulas for the coefficients of parabolic forms relative
to the group $\Gamma_0(N)$, which call to mind the noncommutative reciprocity law or the
Eichler relations, where, however, we have an indefinite rather than a definite quater-
nion quadratic form.

Finally, §8 contains tables of arithmetic invariants and a discussion of them.

I am grateful to A. N. Andrianov, whose conversations with me stimulated some
new ideas for this paper.

I am also grateful to M. Z. Rozenfel'd, who computed vast tables of the functions
$x^{\pm}$ for the group $\Gamma_0(11)$ on the computer "System 4" of the Institute for Control Prob-
lems of the Academy of Sciences of the USSR, and to V. Drinfel'd, who composed similar
tables for the groups $\Gamma_0(N)$ with $N = 14, 17, 19$ and who kindly agreed to their publi-
cation in this article.

After completing this work, I learned that Professor Birch (England) has also ob-
tained some results close to ours, and that Professor Mazur (USA) and Professor
Swinnerton-Dyer (England) have independently examined the functions $x^{\pm}$.

§1. Homology of modular curves

1. 1. General information. For the duration of the paper we use the following notation: $H = \{z \in \mathbf{C} \mid \operatorname{Im} z > 0\}$ is the upper halfplane; $\overline{H} = H \cup \mathbf{Q} \cup (i\infty)$ is its compactification with the usual topology;

$$\Gamma = \left\{ z \rightsquigarrow \frac{az+b}{cz+d} \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z}) \right\}$$

is the group of automorphisms of $\overline{H}$, which we identify with $\mathrm{PL}(2, \mathbf{Z}) = \mathrm{SL}(2, \mathbf{Z})/(\pm 1)$ and whose elements are written as the corresponding matrices.

Let $G \subset \Gamma$ be a subgroup of finite index. The topological space $X_G(\mathbf{C}) = G\backslash\overline{H}$ has a natural structure of a smooth compact complex space of topological dimension 2. By $\phi : \overline{H} \to X_G(\mathbf{C})$ we always designate the natural projection mapping.

Let $i \in H$, $i^2 = -1$; $\rho = e^{\pi i/3} \in H$. Points in the set $\phi(\Gamma i \cup \Gamma\rho) \subset X_G(\mathbf{C})$ are called **elliptic points**, and points in $\phi(\mathbf{Q} \cup (i\infty)) = \phi(\Gamma(i\infty)) \subset X_G(\mathbf{C})$ are called **parabolic points**. The map ϕ is unramified outside these points. Both sets are finite.

1. 2. The classes $\{\alpha, \beta\}_G$. Let $\alpha, \beta \in \overline{H}$ be two points such that $\phi(\alpha) = \phi(\beta) \in X_G(\mathbf{C})$, or, equivalently, $G\alpha = G\beta$. Then any path from α to β on $\overline{H}$ becomes a closed path on $X_G(\mathbf{C})$ whose homology class depends only on α and β. This homology class will always be denoted by the symbol $\{\alpha, \beta\}_G \in H_1(X_G(\mathbf{C}), \mathbf{Z})$.

More generally, integration allows us to associate a homology class with *real* coefficients to any pair of points $\alpha, \beta \in \overline{H}$ even if $\phi(\alpha) \neq \phi(\beta)$. We consider the differentials of the first kind $\omega \in H^0(X_G(\mathbf{C}), \Omega^1)$. Any class $\gamma \in H_1(X_G(\mathbf{C}), \mathbf{Z})$ determines a functional on the space of these differentials: $\omega \rightsquigarrow \int_\gamma \omega$. The group of such functionals forms a lattice of maximal rank in the dual space of $H^0(X_G(\mathbf{C}), \Omega^1)$. Extending this map by $\mathbf{R}$-linearity, we obtain an $\mathbf{R}$-isomorphism

$$H_1(X_G(\mathbf{C}), \mathbf{R}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{C}}(H^0(X_G(\mathbf{C}), \Omega^1), \mathbf{C}).$$

Consequently for any two points $\alpha, \beta \in \overline{H}$ the functional $\omega \rightsquigarrow \int_\alpha^\beta \phi^*(\omega)$ can be identified with a real first homology class, which we shall denote by $\{\alpha, \beta\}_G$ in the general case. Obviously, if $\phi(\alpha) = \phi(\beta)$ this notation coincides with the earlier notation. We shall sometimes write $\{\alpha, \beta\}$ instead of $\{\alpha, \beta\}_G$ and $\int_{\{\alpha,\beta\}} \omega$ instead of $\int_\alpha^\beta \phi^*(\omega)$.

1. 3. First properties of the classes $\{\alpha, \beta\}$. Obviously, $\{\alpha, \alpha\} = 0$, $\{\alpha, \beta\} = -\{\beta, \alpha\}$. The following properties are also obtained immediately from the definition:

a) $\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} = 0$.

b) $\{g\alpha, g\beta\}_G = \{\alpha, \beta\}_G$ for all $g \in G$.

c) If the genus of $X_G(\mathbf{C})$ is nonzero, then $\{\alpha, \beta\}_G \in H_1(X_G(\mathbf{C}), \mathbf{Z})$ if and only if $\beta \in G\alpha$ or, equivalently, $\phi(\alpha) = \phi(\beta)$.

(Sufficiency follows from the definition, and necessity follows from the Abel-Jacobi inversion theorem.)

The following fact requires a somewhat more detailed discussion.

1. 4. Proposition. *Let $\alpha \in \overline{H}$. The map*

$$G \to H_1(X_G(\mathbf{C}), \mathbf{Z}) : g \rightsquigarrow \{\alpha, g\alpha\}_G$$

is a surjective group homomorphism which does not depend on the choice of α. The kernel of this homomorphism is generated by the commutator, by the elliptic elements, and by the parabolic elements of the group G.

Proof. The fact that the map $g \rightsquigarrow \{\alpha, g\alpha\}$ is a homomorphism is easily obtained formally by applying 1.3 a) and b):

$$\{\alpha, gh\alpha\} = \{\alpha, g\alpha\} + \{g\alpha, gh\alpha\} = \{\alpha, g\alpha\} + \{\alpha, h\alpha\}.$$

To prove the remaining assertions, we must use a direct geometric interpretation of this homomorphism.

We first suppose that $\phi(\alpha) \in X_G(\mathbf{C})$ is neither an elliptic nor a parabolic point. Let H^0 be the complement of $\Gamma i \cup \Gamma\rho$ in H, and let $X_G^0(\mathbf{C})$ be the complement of the set of elliptic and parabolic points. The map $\phi: H^0 \to X_G^0(\mathbf{C})$ is an unramified covering with Galois group G. Consequently any point $\alpha \in H^0$ determines a surjective homomorphism $\pi_1(X_G^0(\mathbf{C}), \phi(\alpha)) \to G$. Its explicit description is as follows: suppose we are given a closed path on $X_G^0(\mathbf{C})$ starting at $\phi(\alpha)$. We lift it to a path in H^0 starting at α. The endpoint of this path has the form $g\alpha$ for a uniquely determined element $g \in G$. This element is what we associate to the class of the original path on $X_G^0(\mathbf{C})$.

It is clear from this description that the composite map

$$\pi_1(X_G^0(\mathbf{C}), \varphi(\alpha)) \to G \to H_1(X_G(\mathbf{C}), \mathbf{Z})$$

(the second row takes g to $\{\alpha, g\alpha\}_G$) coincides with the canonical homorphism of the fundamental group of the surface $X_G^0(\mathbf{C})$ into the homology group of the compactification $X_G(\mathbf{C})$. This immediately implies that the map is surjective and does not depend on the choice of the point α. Further, the structure of the group π_1 is well known; using this, we easily observe that the kernel of the homomorphism $\pi_1 \to H_1$ is generated in π_1 by the commutator and the circuits around the elliptic and parabolic points, which contract in compactification. But the images of these circuits in G make up precisely the elliptic and parabolic elements. This completes the discussion of the case $\alpha \in H^0$.

Finally, let $\alpha \in \Gamma(i, \rho, i\infty)$ and $g \in G$. We choose a point $\alpha_0 \in H^0$ so close to α that there exist open neighborhoods $U_1 \supset (\alpha, \alpha_0)$, $U_2 \supset (g\alpha, g\alpha_0)$ in $\overline{H}$ such that the union of their images $\phi(U_1) \cup \phi(U_2)$ in $X_G(\mathbf{C})$ is simply connected. We choose a path from α to $g\alpha$ and one from α_0 to $g\alpha_0$, which coincide outside $U_1 \cup U_2$. Since their images on $X_G(\mathbf{C})$ coincide outside $\phi(U_1) \cup \phi(U_2)$, it follows that the homology classes of these paths are identical, so that $\{\alpha, g\alpha\}_G = \{\alpha_0, g\alpha_0\}_G$. This completes the proof, because all the required properties have been proved for the classes $\{\alpha_0, g\alpha_0\}_G$. □

1.5. **Distinguished classes.** Let $J = G\backslash\Gamma$ be the set of right cosets. We define the map

$$\xi: J \to H_1(X_G(\mathbf{C}), \mathbf{R})$$

as follows: if $j \in J$ and g is any representative of the class j, then

$$\xi(j) = \{g(0), g(i\infty)\}_G. \tag{1}$$

Obviously this class does not depend on the choice of the representative g (see 1.3 b)). We have thereby defined a finite family of homology classes $\xi(J)$; we shall call its elements **distinguished classes.** We note that, in general, they are not integral.

1.6. **Proposition.** a) *Any class in $H_1(X_G(\mathbf{C}), \mathbf{Z})$ can be represented as a sum of distinguished classes. In particular, the distinguished classes generate $H_1(X_G(\mathbf{C}), \mathbf{R})$ as an $\mathbf{R}$-space.*

b) *The representation of any class $h \in H_1(X_G(\mathbf{C}), \mathbf{Z})$ as a sum $\Sigma m_k\{\alpha_k, \beta_k\}$ of distinguished classes can be chosen so that $\Sigma m_k(\phi(\beta_k) - \phi(\alpha_k)) = 0$ (as a zero-dimensional cycle on $X_G(\mathbf{C})$).*

Proof. By Proposition 1.4, any class in $H_1(X_G(\mathbf{C}), \mathbf{Z})$ has the form $\{0, g(0)\}$, where $g \in G$. If $g(0) = i\infty$, then this class is distinguished and $\phi(i\infty) - \phi(0) = 0$. Otherwise, let $g(0) = b/a$ be a rational number in lowest terms, $a > 0$. Also let $b > 0$; the case $b < 0$ is treated similarly. We expand b/a as a continued fraction and consider the successive convergents in lowest terms:

$$\frac{b}{a} = \frac{b_n}{a_n}, \frac{b_{n-1}}{a_{n-1}}, \ldots, \frac{b_0}{a_0} = \frac{b_0}{1}, \frac{b_{-1}}{a_{-1}} = \frac{1}{0}, \frac{b_{-2}}{a_{-2}} = \frac{0}{1}$$

(the last two "fractions" are added formally).

It is well known that $b_k a_{k-1} - b_{k-1}a_k = (-1)^{k-1}$, so that

$$g_k = \begin{pmatrix} b_k & (-1)^{k-1}b_{k-1} \\ a_k & (-1)^{k-1}a_{k-1} \end{pmatrix} \in \Gamma.$$

Hence the classes

$$\left\{\frac{b_{k-1}}{a_{k-1}}, \frac{b_k}{a_k}\right\} = \{g_k(0), g_k(i\infty)\}$$

are distinguished. Finally, by 1.3 a),

$$\left\{0, \frac{b}{a}\right\} = \sum_{k=-1}^{n} \left\{\frac{b_{k-1}}{a_{k-1}}, \frac{b_k}{a_k}\right\} = \sum_{k=-1}^{n} \xi(Gg_k). \tag{2}$$

This representation obviously has the required properties, so the proof is finished. ■

1.7. **Relations between distinguished classes.** The group Γ acts on the right on the set of right cosets $J = G\backslash\Gamma$. In this group we consider the two special elements

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } t = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}; \quad s^2 = t^3 = \mathrm{id}.$$

The element s takes $(0, i\infty)$ to $(i\infty, 0)$ and successive application of t takes $(0, i\infty)$ to $(i\infty, 1)$ and then to $(1, 0)$. Using the definition of $\xi(j)$ (see (1)) and property 1.3 a), we find two types of relations between distinguished classes:

$$\xi(j) + \xi(js) = 0, \quad \xi(j) = 0, \text{ if } j = js; \tag{3}$$

$$\xi(j) + \xi(jt) + \xi(jt^2) = 0, \quad \xi(j) = 0, \quad \text{if} \quad j = jt \tag{4}$$

(the second relation in each group follows because there is no torsion). We show that in some sense this system of relations is complete. In order to formulate the result precisely, we introduce some new notation.

1.8. a) **Algebraic formulation.** We let C designate the abelian group generated by the symbols (j) for all $j \in G\backslash\Gamma$, with the relations

$$(j) + (js) = 0, \quad (j) = 0, \quad \text{if} \quad j = js. \tag{3'}$$

We call the elements of the group C ***G-chains***. Let $g \in \Gamma$ belong to the class $j \in J$, $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. By the ***boundary*** of the chain (j) we mean the difference between the two parabolic points: $\phi(g(i\infty)) - \phi(g(0)) = Ga/c - Gb/d$. We consider this difference as an element of the free abelian group generated by the set of parabolic points $G\backslash(Q \cup (i\infty))$. Since s interchanges 0 and $i\infty$, it follows from (3') that the boundary operator extends to the entire group C by linearity. We designate its kernel by Z; the elements of the kernel are called ***G-cycles***.

Finally, let B be the subgroup of C generated by elements (j) for all $j \in J$ with the condition $j = jt$, and by the elements $(j) + (jt) + (jt^2)$ for the remaining j. We easily see that $B \subset Z$; the elements of B are called ***G-boundaries***.

The map $\xi : G\backslash\Gamma \to H_1(X_G(\mathbf{C}), \mathbf{R})$, defined in 1.5, extends to a homomorphism $\xi : C \to H_1(X_G(\mathbf{C}), \mathbf{R})$ because $\xi(j) + \xi(js) = 0$. Here $\xi(Z)$ coincides with the integral homology subgroup by Proposition 1.6 b), and $\xi(B) = 0$ by (4).

Thus we obtain a surjective homomorphism

$$Z/B \to H_1(X_G(\mathbf{C}), \mathbf{Z}). \tag{5}$$

b) **Geometric formulation.** The groups C, Z and B can be realized as the subgroups of 1-chains (1-cycles, 1-boundaries) of some cell complex $K(G)$, which we shall call a ***parabolic complex***. Here is its description.

0-cells are the elements of the set of parabolic points $G\backslash(Q \cup i\infty)$.

1-cells are in one-to-one correspondence with the set of orbits of the group (id, s), which acts on the right on $G\backslash\Gamma$. Every such cell (j, js) joins two 0-cells in the boundary (j) (or (js)): Ga/c and Gb/d, if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ belongs to the class j. If these 0-cells coincide, then the corresponding 1-cell is a loop. We choose the orientation arbitrarily.

2-cells are of two sorts: two-sided and triangular. Let $j \in J$, $j = jt$. Then the 1-cell corresponding to (j, js), as described above, is a loop: if $g \in \Gamma$ belongs to the class j, then $Gg(0) = Ggt(0) = G(i\infty)$. We glue this loop by a 2-cell: we call such cells **two sided.**

Finally, let $j \in J$, $j \neq jt$. Then the 1-simplices (j, js), (jt, jts) and (jt^2, jt^2s), form a triangle; we glue it with a 2-cell; we call such 2-cells **triangular.**

It is now clear that there exists a map $C \to C_1(K(G))$ which takes a G-chain (j) to a $K(G)$-chain: "the simplex (j, js), oriented from Gb/d to Ga/c" (if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ belongs to the class j). We easily see that this map induces an isomorphism $Z/B \xrightarrow{\sim} H_1(K(G), \mathbf{Z})$, which, together with (5), gives us a surjective map

$$H_1(K(G), \mathbf{Z}) \to H_1(X_G(\mathbf{C}), \mathbf{Z}). \tag{6}$$

The following theorem is the fundamental result of this section. It gives a representation of the group $H_1(X_G(\mathbf{C}), \mathbf{Z})$ by generators and relations which is convenient for computation and is functorial in G.

1.9. **Theorem.** *The maps (5) and (6) are isomorphisms.*

Proof. We construct a complex L of the space $X_G(\mathbf{C})$ and represent $H_1(X_G(\mathbf{C}), \mathbf{Z})$ as the factor group $Z_1(L)/B_1(L)$ of the 1-cycles of L by the 1-boundaries.

We then imbed the group Z in $Z_1(L)$ in such a way that $z \bmod B_1(L) = \xi(z)$ for all $z \in Z$.

Finally, we show that the boundary of any 2-cell of the complex L belongs to Z (under the above imbedding $Z \subset Z_1(L)$) and coincides with one of the generators of the group B of the form (j) (for $j = jt$) or $(j) + (jt) + (jt^2)$.

Obviously all these results and the surjectivity of ξ give us the isomorphism $Z/B \simeq Z_1(L)/B_1(L) = H_1(X_G(\mathbf{C}), \mathbf{Z})$, which we are trying to establish.

We realize this program in several steps.

a) *Preparation for constructing the complex L.* Let $\alpha, \beta \in \overline{H}$ be two points. We let $\langle\alpha, \beta\rangle$ designate the segment joining them along the geodesic oriented from α to β. (We recall that the geodesics are semicircles and lines orthogonal to the real axis.)

The triangles, quadrilaterals, etc. which we refer to will be the figures on $\overline{H}$ formed by geodesic segments joining the vertices of these figures, and also their ϕ-images on $X_G(\mathbf{C})$.

We let E'' designate the interior of the triangle with vertices $(0, 1, i\infty)$, and we let E' designate the union of the interior of the quadrilateral with vertices $(i, \rho, 1 + i, i\infty)$ and the side $\langle i, \rho\rangle$, except for the vertex i. Each of the quadrilaterals E', tE' and t^2E' is a fundamental region for the entire group Γ. In addition, all the 1-simplices in Figure 1—the half-sides and half-medians of the triangle E''—imbed homomorphically into $X_\Gamma(\mathbf{C})$. (These are both classical assertions.)

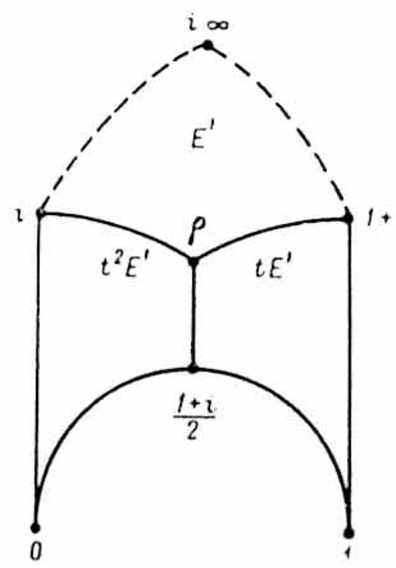

Figure 1

b) *Description of L.*

0-cells. These are all the parabolic points and all the i-elliptic points on $X_G(\mathbf{C})$, the images of the vertices and the midpoints of the sides of the triangles gE'', $g \in \Gamma$.

1-cells. These are the images of the half-sides of the triangles gE'', $g \in \Gamma$, oriented "from the vertex to the midpoint," i. e. from the parabolic point to the i-elliptic point.

It is convenient to introduce a family of 1-cells indexed by the classes $j \in G\backslash\Gamma$ by setting

$$e_1(j) = \text{image } \langle g(i\infty), g(i)\rangle \text{ in } X_G(\mathbf{C}) \tag{7}$$

for any representative $g \in \Gamma$ of the class j.

Since Γ is transitive on half-sides, it follows that any 1-cell has the form $e_1(j)$ for some $j \in J$. On the other hand, the stationary subgroup of i in Γ is equal to

(id, s); hence $e_1(j) = e_1(k)$ is only possible for $k, j \in J$ if $k = j$ or $k = js$; otherwise $e_1(j)$ and $e_1(k)$ have different endpoints. Moreover, for $j \neq js$ we have $e_1(j) \neq e_1(js)$. In fact, in this case the images of the classical fundamental region $(-\bar{\rho}, i\infty, \rho)$ and its s-translation on $X_G(\mathbf{C})$ are disjoint.

2-cells. They are of two types: two-sided and triangular.

The two-sided $e_2'(j)$ are indexed by the classes $j \in J$ for which $jt = j$: by definition, the cell $e_2'(j)$ is $\phi(gE')$, where $g \in \Gamma$ is any representative of the class j. (The interior of E' maps to $e_2'(j)$, and the half-median $g\langle\rho, i\rangle$ becomes a cut from the center to the boundary of this cell.) We orient $e_2'(j)$ in the usual way. Then

$$\partial e_2'(j) = e_1(j) - e_1(js). \tag{8}$$

In fact, $\partial e_2'(j)$ consists of the images of the paths $\langle g(i\infty), g(i)\rangle$ and $\langle g(1+i), g(i\infty)\rangle$, where g is a representative of j. According to (7), the first of them is $e_1(j)$, while the second is equal to the image of

$$\langle gt^2(1+i), gt^2(i\infty)\rangle = \langle g(i), g(0)\rangle = \langle gs(i), gs(i\infty)\rangle,$$

i. e. $-e_1(js)$. Obviously $e_2'(j) \neq e_2'(k)$, if $j \neq k$.

The family of triangles $e_2''(j)$ is indexed by the classes $j \in J$ for which $jt \neq j$. By definition, the cell $e_2''(j)$ is $\phi(gE'')$, where $g \in \Gamma$ is any representative of the class j. (This is the cell: $E'' = E' \cup tE' \cup t^2E'$, and all the classes j, jt and jt^2 are distinct.) In the usual orientation induced by the complex structure, we have

$$\partial e_2''(j) = \sum_{a=0}^{2} (e_1(jt^a) - e_1(jt^a s)) \tag{9}$$

(this follows from the analogous formula for the boundary of E'' on $\bar{H}$, which the reader can easily verify). Obviously $e_2''(j) = e_2''(k) \Leftrightarrow j = kt^a$ for some a.

We easily see that L is a complex of the space $X_G(\mathbf{C})$.

c) *Conclusion of the proof of Theorem* 1.9. Following the plan announced at the beginning of the proof, we construct the groups C_1, Z_1 and B_1 of 1-chains, 1-cycles, and 1-boundaries of the complex L, and we define the imbedding $C \to C_1$ as follows: the G-chain (j) corresponds to the L-chain $e_1(js) - e_1(j)$. We easily see that this definition is correct and commutes with the boundary homomorphism (the group of linear combinations of parabolic points is naturally imbedded in the group of 0-chains of L).

We show that the kernel of this homomorphism $C \to C_1$ is trivial. We consider a nonzero G-chain $\Sigma n_j(j)$. Using the relations $(j) + (js) = 0$ and $(j) = 0$ for $j = js$, we may assume this expression normalized so that $n_j n_{js} = 0$ for all j. This G-chain corresponds to the L-chain $\Sigma n_j(e_1(js) - e_1(j))$. If $n_j \neq 0$, then $j \neq js$, and hence, as noted above, $e_1(j) \neq e_1(js)$. In addition, if $n_j n_k \neq 0$, then $j \neq k, ks$, so that all the simplices $e_1(j)$, $e_1(js)$, $e_1(k)$ and $e_1(ks)$ are distinct. It hence follows that $\Sigma n_j(e_1(js) - e_1(j)) \neq 0$.

We now assume that $Z \subset Z_1$ using the above imbedding. Then $(j) \bmod B_1(L) = \xi(j)$, because the chain $e_1(js) - e_1(j)$ belongs to the homology class $\{g(0), g(i\infty)\}$ by (7), where $g \in \Gamma$ is any representative of the class j. It hence follows by linearity that $z \bmod B_1(L) = \xi(z)$ for all $z \in Z$.

Finally, it is clear from (8) and (9) that all the generators of $B_1(L)$—the boundaries of 2-cells—belong to $B \subset Z$ and have the form $-(j)$ for $j = jt$ and $-(j) - (jt) - (jt^2)$ for $j \neq jt$. Hence $Z \cap B_1(L) = B$.

This completes the proof of the theorem.

Remarks. a) The parabolic complex $K(G)$ constructed in 1.8 b) has the same 1-homology as L, but is more economic than L; of the 0-cells of L only the parabolic points are left, since a pair of 1-cells of L with a common i-elliptic vertex corresponds to a single 1-cell in $K(G)$.

b) The construction of the G-complex in 1.8 a) is formally applicable to any subgroup $G \subset \Gamma$, for example to the unit subgroup. Taking into account the possible interest in studying the limits $\varprojlim H_1(X_G(\mathbf{C}))$ and $\varinjlim H^1(X_G(\mathbf{C}))$ over systems of subgroups $(G_i) \subset \Gamma$, we mention the following algebraic situation: in the case $G = \{e\}$, the system of equations (3) admits an explicit parametric solution. In order to construct it, we recall that Γ is the free product of its subgroups $\mathbf{Z}_2$ and $\mathbf{Z}_3$, which are generated by s and t, respectively. Consequently any element of Γ can be uniquely represented as a word $es^{\alpha_0}t^{\beta_0}\dots s^{\alpha_n}t^{\beta_n}$, where $\alpha_i = 0$ or 1 and $\beta_i = 0$, 1 or 2; in addition, α_i and β_i can only be zero at the ends of a word.

By **t-words** we mean the word et^2, and also all words with $\beta_n = 1$; by **t^2-words** we mean all words with $\beta_n = 2$, except for et^2; by **s-words** we mean all words with $\beta_n = 0$ and $\alpha_n = 1$. Every t^2-word can be uniquely represented in the form $g(st^2)^m$, where $m \geq 0$ and g is a t-word. Every s-word, except for es, can be uniquely represented in the form $g(st^2)^m s$, where $m \geq 0$ and g is a t-word.

We introduce a family of independent variables $U(g)$ indexed by all t-words g of the group Γ.

1.10. Proposition. *The infinite system of equations* (3) *in the unknowns* $\xi(g)$, $g \in \Gamma$, *has the following general solution*:

$$\xi(e) = -U(t) - U(t^2), \quad \xi(s) = U(t) + U(t^2),$$

$$\xi(st^2) = -U(t) - U(t^2) - U(st), \quad \xi(h) = U(h),$$

$$\xi(h(st^2)^m) = \sum_{i=0}^{m-1} (-1)^{m-i} U(h(st^2)^i st) + (-1)^m U(h),$$

$$\xi(h(st^2)^m s) = -\xi(h(st^2)^m)$$

for any t-word h.

Proof. The relations $\xi(gs) = -\xi(g)$ and $\xi(gt^2) = -\xi(gt) - \xi(g)$ allow us inductively to express all the ξ indexed by s-words and t^2-words in terms of the ξ indexed by t-words. It can be immediately verified that $\xi(g)$ can be chosen independently for all the t-words g, and that the above formulas are obtained as a result of induction.

(Passing to a nontrivial subgroup $G \subset \Gamma$ naturally imposes additional relations on the parameters $U(g)$.)

§2. The curves X_N

2.1 From now on, we shall work with the subgroups $G \subset \Gamma$ of the form

$$G = \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,\middle|\, c \equiv 0 \bmod N \right\}$$

For the most part we keep the notation of §1, but we write $X_N(\mathbf{C})$, $\{\alpha, \beta\}_N$ etc. instead of $X_{\Gamma_0(N)}(\mathbf{C})$, $\{\alpha, \beta\}_{\Gamma_0(N)}$. Some of the results become trivial or require slight modifications in the case when genus $X_N(\mathbf{C}) = 0$; we usually exclude this case without explicit mention.

The basic purpose of this section is to specialize the results of §1 to the case of the groups $\Gamma_0(N)$ and "explicitly" compute the groups $H_1(X_N(\mathbf{C}), \mathbf{Z})$. However, we begin by describing the special properties of the Riemann surfaces $X_N(\mathbf{C})$ which we need later.

The principal property is the existence of a special smooth projective curve X_N defined over $\mathbf{Q}$ for which the space $X_N(\mathbf{C}) = \Gamma_0(N) \backslash \overline{H}$ is canonically identified with the set of $\mathbf{C}$-points of X_N (also $X_N(\mathbf{C})$ in the traditional notation).

We enumerate some features of the $\mathbf{Q}$-structure and the induced $\mathbf{R}$-structure on X_N.

Let $j : H \to C$ be the classical modular invariant; this is a holomorphic function on H; we define j_N by the condition $j_N(z) = j(Nz)$. Let $\mathbf{Q}(j, j_N)$ be the field of rational functions generated by j and j_N. It has transcendence degree 1, and $\mathbf{Q}$ is algebraically closed in it. The curve X_N is a smooth projective model of this field.

We further set $Y_N = \operatorname{Spec} \mathbf{Q}[j, j_N]$; this is an affine model of the field. The map $H \to Y_N(\mathbf{C}) : z \rightsquigarrow (j(z), j(Nz))$ extends to a map $\phi : \overline{H} \to X_N(\mathbf{C})$ which, in turn, induces an isomorphism $\Gamma_0(N) \backslash \overline{H} \xrightarrow{\sim} X_N(\mathbf{C})$.

Let $f \in \mathbf{C}(j, j_N)$ be a rational function on $X_N \otimes \mathbf{C}$. Its lifting $\phi^*(f)$ to H expands in a Fourier series $\sum a_n e^{2\pi i n z}$ with a finite number of coefficients $a_n \neq 0$ for $n < 0$. This function is defined over $\mathbf{Q}$, i. e. it belongs to $\mathbf{Q}(j, j_N)$, if and only if $a_n \in \mathbf{Q}$ for all n. Analogously, the differential on $X_N \otimes \mathbf{C}$ with Fourier expansion on H

$$\sum b_n e^{2\pi i (n-1) z} d(e^{2\pi i z}) = 2\pi i \sum b_n e^{2\pi i n z}\, dz$$

is defined over $\mathbf{Q}$ if and only if $b_n \in \mathbf{Q}$ for all n.

The local ring of the point $\phi(i\infty)$ consists of all functions with Fourier coefficients $a_n = 0$ for $n < 0$, so that, algebraically, $e^{2\pi i z}$ is a preferred formal parameter of this ring in the $\mathbf{Q}$-structure. In particular, $f(\phi(i\infty)) = \phi^*(f)(i\infty)) = a_0$. Hence the values at the point $\phi(i\infty)$ of all functions defined over $\mathbf{Q}$ belong to $\mathbf{Q}$. This means that $\phi(i\infty) \in X_N(\mathbf{Q})$.

The map $z \rightsquigarrow -1/Nz$ belongs to the normalizer of the group $\Gamma_0(N)$, and hence induces an involution on $\Gamma_0(N) \backslash H$. We easily see that this involution interchanges j and j_N, and thus comes from the canonical involution of the curve X_N over $\mathbf{Q}$. This involution takes $\phi(i\infty)$ to $\phi(0)$; hence also $\phi(0) \in X_N(\mathbf{Q})$.

The parabolic points on $X_N(\mathbf{C})$ other than $\phi_N(0)$ and $\phi_N(i\infty)$ do not necessarily belong to $X_N(\mathbf{Q})$ (or even $X_N(\mathbf{R})$).

In fact, complex conjugation acts naturally on $X_N(\mathbf{C})$. Denoting this action by a bar, we have

$$\overline{\varphi(z)} = \varphi(-\bar{z}).$$

In other words, reflection of H relative to the imaginary axis becomes complex conjugation on $X_N(\mathbf{C})$. This follows from the formula $e^{\overline{2\pi i z}} = e^{-2\pi i \bar{z}}$ and from the fact that $e^{2\pi i z}$, as an analytic local parameter, is defined over $\mathbf{R}$. Hence to construct a non-real parabolic point it suffices to find a rational number $\alpha \in \mathbf{Q}$ such that $-\alpha \notin \Gamma_0(N)\alpha$. Such numbers always exist if N is divisible by the square of a prime number ≥ 3, as is clear from the classical description given below of parabolic points.

Parabolic points. The parabolic points of $X_N(\mathbf{C})$ are in one-to-one correspondence with the classes $\Gamma_0(N) \backslash \mathbf{Q} \cup (i\infty)$. In order to describe them we introduce the set $\Pi(N)$, which consists of pairs of the form $[\delta; a \bmod (\delta, N\delta^{-1})]$. Here δ runs through all positive divisors of N, and the second coordinate of the pair runs through any invertible class of residues modulo the greatest common divisor of δ and $N\delta^{-1}$. If $(\delta, N\delta^{-1}) = 1$ we sometimes put simply 1 in place of the second coordinate.

2.2. Proposition. *Let $\delta \mid N$, $u, v \in \mathbf{Z}$; $(u, v\delta) = (v, N\delta)^{-1} = 1$. The map $\mathbf{Q} \cup (i\infty) \to \Pi(N)$ of the form*

$$\frac{u}{v\delta} \rightsquigarrow [\delta; uv \bmod (\delta, N\delta^{-1})], \qquad i\infty \rightsquigarrow [N; 1]$$

gives an isomorphism of the set of parabolic points on X_N with $\Pi(N)$.

Proof. The substitution

$$\begin{pmatrix} 1 & 1 \\ N & N+1 \end{pmatrix} \in \Gamma_0(N)$$

takes $i\infty$ into $\mathbf{Q}$, so that it suffices to examine the action of $\Gamma_0(N)$ on $\mathbf{Q}$. The substitution $\left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right)$ takes

$$\frac{u}{v\delta} \text{ to } \frac{au + bv\delta}{Ncu + dv\delta}.$$

This fraction is irreducible, and $\delta = (Ncu + dv\delta, N)$, because $(dv, N\delta^{-1}) = 1$. Finally,

$$(au + bv\delta)(N\delta^{-1}cu + dv) \equiv aduv \equiv uv \bmod (\delta, N\delta^{-1}),$$

because $ad - Nbc = 1 \Rightarrow ad \equiv 1 \bmod (\delta, N\delta^{-1})$. Consequently every class $\Gamma_0(N)u/v\delta$ corresponds to the same element in $\Pi(N)$. The induced map $\Gamma_0(N) \backslash \mathbf{Q} \cup (i\infty) \to \Pi(N)$ is obviously surjective; the fractions u/δ, $(u, \delta) = 1$, cover all pairs with first coordinate δ. Finally, this map can either be checked to be injective directly, or else we

can refer to the fact that both sets consist of the same number of elements $\sum_{\delta|N}\phi((\delta, N\delta^{-1}))$. The proposition is proved.

Remark. The stationary subgroup of the point u/δ in $\Gamma_0(N)$ is generated by the element

$$\begin{pmatrix} u & u' \\ \delta & \delta' \end{pmatrix}\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \delta' & -u' \\ -\delta & u \end{pmatrix},$$

where $e = N\delta^{-1}/(\delta, N\delta^{-1})$ and $u\delta' = u'\delta = 1$.

2.3. The set $\Gamma_0(N)\backslash\Gamma$. We define the set $\mathbf{P}^1(\mathbf{Z}/(N))$, "the projective line over $\mathbf{Z}/(N)$" using homogeneous coordinates.

Let $\widetilde{c} = c \bmod N$, $\widetilde{d} = d \bmod N$ be two residue classes mod N which are represented by the relative prime integers c and d. We call two such pairs $(\widetilde{c}, \widetilde{d})$ and $(\widetilde{e}, \widetilde{f})$ **equivalent** if there exists an invertible residue class $u \in (\mathbf{Z}/(N))^*$ such that $(u\widetilde{c}, u\widetilde{d}) = (\widetilde{e}, \widetilde{f})$. We designate the equivalence class of the pair $(\widetilde{c}, \widetilde{d})$ by the symbol $\widetilde{c} : \widetilde{d}$. By definition, the set of these classes is $\mathbf{P}^1(\mathbf{Z}/(N))$.

The group Γ acts on the right on $\mathbf{P}^1(\mathbf{Z}/(N))$ by the formula

$$(\tilde{e}:\tilde{f})\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (\tilde{a}\tilde{e} + \tilde{c}\tilde{f} : \tilde{b}\tilde{e} + \tilde{d}\tilde{f}).$$

2.4. **Proposition.** *The map $\Gamma \to \mathbf{P}^1(\mathbf{Z}/(N))$, which associates the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to the point $\widetilde{c} : \widetilde{d}$ is constant on the cosets $\Gamma_0(N)g$ and induces an isomorphism of right Γ-sets*

$$\Gamma_0(N)\backslash\Gamma \xrightarrow{\sim} \mathbf{P}^1(\mathbf{Z}/(N)).$$

Proof. We immediately verify that the map

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightsquigarrow \tilde{c} : \tilde{d}$$

is constant on right cosets and commutes with the action of Γ. In addition, the group Γ acts transitively on both sets $\Gamma_0(N)\backslash\Gamma$ and $\mathbf{P}^1(\mathbf{Z}/(N))$, the unit class goes to the point $(\widetilde{0} : \widetilde{1})$, and the stationary subgroups of these two elements coincide: they equal $\Gamma_0(N)$. This completes the proof. □

From now on, we shall often identify $\Gamma_0(N)\backslash\Gamma$ with $\mathbf{P}^1(\mathbf{Z}/(N))$ by means of the above isomorphism. We translate the structures in §1 connected with $\Gamma_0(N)\backslash\Gamma$ to the language of $\mathbf{P}^1(\mathbf{Z}/(N))$. See 1.5 for the definition of the map ξ: we recall that

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad t = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

2.5. **Corollary.** a) *The function $\xi : \mathbf{P}^1(\mathbf{Z}/(N)) \to H_1(X_N(\mathbf{C}), \mathbf{R})$ has the form*

$$\xi(\tilde{c}:\tilde{d}) = \left\{\frac{b}{d}, \frac{a}{c}\right\}_N, \tag{10}$$

where a, b, c, d are any integers with the conditions $ad - bc = 1$, $\widetilde{c} = c \bmod N$, $\widetilde{d} = d \bmod N$ (by definition, $a/0 = i\infty$).

b) *The action of the elements s and t on $\mathbf{P}^1(\mathbf{Z}/(N))$ is described by the formulas*

$$(\tilde{c}:\tilde{d})s = -\tilde{d}:\tilde{c}, \quad (\tilde{c}:\tilde{d})t = (\tilde{c}-\tilde{d}):\tilde{c}. \tag{11}$$

c) *Complex conjugation (see the end of 2.1) acts on the distinguished classes $\xi(\widetilde{c} : \widetilde{d})$ by the formulas*

$$\overline{\xi(\tilde{c}:\tilde{d})} = -\xi(\tilde{d}:\tilde{c}). \tag{12}$$

All these facts are verified directly from the definitions.

In 1.8 we define the "boundary" of any element in $\Gamma_0(N)\backslash\Gamma$: this is an element of the free abelian group generated by the parabolic points of $X_N(\mathbf{C})$. Identifying the set of parabolic points with $\Pi(N)$ as in 2.2, we describe the boundary map:

2.6. **Corollary.** *The boundary of the "simplex" $\widetilde{c} : \widetilde{d}$ equals*

$$\partial(\tilde{c}:\tilde{d}) = \left[\delta_1; \frac{c}{\delta_1}d^{-1} \bmod (\delta_1, N\delta_1^{-1})\right] - \left[\delta_2; -c^{-1}\frac{d}{\delta_2} \bmod (\delta_2, N\delta_2^{-1})\right], \tag{13}$$

where $\delta_1 = (c, N)$, $\delta_2 = (d, N)$.

Proof. It is clear from (10) and the definition of the boundary that the boundary is equal to the difference between the classes $\Gamma_0(N)a/c$ and $\Gamma_0(N)b/d$. By Proposition 2.2, the point a/c corresponds to the pair $[\delta_1; a(c/\delta_1) \bmod (\delta_1, N\delta_1^{-1})]$, and $ad - bc = 1$, so that $ad \equiv 1 \bmod (\delta_1, N\delta_1^{-1})$ and $a \equiv d^{-1}$. The second pair is computed analogously, and this proves the corollary.

2.7. **Theorem.** a) *Construct the maximal torsion-free abelian group generated by the symbols $(\widetilde{c} : \widetilde{d})$, one for each point $\widetilde{c} : \widetilde{d} \in \mathbf{P}^1(\mathbf{Z}/(N))$, with the relations*

$$(\tilde{c}:\tilde{d}) + (-\tilde{d}:\tilde{c}) = 0, \tag{14}$$

$$(c:\tilde{d}) + ((\tilde{c}-\tilde{d}):\tilde{c}) + (-\tilde{d}:(\tilde{c}-\tilde{d})) = 0. \tag{15}$$

Further, let $H(N)$ designate the subgroup in it which is the kernel of the boundary homomorphsim (13). Then the map $\xi : (\widetilde{c} : \widetilde{d}) \rightsquigarrow \{b/d, a/c\}_N$, as in (10), induces an isomorphism

$$\xi : H(N) \xrightarrow{\sim} H_1(X_N(\mathbf{C}), \mathbf{Z}).$$

b) *Let*

$$\frac{b}{a} = \frac{b_n}{a_n}, \frac{b_{n-1}}{a_{n-1}}, \ldots, \frac{b_1}{a_1}, \frac{b_0}{a_0} = \frac{b_0}{1}$$

be the successive convergents of the rational number $b/a > 0$. *Then*

$$\left\{0, \frac{b}{a}\right\}_N = \sum_{k=1}^{n} \xi((-1)^{k-1}\tilde{a}_k : \tilde{a}_{k-1}). \tag{16}$$

2.8. **Special case.** Let $N = p$, a prime number. In this case there are two parabolic points $[1; 1]$ and $[p; 1]$ in the notation of 2.2. The points of $\mathbf{P}^1(\mathbf{Z}/(p))$ have the form $\tilde{c} : 1$ or $\tilde{1} : \tilde{0}$. The simplex in $K(\Gamma_0(N))$ corresponding to the pair $\tilde{0} : \tilde{1}$ and $\tilde{1} : \tilde{0}$, joins $[1; 1]$ and $[p; 1]$; all the other simplices of the parabolic complex are loops which begin and end at $[1; 1]$. Hence, introducing the affine coordinate system $\tilde{c} : \tilde{1} = \tilde{c}$, $\tilde{1} : \tilde{0} = \infty$, in $\mathbf{P}^1(\mathbf{Z}/(p))$, we find that the map $\xi : \mathbf{Z}/(p) \cup (\infty) \to H_1(X_p(\mathbf{C}), \mathbf{Z})$, whose definition is provisionally completed by the conditions $\xi(0) = \xi(\infty) = 0$, is the ***universal function*** satisfying the functional equations:

$$\left.\begin{aligned} \xi(\tilde{c}) + \xi(-\tilde{c}^{-1}) &= 0, \\ \xi(\tilde{c}) + \xi(1 - \tilde{c}^{-1}) + \xi\left(\frac{1}{1-\tilde{c}}\right) &= 0, \\ \xi(0) = \xi(\infty) &= 0. \end{aligned}\right\} \tag{17}$$

(Universality holds in the class of such functions with values in torsion-free abelian groups.) We note that $\xi(\tilde{c}) = \{0, 1/c\}$ by (10) if $\tilde{c} \neq 0$.

§3. Arguments of parabolic points

In this section we give explicit expressions for the integrals $\int_{\{\alpha,\beta\}} \omega$ in the case when the class $\{\alpha, \beta\}$ is not necessarily integral. To formulate and prove our results, we need some elementary facts about Hecke operators. We give them in the limited context in which we need them.

3.1. **Hecke operators and parabolic forms.** Let $a, b, c, d \in \mathbf{R}$, $ad - bc > 0$. For any function Φ on H we set

$$\Phi\left|\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \Phi\left(\frac{az+b}{cz+d}\right)\frac{d}{dz}\left(\frac{az+b}{cz+d}\right).\right.$$

This defines a right action of the group $PL(2, \mathbf{R})$ on the space of functions on H. This action extends by linearity to the entire group ring:

$$\Phi\left|\left(\sum a_i g_i\right) = \sum a_i \Phi\right| g_i, \qquad a_i \in \mathbf{C}, \quad g_i \in PL.$$

The following special elements of this ring are called **Hecke operators:**

$$T_m = \sum_{\substack{d|m \\ b=0,\ldots,d-1}} \begin{pmatrix} md^{-1} & b \\ 0 & d \end{pmatrix}, \quad m \in \mathbf{Z}, \quad m > 0. \tag{18}$$

They satisfy the following relations on the space of functions on H with period 1: $T_m T_n = T_{mn}$ for $(m, n) = 1$, and $T_p T_{p^r} = T_{p^{r+1}} + pT_{p^{r-1}}$.

Let $G \subset \Gamma$ be a subgroup of finite index. A function $\Phi(z)$ on H is called a **G-parabolic form** if there exists a differential of the first kind ω on the surface $X_G(\mathbf{C})$ such that $\phi^*(\omega) = \Phi(z)dz$, where $\phi : H \to X_G(\mathbf{C})$ is the canonical projection.

3.2. **Proposition.** *If* $(m, N) = 1$, *then* T_m *takes the space of* $\Gamma_0(N)$*-parabolic forms* P_N *into itself.*

Thus the operators $\{T_m \mid (m, N) = 1\}$ generate a commutative operator alegbra on the space of $\Gamma_0(N)$-parabolic forms P_N. They are Hermitian relative to the Peterson scalar product. It is also worthwhile to keep in mind that the $\mathbf{Q}$-subspace $\phi_N^*(H^0(X_N, \Omega))$ is invariant relative to T_m: this is clear either from the direct description of the action of T_m on the Fourier coefficients (Atkin and Lehner [1], formula (3.1)), or else from the invariant definition of T_m using correspondences on $X_N \times X_N$. In particular, P_N has a basis of eigenfunctions for the Hecke algebra all of whose Fourier coefficients are algebraic.

The theory of Hecke operators with indices not prime to N is more complicated. We shall only indicate the operators U_p, p prime:

$$U_p = \sum_{b=1}^{p-1} \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} = T_p - \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}. \tag{19}$$

In the article by Atkin and Lehner [1] it is shown that $U_p(P_N) \subset P_N$ if $p \mid N$, and that the U_p commute with all the T_m, $p \nmid m$.

We shall henceforth assume N fixed; $\{\alpha, \beta\}_N$ denotes the element in $H_1(X_N(\mathbf{C}), \mathbf{R})$, defined in 1.2. In addition to the general properties of the classes $\{\alpha, \beta\}$ we note that $\{\alpha + m, \beta + n\}_N = \{\alpha, \beta\}_N$ for all $m, n \in \mathbf{Z}$. This follows because the parabolic element $\left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$ belongs to $\Gamma_0(N)$ if we use Proposition 1.4: the class $\{\alpha, \alpha + m\}_N = \{\alpha, \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)\alpha\}$ is equal to zero as the image of a parabolic element under the homomorphism $\Gamma_0(N) \to H_1(X_N(\mathbf{C}), \mathbf{Z})$.

3.3. **Theorem.** *Let the* $\Gamma_0(N)$*-parabolic form* $\Phi = \phi^*(\omega)/dz$ *be an eigenfunction for the Hecke operator* T_m, $(m, N) = 1$: $\Phi | T_m = c_m \Phi$. *Then*

$$\left(\sum_{d|m} d - c_m\right)\int_0^{i\infty} \Phi\, dz = \sum_{\substack{d|m \\ b \bmod d}} \int_{\{0, \frac{b}{d}\}} \omega. \tag{20}$$

Comment. Since $(m, N) = 1$, we have $b/d \in \Gamma_0(N)(0)$ for all $d|m$ by Proposition 2.2. Hence $\{0, b/d\} \in H_1(X_N(\mathbf{C}), \mathbf{Z})$, so that the right side of (20) consists of integral linear combinations of the fundamental periods of the differential ω with respect to some integral homology basis. The coefficients of these linear combinations are computed using the theory in §§1 and 2 (see, in particular, formula (16)). In addition,

$\Sigma_{d|m} d - c_m \neq 0$ for sufficiently large m by the well-known growth estimates for the coefficients of parabolic forms.

Thus we may assume that the expressions (20) give us an explicit form for the arguments of the point $\phi(0)$ under the Abel-Jacobi map of the curve $X_N(\mathbf{C})$ (with origin $\phi(i\infty)$) relative to the basis of differentials of the first kind for which the corresponding parabolic forms are eigenfunctions for the Hecke operators.

Another point of view on formulas (20) emerges if we consider m variable and fix Φ. Then, under the assumption $\int_0^{i\infty} \Phi dz \neq 0$, (20) and (16) give expressions for the eigenvalues c_m of the operators T_m on Φ in terms of the expansion in continued fractions of all numbers of the form b/d, $d|m$, $0 \leq b \leq d-1$.

Both points of view lead to interesting number-theoretic results, which we shall examine in greater detail below in §§6 and 7.

3.4. Proof of Theorem 3.3. For any element $g \in PL(2, \mathbf{R})$ and function Φ on H we have

$$\int_\alpha^\beta (\Phi|g)dz = \int_\alpha^\beta \Phi(gz)d(gz) = \int_{g(\alpha)}^{g(\beta)} \Phi(z)dz.$$

Using this, we obtain the following formulas for the action of the Hecke operators (18):

$$\int_\alpha^\beta (\Phi|T_m)dz = \sum_{d|m} \sum_{b=0}^{d-1} \int_{\frac{m}{d^2}\alpha+\frac{b}{d}}^{\frac{m}{d^2}\beta+\frac{b}{d}} \Phi\, dz. \qquad (21)$$

We susbtitute $\alpha = 0$, $\beta = i\infty$ here and use the fact that $\Phi|T_m = c_m\Phi$:

$$c_m \int_0^{i\infty} \Phi\, dz = \sum_{d|m} \sum_{b=0}^{d-1} \left(\int_{\frac{b}{d}}^{0} + \int_0^{i\infty} \right) \Phi\, dz,$$

so that

$$\left(\sum_{d|m} d - c_m \right) \int_0^{i\infty} \Phi\, dz = \sum_{d|m} \sum_{b=0}^{d-1} \int_0^{\frac{b}{d}} \Phi\, dz = \sum_{\substack{d|m \\ b \bmod d}} \int_{\left\{0, \frac{b}{d}\right\}} \omega,$$

as was to be proved.

More generally, this same device of "closing the path of integration" allows us to compute the arguments of any parabolic point.

3.5. Theorem. *Under the conditions of Theorem 3.3, let $\alpha \in \mathbf{Q}$. Then*

$$\left(\sum_{d|m} d - c_m \right) \int_\alpha^{i\beta} \Phi\, dz = \sum_{\substack{d|m \\ b \bmod d}} \int_{\left\{\alpha, \frac{m}{d^2}\alpha+\frac{b}{d}\right\}_N} \omega. \qquad (22)$$

For every N there exist infinitely many values of m, $(m, N) = 1$, such that $\{\alpha, m\alpha/d^2 + b/d\}_N \in H_1(X_N(\mathbf{C}), \mathbf{Z})$ for all b. Hence if Φ is an eigenfunction for all the Hecke operators T_m, $(m, N) = 1$, then m can be chosen so that the right side of (22) contains the periods of ω over integral homology classes.

Proof. (22) follows immediately from (21), as in the previous theorem.

To prove the second assertion, we set $\alpha = u/v\delta$, where $\delta|N$ and $(u, v\delta) = (v, N\delta^{-1}) = 1$, and take for m any prime number l with the conditions $l \nmid N$ and $l \equiv 1 \bmod (\delta, N\delta^{-1})$.

According to 1.3 c), integrality of the class $\{\alpha, l\alpha/d^2 + b/d\}$ is equivalent to the inclusion $l\alpha/d^2 + b/d \in \Gamma_0(N)\alpha$. Taking into account that $d = 1$ or l and using Proposition 2.2, we conclude that we must verify that, in the irreducible representation of any of the fractions

$$l\alpha = \frac{lu}{v\delta}, \qquad \frac{1}{l}\alpha + \frac{b}{l} = \frac{u + bv\delta}{lv\delta}$$

the product (numerator) × (denominator) δ^{-1} is congruent to $uv \bmod (\delta, N\delta^{-1})$. We must consider separately the cases when this fraction is reducible (then the greatest common divisor of the numerator and denominator equals l) and when it is irreducible. In both cases the required congruence follows from $l \equiv 1 \bmod (\delta, N\delta^{-1})$.

We note that all $l \nmid N$ are suitable for square-free N, and that all $l \equiv 1 \bmod N$.

The theorem is proved.

The case when the eigenvalues of T_m on Φ are rational is especially interesting: it then follows from (21) and (22) that the corresponding arguments of all the parabolic points of $X_N(\mathbf{C})$ are rational linear combinations of the fundamental periods. Here is the algebraic-geometric formulation of this fact:

3.6. Corollary. *Let $\psi: X_N \to X$ be a morphism of curves over $\mathbf{Q}$, and let the space $\psi^*(H^0(X, \Omega_X))$ be invariant relative to the Hecke operators T_m, $(m, N) = 1$, and have a basis of eigenvectors for T_m with rational eigenvalues at least for some sufficiently large m. Then for any two parabolic points $x, y \in X_N(\mathbf{C})$ the divisor class $\psi(x) - \psi(y)$ on $X \otimes \mathbf{C}$ has finite order.* (1)

3.7. Special case. Let $\psi: X_N \to X$ be a morphism of X_N onto an elliptic curve X over $\mathbf{Q}$. We call this morphism a *Weil uniformization* for X (in the weak sense) if $\psi \circ \phi(i\infty)$ is zero on X, and the one-dimensional subspace $(\psi \circ \phi)^* H^0(X, \Omega^1)$ is invariant relative to the operators T_m, $(m, N) = 1$, with rational eigenvalues.

The following assertions are easily deduced from the above:

a) *If the curve X has a weak uniformization $\psi: X_N \to X$, then there exists another weak uniformization for which the images of all the parabolic points coincide with zero on X.*

In fact, it suffices to take the composition of ψ with the multiplication $X \xrightarrow{n} X$ for suitable n and then use 3.6.

---

(1) *Added in proof*. V. Drinfel'd has shown me that Theorem 3.5 easily implies that such classes even have finite order on X_N.

b) *Let* $\psi : X_N \to X$ *be a weak uniformization, let* ω *be a differential of the first kind on* X, *and let* $\Phi(z)dz$ *be its preimage on* H. *Further, let* γ^+ *be a generator of the subgroup of real (invariant relative to conjugation) classes in* $H_1(X_N(\mathbf{C}), \mathbf{Z})$, $W^+ = \int_{\gamma^+} \omega$, *and let* t *be the maximal period of a point of finite order in* $X(\mathbf{Q})$. *Then*

$$\int_0^{i\infty} \Phi\, dz = \frac{s}{t} W^+, \quad s \in \mathbf{Z}. \tag{23}$$

In fact,

$$\int_0^{i\infty} \Phi\, dz = \int_{\psi\circ\varphi(0)}^{\psi\circ\varphi(i\infty)} \omega.$$

The second integral is taken over the image of the imaginary axis, which lies entirely in $X(\mathbf{R})$ and joins the point of finite order $\psi \circ \phi(0) \in X(\mathbf{Q})$ with zero $\psi \circ \phi(i\infty) \in X(\mathbf{Q})$. This implies the assertion.

3.8. Finally, we give a somewhat strengthened result from the second chapter of [9], where the device of closing the path was first introduced in a somewhat different context. Here we are not required to apply the Hecke operators, but, on the other hand, the integrand contains parabolic forms of a special type arising in the Hecke-Weil theory and in the study of zeta-functions of modular curves over abelian extensions of the field $\mathbf{Q}$.

Suppose that $\Phi = \sum a_n e^{2\pi i n z}$ is a parabolic form relative to $\Gamma_0(N)$, $m > 1$, $m \in \mathbf{Z}$; let $\chi : \mathbf{Z} \to \mathbf{C}$ be a primitive Dirichlet character mod m. We set

$$g(\chi) = \sum_{b \bmod m} \chi(b) e^{2\pi i \frac{b}{m}} \text{ (Gaussin sum) and } \Phi_\chi = \sum_{n=1}^{\infty} \chi(n) a_n e^{2\pi i n z};$$

finally, let $\Phi dz = \phi^*(\omega)$.

3.9. Theorem. *Let* $\delta = (m, N)$, *and let* $(\delta, N\delta^{-1}) = 1$. *Then*

$$\int_0^{i\infty} \Phi_\chi\, dz = \frac{g(\chi)}{m} \sum_{b \bmod m} \overline{\chi}(b) \int_{\left\{-\frac{b}{m}, \frac{1}{\delta}\right\}_N} \omega \tag{24}$$

and $\{-b/m, 1/\delta\}_N \in H_1(X_N(\mathbf{C}), \mathbf{Z})$ *for all* $b \bmod m$, $\overline{\chi}(b) \neq 0$.

Proof. In fact, by a well-known lemma (see Weil [16], Ogg [12] or Manin [9]),

$$\Phi_\chi(z) = \frac{g(\chi)}{m} \sum_{b \bmod m} \overline{\chi}(-b) \Phi\left(z + \frac{b}{m}\right),$$

so that

$$\int_0^{i\infty} \Phi_\chi\, dz = \frac{g(\chi)}{m} \sum_{b \bmod m} \overline{\chi}(b) \int_{-\frac{b}{m}}^{i\infty} \Phi(z)\, dz = \frac{g(\chi)}{m} \sum_{b \bmod m} \overline{\chi}(b) \int_{-\frac{b}{m}}^{a} \Phi(z)\, dz$$

for any $a \in \overline{H}$, because $\sum_{b \bmod m} \overline{\chi}(b) = 0$ since the character χ is primitive.

In particular, if $(\delta, N\delta^{-1}) = 1$, then for any b with $\overline{\chi}(b) \neq 0$, i. e. $(b, m) = 1$, we have $b/m \in \Gamma_0(N)\delta^{-1}$ by Proposition 2.2. Hence $\{b/m, 1/\delta\}_N \in H_1(X_N(\mathbf{C}), \mathbf{Z})$, which explains the choice $a = 1/\delta$. The theorem is proved.

In [9] we examine the case $\delta = 1$.

§4. L-series at the center of the critical strip

4.1. Let ω be a differential of the first kind on $X_N \otimes \mathbf{C}$. As above, we set $\Phi_\omega = \phi_N^*(\omega)/dz = -2\pi i \sum a_n e^{2\pi i n z}$ and define the Dirichlet series L_ω by the formula

$$L_\omega(s) = \sum_{n=1}^{\infty} a_n n^{-s}. \tag{25}$$

It is well known that $L_\omega(s)$ has an analytic continuation onto the entire plane given by the formula

$$L_\omega(s) = -\frac{1}{2\pi i} \frac{(2\pi)^s}{\Gamma(s)} \int_0^{\infty} \Phi_\omega(iy)\, y^{s-1}\, dy$$

and, in particular,

$$L_\omega(1) = \int_0^{i\infty} \Phi_\omega(z)\, dz = \int_{\{0, i\infty\}_N} \omega \tag{26}$$

(see, for example, Manin [9], Lemma 9.2).

This allows us to interpret the fundamental results of the last section in terms of explicit formulas for the values of the series L_ω at the point $s = 1$, the center of their critical strip; and we gather these formulas together here for more convenient reference.

4.2. Theorem. a) *Under the conditions of* 3.1, *suppose that* Φ_ω *is an eigen-form for the Hecke operator* T_m, $(m, N) = 1$, *and that* $a_1 = 1$. *Then*

$$\left(\sum_{d/m} d - a_m\right) L_\omega(1) = \sum_{\substack{d/m \\ b \bmod d}} \int_{\left\{0, \frac{b}{d}\right\}_N} \omega. \tag{27}$$

b) *Under the conditions of* 3.1, *let* χ *be a primitive character* mod $m > 1$, *let* $g(\chi)$ *be the Gaussian sum, and let* $L_{\omega,\chi}(s) = \sum_{n=1}^{\infty} \chi(n) a_n n^{-s}$. *If* $(m, N) = \delta$, $(\delta, N\delta^{-1}) = 1$, *then*

$$L_{\omega,\chi}(1) = \frac{g(\chi)}{m} \sum_{b \bmod m} \overline{\chi}(b) \int_{\left\{-\frac{b}{m}, \frac{1}{\delta}\right\}_N} \omega. \tag{28}$$

Proof. Formula (27) follows from (20) and (26) if we take into account that $\Phi_\omega | T_m = a_m \Phi_\omega$ for $a_1 = 1$. Formula (28) coincides with (24).

4.3. It is interesting to compare formulas (27) and (28) with the Birch–Swinnerton-Dyer conjecture (see [8], [9] and [15]). In the next two sections we do this for Weil uniformized elliptic curves over $\mathbf{Q}$ and for some abelian extensions of $\mathbf{Q}$. Here we shall limit ourselves to a remark on the behavior of the curve X_N itself.

Let

$$\Phi_{\omega(k)} = -2\pi i \sum_{n=1}^{\infty} a_n(k) e^{2\pi i n z}$$

be the family in P_N consisting of the eigenfunctions for the Hecke operators with the proper multiplicities ($k = 1, \cdots$, genus X_N; $a_1(k) = 1$). Then the product $\prod_{k=1}^{\text{genus}} L_{a(k)}(s)$ coincides with the Hasse-Weil series of the curve X_N corresponding to the one-dimensional cohomology of X_N, to within the Euler factors for $p | N$. It appears that the precise form of these exceptional factors is not known: Serre suggests characterizing them in terms of the l-adic representations connected with X_N, but these are not sufficiently well known. On the other hand, Atkin and Lehner [1] introduced the useful notions of "new forms" in P_N and the canonical partition of P_N into two terms. The first term is generated by the new forms; there a one-dimensional subspace corresponds to every weight of the Hecke algebra. The second term is generated by the "old forms," which are constructed in a natural way from the new forms in P_d for $d | N$.

A more detailed examination of this construction and its translation in $H_1(X_N(\mathbf{C}), \mathbf{Z})$ (or, rather, $H_1(X_N, \mathbf{Q})$) should allow us to conjecture the correct form of the L-function of the curve X_N and compute the exact value of $L(1)$ using (27).

§5. Weil uniformization

5.1. Let X be an elliptic curve on $\mathbf{Q}$. The following notation will be fixed for the duration of this and the next sections: N is the conductor of X; ω is a Néron differential on X; $L(X, s) = \sum_{n=1}^{\infty} a_n n^{-s}$ is the canonical Dirichlet series connected with X, the fundamental part of the Hasse-Weil zeta-function of this curve, and $L(X \otimes K, s)$ is the analogous series for X over K if $K \supset \mathbf{Q}$ is any finite extension. We emphasize that the Euler factors of L at the points of degeneracy of X are assumed to be normalized in the way that is now generally accepted, as described, for example, in Weil's article [16] and in the author's survey article [9].

5.2. Definition. A ***Weil uniformization*** (**in the strong sense**) of the curve X is a morphism of curves $\psi : X_N \to X$ over $\mathbf{Q}$ with the following properties:

a) $\psi \circ \phi : \overline{H} \to X_N(\mathbf{C}) \to X(\mathbf{C})$ takes $i\infty$ to the zero point of $X(\mathbf{Q})$.

b) $(\psi \circ \phi)^* \omega = \Phi(z) dz = -2\pi i \sum_{n=1}^{\infty} a_n e^{2\pi i n z} dz$, where (a_n) are the coefficients of the Dirichlet series $L(X, s)$.

c) The form $\Phi(z)$ is an eigenfunction of all the Hecke operators T_m (see (18)) for $(m, N) = 1$, of all the operators U_p for the primes $p | N$ (see (19)), and of the standard involution operator $\left(\begin{smallmatrix} 0 & 1 \\ -N & 0 \end{smallmatrix}\right)$ of the curve X_N.

It probably follows from a) and b) that $\Phi(z)$ is a "new form" in the sense of Atkin-Lehner (see [1]). Then properties c) are automatically fulfilled. In any case, conditions a), b) and c) are not independent (see, for example, Cartier [4]).

Weil conjecture. *Any elliptic curve over* $\mathbf{Q}$ *admits a Weil uniformization in the strong sense.*

For discussions of this conjecture, see, in particular, the articles by Weil [16], by the author [9], §10, and by Cartier [4]. In [16] and [9] it is shown that, for curves admitting a Weil uniformization, the L-series over $\mathbf{Q}$ and over any abelian extension of $\mathbf{Q}$ have analytic continuations onto the entire plane, as in §4. In this section we give formulas for the values of L-series at one (the center of their critical strip), and we deduce from them that the uniformization ψ is unique.

5.3. Let the curve X, the differential ω and the strong uniformization ψ be fixed. We introduce two fundamental number-theoretic functions connected with (X, ω, ψ). We let γ^+ and γ^- designate the generators of the groups of real classes and of purely imaginary classes, respectively, in $H_1(X(\mathbf{C}), \mathbf{Z})$ and we set $W^{\pm} = \int_{\gamma^{\pm}} \omega$.

5.4. Definition. The functions $x^{\pm} : \mathbf{Q} \cup (i\infty) \to \mathbf{Q}$ are defined by the equations

$$\psi_* \{-\alpha, 0\}_N \pm \psi_* \{\alpha, 0\}_N = x^{\pm}(\alpha) \gamma^{\pm}$$

(the signs are taken either all plus or all minus).

We recall that $\{\alpha, 0\}_N \in H_1(X_N(\mathbf{C}), \mathbf{R})$. $x^{\pm}(\alpha)$ is rational by the results of 3.6 and 3.7. If the denominator of α is relatively prime to N, then we even have $x^{\pm}(\alpha) \in \mathbf{Z}$. The functions x^+ ans x^- have period 1; x^+ is even, and x^- is odd. We have normalized the signs in a way that is not entirely natural because of a desire to remain compatible with the notation in [9].

Using these functions, we can explicitly distinguish irrationality in the formulas for $L(1)$.

5.5. Theorem. *For all* m, $(m, N) = 1$, *we have*

$$\left(\sum_{d|m} d - a_m\right) L(X, 1) = -\frac{W^+}{2}\left(\sum_{\substack{d|m \\ b \bmod d}} x^+\left(\frac{b}{d}\right)\right). \tag{29}$$

Proof. Formula (29) follows from (27) with $\psi^*(\omega)$ in place of ω, if we take into account that the differential ω is defined over $\mathbf{R}$, so that $L(X, 1) \in \mathbf{R}$ and

$$\overline{\int_{\{0, \frac{b}{d}\}} \psi^*(\omega)} = \int_{\{0, -\frac{b}{d}\}} \psi^*(\omega).$$

Hence the real part of the sum on the right in (27), which is equal to half of its sum with it complex conjugate, has the form

$$\frac{1}{2} \sum_{\substack{d|m \\ b \bmod d}} \int_{\{0, \frac{b}{d}\} + \{0, -\frac{b}{d}\}} \psi^*(\omega) = -\frac{1}{2} \sum_{\substack{d|m \\ b \bmod d}} x^+\left(\frac{b}{d}\right) \int_{\gamma^+} \omega = -\frac{W^+}{2} \sum_{\substack{d|m \\ b \bmod d}} x^+\left(\frac{b}{d}\right),$$

is was to be proved.

To formulate the next result, we consider two abelian extensions $K \subset K'$ of the field $\mathbf{Q}$. Let the discriminants D and D' of these fields be relatively prime to N. Further, let r_1 be the number of real points of the field K, r_2 the number of purely imaginary points, and $r = r_1 + r_2$; let r_1', r_2' and r' have the analogous meaning for K'. We let M designate the set of Dirichlet characters belonging to K' but not to K; let m_χ be the conductor of the charater χ; sign $\chi = +$ if $\chi(-1) = 1$ and $-$ if $\chi(-1) = -1$.

5.6. Theorem. *In the above notation we have*

$$L(X \otimes K', s)/L(X \otimes K, s)|_{s=1}$$

$$= \pm \left|\frac{D}{D'}\right|^{\frac{1}{2}} (W^+)^{r'-r} (W^-)^{r_2'-r_2} \prod_{\chi \in M} \frac{1}{2}\left(\sum_{b \bmod m_\chi} \chi(b)^{\varkappa \operatorname{sign} \varkappa}\left(\frac{b}{m_\chi}\right)\right). \tag{30}$$

Proof. We set $L_\chi(X, s) = \sum_{n=1}^{\infty} \chi(n) a_n n^{-s}$ and use the formula

$$L(X \otimes K, s) = \prod L_\chi(X, s), \tag{31}$$

where χ runs through the Dirichlet characters associated with the field K (here we use the fact that D and N are relatively prime: otherwise the product in the right side of (31) may differ from the canonical Dirichlet series for $X \otimes K$ by a finite number of Euler factors; see [9], Lemma 7.3). Dividing the formulas (31) corresponding to K' and K by one another and substituting in the right side of expression (28), we find

$$L(X \otimes K', s)/L(X \otimes K, s)|_{s=1} = \coprod_{\chi \in M} L_\chi(X, 1)$$

$$= \coprod_{\chi \in M} \frac{g(\chi)}{m_\chi}\left(\sum_{b \bmod m_\chi} \overline{\chi}(b) \int_{\left\{-\frac{b}{m}, 0\right\}} \psi^*(\omega)\right). \tag{32}$$

Further, we know that

$$|g(\chi)| = m_\chi^{\frac{1}{2}} \text{ and } \prod_{\chi \in M} \frac{g(\chi)}{m_\chi} = \pm \left|\frac{D}{D'}\right|^{\frac{1}{2}}$$

by the Hasse-Artin formula. Finally, the inner sum in (32) transforms as in the previous theorem, giving

$$\sum_{b \bmod m_\chi} \overline{\chi}(b) \int_{\left\{-\frac{b}{m}, 0\right\}} \psi^*(\omega) = \frac{\tau^{\operatorname{sign} \chi}}{2} \sum_{b \bmod m_\chi} \overline{\chi}(b) \varkappa^{\operatorname{sign} \chi}\left(\frac{b}{m_\chi}\right). \tag{33}$$

To complete the transisition from (32) to (30), it remains to note that the number of even characters in M equals $r' - r$, and the number of odd characters equals $r_2' - r$. The theorem is proved.

We note that, since the fields K and K' are normal over $\mathbf{Q}$, it follows that only the following three combinations of the numbers r and r' are possible: either $r_2 = r_2' = 0$, or $r_2 = 0$, $r_2' = \frac{1}{2} r'$ or else $r_2 = \frac{1}{2} r$, $r_2' = \frac{1}{2} r'$.

5.7. Theorem. *If a Weil uniformization (more precisely, a pair (X, ω)) exists for the curve X, then it is unique.*

Proof. The values of $L(X, 1)$ and $L_\chi(X, 1)$ are uniquely defined and are characterized by formulas (29) and (33), in which the numbers $x^{\pm}(\alpha)$ can be computed from any uniformization. We consider all characters χ with *prime* conductor $l \nmid 2N$. Then (30) allows us to compute the sum $\sum_{b \bmod l} x^+(b/l)$, and (33) allows us to compute all the sums $\sum_{b \bmod l} \chi(b) x^{\pm}(b/l)$ with nonprincipal characters mod l in terms which do not depend on the choice of uniformization. Consequently the numbers $x^{\pm}(b/l)$ for $l \nmid 2N$ do not depend on the choice of uniformization ψ. These numbers determine the values of the homomorphism of homology groups $\psi_* : H_1(X_N(\mathbf{C}), \mathbf{Z}) \to H_1(X(\mathbf{C}), \mathbf{Z})$ on the homology classes of the form $\{0, b/l\}_N$, as is clear from Definition 5.4. Suppose that these classes generate the entire group $H_1(X_N(\mathbf{C}), \mathbf{Z})$. Then it follows from the above that the homomorphism ψ_* is uniquely determined. But ψ is also determined uniquely from ψ_* if we require, as in 5.2 a), that the distinguished points of the curves X_N and X corresponds to each other. Hence it remains to prove the following fact:

5.8. Lemma. *The homology classes $\{0, b/l\}_N \in H_1(X_N(\mathbf{C}), \mathbf{Z})$ generate the entire homology group when $l \nmid 2N$ runs through the prime numbers and b runs through a complete system of residues* mod l.

Proof. We use a method of Weil [16]. Let $\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0(N)$ be any element. We have

$$\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} * & * \\ * & Ncx + d \end{pmatrix}.$$

By Dirichlet's theorem, x can always be chosen so that the number $Ncx + d$ is a prime $\neq 2$; obviously it does not divide $2N$. Hence $\Gamma_0(N)$ is generated by the elements and by the matrices having a prime $l \nmid 2N$ in the lower right-hand corner.

Setting $\alpha = 0$ in Proposition 1.4, we now immediately obtain the assertion of the lemma, and with it the uniqueness theorem.

Remark. Another variant of the uniqueness theorem (with a completely different proof) is contained in Cartier's report [4].

§ 6. The Birch–Swinnerton-Dyer conjecture and Mazur's theory

We keep the notation of the last section; in particular, X is an elliptic curve over $\mathbf{Q}$, N is its conductor, and $\psi : X_N \to X$ is a Weil uniformization in the strong sense.

In this section we compare formulas (29) and (30) with the Birch–Swinnerton-Dyer conjecture. Its complete formulation in the form convenient for us is given in [9]. Here we limit ourselves to several special cases with which our results may be directly compared.

All of these special cases, along with the conditional results whose proofs use the Birch–Swinnerton-Dyer conjecture and the conditional formulas of this type, are marked

in the text with an asterisk.

6.1. Conditional formula for $L(X, 1)$:

$$L(X,1)=\begin{cases}0, & \text{if rank } X(\mathbf{Q})>0,\\ W^{+}\dfrac{[Ш]}{[\tilde{X}(Q)]^{2}}[\pi_0(X(\mathbf{R}))]\prod\limits_{p/N}[\pi_0(X \bmod p)], & \end{cases} \tag{34}^{*}$$

In this and the other formulas, the following notation is used: $[G]$ is the number of elements in the set G; Ш is the Šafarevič-Tate group of the curve X; $\tilde{X}(\mathbf{Q})$ is the group of $\mathbf{Q}$-points of finite order; $\pi_0(X(\mathbf{R}))$ is the group of connected components of the real points of X; and $\pi_0(X \bmod p)$ is the group of connected components of the closed fiber of the Néron model of the curve X over the point p.

In comparing $(34)^*$ with (23) and (29), the following circumstances deserve mention:

a) The general structure of the formulas is the same: $L(X, 1)$ is the product of W^+ by a rational number. However, in our formula the denominator of this number divides $[\tilde{X}(\mathbf{Q})]$ and even the maximal period of the points of finite order in $X(\mathbf{Q})$. This evidently means that the local factors in $(34)^*$ must strongly cancel with $[\tilde{X}(\mathbf{Q})]^2$. Ligozat [8] computed these factors for all twelve curves X_N of genus 1. According to his computations, the product of the local factors is always exactly equal to $[\tilde{X}(\mathbf{Q})]$, and the hypothetical value of $[Ш]$ equals 1.

b) The condition $L(X, 1) = 0$ expresses a simple topological property of the uniformization map $\psi \circ \phi : H \to X(\mathbf{C})$. This is the property that $\psi \circ \phi$ takes the imaginary semiaxis to a closed path which is homotopic to zero in $X(\mathbf{R})$. In particular, in this case there are branch points of $\psi \circ \phi$ on the imaginary semiaxis, namely the zeros of the form $(\psi \circ \phi)^{*}\omega$. Do they have any relation to the points of infinite order in $X(\mathbf{Q})$ whose existence is predicted by the Birch–Swinnerton-Dyer conjecture?

6.2. Conditional formulas for $L(X \otimes K', s)/L(X \otimes K, s)|_{s=1}$. With the conditions and notation of Theorem 5.6, we further suppose that $X(K') = X(K)$: the group of rational points of X does not increase when going from K to K'. Then the Birch–Swinnerton-Dyer conjecture leads to the following expression (for the details, see [9]):

$$L(X\otimes K',s)/L(X\otimes K,s)|_{s=1}=\left|\frac{D}{D'}\right|^{\frac{1}{2}}(W^{+})^{r'-r}\,|W^{-}|^{r_2-r}\,[\pi_0(X(\mathbf{R}))]^{r'-r}$$
$$\times\frac{\prod\limits_{v'/N}[\pi_0(X \bmod v')]}{\prod\limits_{v/N}[\pi_0(X \bmod v)]}\,\frac{[Ш']}{[Ш]}. \tag{35}^{*}$$

The notation here is similar to that used in $(34)^*$, except that $[Ш]$ denotes the order of the Šafarevič-Tate group of the curve $X \otimes K$ and $[Ш']$ denotes the same for the curve $X \otimes K'$, and so on. In the case when $\operatorname{rk} X(K') > \operatorname{rk} X(K)$, we must have zero on the right in $(35)^*$, while if the index $[X(K') : X(K)]$ is finite, then the right side is multiplied by a rational number, which we do not write out explicitly here.

Comparing (30) and $(35)^*$ again shows a good structural agreement of the formulas and allows us to derive a hypothetical formula for the ratio of the orders of the Šafarevič-Tate groups under the above conditions:

$$\frac{[Ш']}{[Ш]}=\frac{\prod\limits_{v/N}[\pi_0(X \bmod v)]}{[\pi_0(X(R))]^{r'-r}\prod\limits_{v'/N}[\pi_0(X \bmod v')]}\prod_{\chi\in M}\frac{1}{2}\left(\sum_{b \bmod m_\chi}\chi(b)\varepsilon_\chi\operatorname{sign}\chi\left(\frac{b}{m_\chi}\right)\right). \tag{36}^{*}$$

The left side must be the square of a rational number by Cassels' theorem. We can independently prove the following assertion about the right side being a square.

6.3. Proposition. *Let* $\overline{M} = \{\chi \in M \mid \chi \text{ is not real}\}$. *Then*

$$\prod_{\chi\in\overline{M}}\frac{1}{2}\left(\sum_{b \bmod m_\chi}\chi(b)\varepsilon_\chi\operatorname{sign}\chi\left(\frac{b}{m_\chi}\right)\right)=\Delta S^{2}, \tag{37}$$

where Δ *and* S *are integers and* Δ *consists only of ramified primes in the value field of the characters* $\chi \in \overline{M}$.

Proof. According to 5.2 c), the standard involution $z \rightsquigarrow -1/Nz$ also induces an involution on the curve X. Let this involution act on the homology of X by multiplication by $-C = +1$ (the sign is chosen to agree with Weil's notation in [16]).

We now compute its action directly. It acts on the group $\Gamma_0(N)$ by matrix conjugation $\left(\begin{smallmatrix}0 & 1\\ -N & 0\end{smallmatrix}\right)$ and hence takes $\left(\begin{smallmatrix}a & b\\ Nc & d\end{smallmatrix}\right)$ to $\left(\begin{smallmatrix}a & c\\ Nb & d\end{smallmatrix}\right)^{-1}$. Thus the class

$$\left\{-\frac{b}{a},0\right\}=\left\{-\frac{b}{a},\begin{pmatrix}a & b\\ Nc & d\end{pmatrix}\left(-\frac{b}{a}\right)\right\}$$

goes to the class

$$-\left\{-\frac{c}{a},0\right\}=-\left\{-\frac{c}{a},\begin{pmatrix}a & c\\ Nb & d\end{pmatrix}\left(-\frac{c}{a}\right)\right\}$$

(we are using Proposition 1.4). But $c \equiv -N^{-1}b^{-1} \bmod a$, because $ad - Nbc = 1$.

Turning now to Definition 5.4, we find from this a functional equation for the functions $x^{\pm}$:

$$x^{\pm}\left(\frac{b}{a}\right)=Cx^{\pm}\left(\frac{-N^{-1}b^{-1} \bmod a}{a}\right),$$

so that

$$\sum_b\chi(b)x^{\pm}\left(\frac{b}{m}\right)=\sum_b\chi(-N^{-1}b^{-1} \bmod m)\,x^{\pm}\left(\frac{-N^{-1}b^{-1} \bmod m}{m}\right)$$
$$=C\overline{\chi}(-N)\sum_b\overline{\chi}(b)x^{\pm}\left(\frac{b}{m}\right) \tag{38}$$

(here $m = m_\chi$, b runs through the residue classes mod m, and $x^{\pm}$ is chosen corresponding to sign χ). Thus, combining the sums in (37) corresponding to complex conjugation characters and bringing all factors outside, we obtain

$$\prod_{\chi \in \overline{M}} \frac{1}{2}\left(\sum_{b \bmod m_\chi} \chi(b)\, x^{\pm}\left(\frac{b}{m_\chi}\right)\right) = \varepsilon T^2, \tag{39}$$

where ϵ is a root of unity and T is an integer in the value field of the characters $\chi \in \overline{M}$ (T is integral because $(m_\chi, N) = 1$ by assumption, because $x^{\pm}(b/m) \in \mathbf{Z}$, and finally because the functions $b \rightsquigarrow \chi(b) x^{\operatorname{sign}\chi}(b/m_\chi)$ are even functions, so that the sums $\Sigma_{b \bmod m_\chi}$ contain each term twice).

On the other hand, $\Pi_{\chi \in \overline{M}}$ is an ordinary integer, because all of the conjugates over $\mathbf{Q}$ appear with every sum under the product sign. Formula (39) shows that adjoining a square root of this number (divided by ϵ) to $\mathbf{Q}$ does not take us outside the value field of the characters χ. Consequently, only primes which ramify in this value field appear with odd exponent in the left side of (32). (This argument was mentioned to me by A. N. Andrianov.)

The proposition is proved.

Remark. Of course, formula (38) is also applicable to real characters χ; it is trivial in the case $C\chi(-N) = 1$, and in the case $C\chi(-N) = -1$ it shows that $\Sigma_{b \bmod m} \chi(b) x^{\pm}(b/m) = 0$. This argument was used earlier in a somewhat different form to actually construct forms of the curve X over quadratic extensions (corresponding to real χ) whose L-series vanishes at $s = 1$ (see, for example, the appendix to Birch [2]).

6.4. We now compare the behavior of the right sides of (30) and (35)* over cyclotomic Γ-extensions K of the field $\mathbf{Q}$. In this case we have Mazur's results [10], [11], [9] concerning the behavior of the groups $X(K)$ and $Ш(X \otimes K)$ obtained using Iwasawa's theory of Γ-modules. Our formulas agree very well with the conditional interpretation of Mazur's theory in the language of L-functions, and they also allow us to make some predictions in the cases when the Γ-module technique has so far been insufficient.

We introduce the following notation. Let l be an odd prime, $l \nmid 2N$ (the case $l = 2$ differs in inessential details, and the case $l \mid N$ requires separate consideration, which we shall not go into here). Let $G = \{\epsilon \in \mathbf{Z}_l \mid \epsilon^{l-1} = 1\}$. The group G acts on the field $\mathbf{Q}(\zeta_n)$: $\zeta_n = e^{2\pi i/l^n}$, $\zeta_n \rightsquigarrow \zeta_n^g$, $g \in G$. We set $K_n = \mathbf{Q}(\zeta_{n+1})^G$, $K_\infty \mathbf{U}_{n=1}^{\infty} K_n$. Obviously $\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_\infty$. The Galois group $\Gamma = \operatorname{Gal} K_\infty/\mathbf{Q}$ is canonically isomorphic to $(1 + l\mathbf{Z}_l)^* \overset{\log}{\simeq} \mathbf{Z}_l$. We set $\Gamma_n = \Gamma^{l^n}$; then $\operatorname{Gal}(K_n/\mathbf{Q}) \cong \Gamma/\Gamma_n \cong \mathbf{Z}_l/l^n$.

The extension $K_{n-1}/\mathbf{Q}$ corresponds to the primitive Dirichlet characters modulo $1, \cdots, l^n$ whose values are roots of 1 of order l^k. All of these characters are even. Let M_{n-1} be the subset of them which are associated with the field K_{n-1} but not with the field K_{n-2}.

we set

$$\Lambda_{n-1} = \prod_{\chi \in M_{n-1}} \frac{1}{2}\left(\sum_{b \bmod l^n} \chi(b)\, x^{+}\left(\frac{b}{l^n}\right)\right). \tag{40}$$

According to (30), Λ_{n-1} is the nontrivial additional factor in the value of L at one which appears in going from K_{n-2} to K_{n-1}. If $X(K_{n-2}) = X(K_{n-1})$, then, by (36)*, this same number must also be the nontrivial factor in the expression for the order of $Ш_{n-1}$. As has already been noted, $\Lambda_n \in \mathbf{Z}$.

We further set $\lambda = L(X, 1)/W^+$; this is a rational number (possibly zero). We recall that (a_n) are the coefficients of the canonical series $L(X, s)$.

6.5. Theorem. a) $\Lambda_1 \equiv 0 \bmod l$ *if and only if either* $a_l \equiv 1 \bmod l$, *or* l *divides the numerator of* λ (*all primes divide zero*).

b) *For* $n \geq 2$ *we have* $\Lambda_n \equiv 0 \bmod l$ *if and only if either* $a_l \equiv 1 \bmod l$, *or* $a_l \equiv 0 \bmod l$, *or* l *divides the numerator of* λ.

In particular, for all other l *we have* $\Lambda_n \neq 0$ *for all* n.

Proof. Let l_n be a prime divisor of l in $Q(\zeta_n)$. If $m_\chi = l^n$, then $\chi(b)^{l^{n-1}} = 1$ for all b, $(b, l) = 1$, so that $\chi(b) \equiv 1 \bmod l_{n-1}$. Consequently

$$\Lambda_{n-1} \equiv \prod_{\chi \bmod l} \frac{1}{2}\left(\sum_{\substack{b \bmod l^n \\ (b,l)=1}} x^{+}\left(\frac{b}{l^n}\right)\right) \bmod l \equiv \left(\frac{1}{2}\sum_{(b,l)=1} x^{+}\left(\frac{b}{l^n}\right)\right)^{\varphi(l^{n-1})} \bmod l. \tag{41}$$

Hence we must clarify the behavior of $\frac{1}{2}\Sigma_{(b,l)=1} x^{+}(b/l^n) \bmod l$. To do this we set $m = l^n$, $n \geq 2$, in formula (29):

$$\frac{1}{2}\sum_{\substack{b \bmod l^i \\ i \leq n}}{}' x^{+}\left(\frac{b}{l^i}\right) = \left(a_{l^n} - \sum_{i=0}^{n} l^i\right)\lambda. \tag{42}_n$$

Subtracting formula $(42)_{n-1}$ from $(42)_n$, we find

$$\frac{1}{2}\sum_{b \bmod l^n}{}' x^{+}\left(\frac{b}{l^i}\right) = (a_{l^n} - a_{l^{n-1}} - l^n)\lambda. \tag{43}_n$$

In the sum on the left the obstacle is the residue classes $b \equiv 0 \bmod l$; in order to remove them, we again subtract $(43)_{n-1}$ from $(43)_n$:

$$\frac{1}{2}\sum_{\substack{b \bmod l^n \\ (b,l)=1}} x^{+}\left(\frac{b}{l^n}\right) = (a_{l^n} - 2a_{l^{n-1}} + a_{l^{n-2}} - l^n + l^{n-1})\lambda. \tag{44}$$

We now consider the cases $n = 2$ and $n > 2$ separately.

The case $n = 2$. Since $a_{l^2} = a_l^2 - l$, we find from (44) that

$$\frac{1}{2}\sum_{(b,l)=1} x^{+}\left(\frac{b}{l^2}\right) = (a_l - 1 + l)(a_l - 1 - l)\lambda.$$

is immediately clear from this that if $l \mid \lambda$ or $l \mid (a_l - 1)$, then $l \mid \Lambda_1$. Conversely, if $\mid \Lambda_1$ but $l \nmid (a_l - 1)$, then l must divide the numerator of λ. This proves assertion a).

The case $n > 2$. We have

$$a_{l^n} = a_l a_{l^{n-1}} - l a_{l^{n-2}} \equiv a_l a_{l^{n-1}} \bmod l,$$

so that $a_{l^n} \equiv a_l^n \bmod l$. Hence the coefficient of λ in (44) is congruent to $l^{n-2}(a_l - 1)^2 \bmod l$. It is hence clear that if $a_l(a_l - 1) \equiv 0 \bmod l$ and l does not appear in the denominator of λ, or if $l \mid \lambda$, then we have $l \mid \Lambda_{n-1}$. We now suppose that $a_l(a_l - 1) \equiv 0 \bmod l$, but that l appears in the denominator of λ. The number $(a_l - 1)\lambda$ is an integer by $(43)_1$; $a_l - l - 1 \neq 0$, because this is the number of points on the reduction of $X \bmod l$; finally, $a_1 - 1 - l$ is divisible by no higher than the first power of l for $l > 2$ by the Weil estimate $|a_l| < 2\sqrt{l}$. Consequently the denominator of λ is not divisible by l^2 and $a_l \equiv 1 \bmod l$. On the other hand, if we twice use the formula $a_{l^n} = a_l a_{l^{n-1}} - l a_{l^{n-2}}$, we easily obtain

$$a_{l^n} - 2a_{l^{n-1}} + a_{l^{n-2}} = (a_l - 1)^2 a_{l^{n-2}} - l(a_l a_{l^{n-3}} + a_{l^{n-2}} - 2a_{l^{n-3}}).$$

Hence the coefficient of λ in (43) is divisible by l^2, so that the left side of (43) and Λ_{n-1} are divisible by l.

Conversely, if l divides Λ_{n-1} but does not divide the numerator of λ, then it is clear from (44) that l divides

$$a_{l^n} - 2a_{l^{n-1}} + a_{l^{n-2}} \equiv a_l^{n-1}(a_l - 1) \bmod l.$$

The theorem is proved.

We derive several conditional corollaries from the theorem, using the Birch–Swinnerton-Dyer conjecture, and we compare them with Mazur's unconditional results.

We recall that $l \nmid 2N$ and that primes l for which $a_l \equiv 0 \bmod l$, are called *supersingular for* X (Deuring), while those for which $a_l \equiv 1 \bmod l$, are called *anomalous for* X (Mazur).

6.6. Corollary*. *If* $[Ш(\mathbf{Q})] < \infty$, *and if* l *does not divide the numerator of* $\lambda = L(X, 1)/W^+$ *and is neither anomalous nor supersingular for* X, *then the group* $X(K_\infty)$ *is finite, and the* l*-component of the groups* $Ш(X \otimes K_n)$ *has bounded order as* $n \to \infty$.

In fact, according to Theorem 6.5, under the conditions of the corollary we have $L(X \otimes K_n, 1) \neq 0$ for all n, so that $\operatorname{rk} X(K_n) = 0$. On the other hand, as Mazur showed, the group $\widetilde{X}(K_\infty)$ is finite. Finally, the ratio of local factors in (36)* becomes 1 as $n \to \infty$ to within a 2-component, and by Theorem 6.5 the new factors in $\Pi_\chi(\frac{1}{2}\Sigma)$ are not divisible by l.

This corollary is conditional, but this very result is proved precisely in Mazur's theory under the assumption that l does not divide

$$[Ш(X)] \prod_{p \mid N} [\pi_0(X \bmod p)]$$

instead of the numerator of λ: this agrees well with (34)*.

6.7. Corollary*. *If* $[Ш(\mathbf{Q})] < \infty$ *and* l *either divides the numerator of* λ *or is a supersingular or anomalous prime for* X, *then*

$$\operatorname{rk} X(K_n) + [Ш(X \otimes K_n)^{(l)}] \to \infty \quad \text{as} \quad n \to \infty.$$

In fact, if the quotients $L(X \otimes K_n, s)/L(X \otimes K_{n-1}, s)\big|_{s=1}$ equal zero for infinitely many values of n, then $\operatorname{rk} X(K_n) \to \infty$; otherwise

$$\frac{[Ш(X \otimes K_n)]}{[Ш(X \otimes K_{n-1})]} \equiv 0 \bmod l$$

for all $n \geq n_0$ by Theorem 6.5 and formula (36)*, if we take into account the stabilization of the local factors.

The parallel unconditional result in Mazur's theory was only proved for anomalous primes, and asserts the following: *if* $a_l \equiv 1 \bmod l$ *then either* $\operatorname{rk} X(K_\infty) > 0$ (*and this rank is necessarily finite*), or $[Ш(X \otimes K_n)^{(l)}] \to \infty$, *or else both hold together.*

Thus, in this place Mazur's theory partially overlaps Corollary 6.7*, but partially complements it: combining both results, we find for $a_l \equiv 1 \bmod l$ we *must** have $[Ш(X \otimes K_n)^{(l)}] \to \infty$.

The supersingular primes have so far resisted the Γ-module technique; hence it might be interesting to note a partial result relating to them:

6.8. Corollary*. *If* $[Ш(\mathbf{Q})] < \infty$, *and if* l *is supersingular and does not divide the numerator of* λ, *then the group* $X(K_1)$ *is still finite.*

In fact, Theorem 6.5 b) shows that $L(X \otimes K_1, 1) \neq 0$. For anomalous numbers l with the condition $L(X, 1) \neq 0$ there are no apparent reasons why $L(X \otimes K_1, 1)$ cannot vanish, but the author does not know any examples where it does vanish.

6.9. Corollary*. *If* $\operatorname{rk} X(\mathbf{Q}) > 0$, *then for all* $l \nmid 2N$

$$\operatorname{rk} X(K_n) + [Ш(X \otimes K_n)^{(l)}] \to \infty.$$

The reasoning is the same as in the proof of Corollary 6.7, since in this case we must have $\lambda = 0$, so that $\Lambda_n \equiv 0 \bmod l$ for all n and l.

Mazur [10] conjectured that the rank of $X(K_n)$ remains bounded (at least for non-supersingular l).

The parallel conjecture under our conditions is the following:

6.10. Conjecture. $\Lambda_n \neq 0$ *for all* $n \geq n_0(X, l)$.

I am unable to prove this result in any case except those which are included in Theorem 6.5. Possibly investigating Λ_n p-adically for $p \mid N$ could give useful information.

In certain special circumstances we can prove that the numbers Λ_n are divisible by certain special primes. In order to formulate the result precisely, we introduce the following

6.11. Definition. An isogeny $\chi : X \to Y$ of elliptic curves over $\mathbf{Q}$ is called

admissible if, for any prime p, it induces a separable morphism of the connected components of the closed fibers of the Néron models of the curves X and Y over p.

The following two properties of admissible isogenies can be proved without difficulty:

a) *Let $\chi : X \to Y$ be an admissible isogeny, and let ω_Y be a Néron differential. Then $\chi^*(\omega_Y)$ is a Néron differential on X.*

In fact, $\chi^*(\omega_Y)$ is regular on the Néron model of X, and a divisor of zeros can only include the components of the fibers where the isogeny χ is inseparable.

b) *If an admissible isogeny $\chi : X \to Y$ exists, then the conductors and the canonical L-series of the curves X and Y coincide.*

We need only verify that the divisors of the conductor and the Euler factors of the L-series coincide at the points of degenerate reduction, and this is proved directly from the definitions.

Let $\chi : X \to Y$ be an isogeny, and let $y_X^{\pm}$ and $y_Y^{\pm}$ be the generators of the real (+) and imaginary (−) homology classes of the curves X and Y, respectively. We shall say that χ has type (q^+, q^-) if $\chi_*(y_X^{\pm}) = q^{\pm} y_Y^{\pm}$.

6.12. Proposition. *Let $\chi : X \to Y$ be an admissible isogeny of curves of type (q^+, q^-), and let N be their common conductor.*

a) *If $\psi : X_N \to X$ is a Weil uniformization of the curve X, then its composition with χ is a Weil uniformization of the curve Y.*

b) *Let $x_Y^{\pm}$ be the functions associated to the curve Y according to Definition 5.4. If the denominator of the number $a \in \mathbb{Q}$ is relatively prime to N, then*

$$x_Y^{+}(a) \equiv 0 \bmod q^+, \quad x_Y^{-}(a) \equiv 0 \bmod q^-. \tag{45}$$

Proof. Assertion a) is obtained from properties 6.11 a), b) and the definition of uniformization in 5.2: we need only choose the Néron differentials on X and Y compatibly. Assertion b) follows from Definition 5.4 and the definition of type (q^+, q^-).

6.13. Corollary. *Let $K' \supset K$ be abelian extensions of the field $\mathbb{Q}$ with discriminant relatively prime to N, and let M, r, r_i, etc. be defined as they were before Theorem 5.6. Then*

$$\coprod_{\chi \in M} \frac{1}{2}\left(\sum_{b \bmod m_\chi} \chi(b) x_Y^{\operatorname{sign} \chi}\left(\frac{b}{m_\chi}\right)\right) \equiv 0 \bmod (q^+)^{r'-r}(q^-)^{r_2-r_1}. \tag{46}$$

Using formula (36)*, we can derive from this conditional corollaries concerning the behavior of $Ш(X \otimes K')$ and $X(K')$, if we only ensure no cancellation of q^+ and q^- with the local factors in the right side of (36)*. For example, this result is obtained for the curve Y by precisely the same reasoning as in Corollary 6.7.

6.14. Corollary*. *Let $\mathbb{Q} \subset K_1 \subset \cdots \subset K_n \subset \cdots$ be a Γ-extension corresponding to the prime $l \nmid 2N$. Then either the rank of $Y(K_n)$ increases without bound, or else the order of $[Ш(Y \otimes K_n)]$ is divisible by $(q^+)^{[K_n:\mathbb{Q}]-\text{const}}$ as $n \to \infty$.*

(The constant in the exponent of q^+ appears because the group $X(K_n)$ can grow in the first few steps of the Γ-extension, and also the contribution of the local factors in (36)* does not manage to stablize to 1.)

This result can be compared with Proposition 9.1 in Mazur's article [10].

6.15. Examples and remarks. a) The existence of admissible isogenies is a rather exceptional phenomenon. (The multiplication $X \xrightarrow{n} X$ is not admissible for $n > 1$!) If the kernel of $\chi : X \to Y$ is cyclic and is generated by a rational point x of order q, then for $(q, N) = 1$ admissibility follows from Lutz's theorem that the "coordinates of x are integers," i.e. the reduction of the kernel of χ does not become trivial. However the case of common divisors of q and N requires special investigation.

Here is the data on the existence of admissible isogenies of curves X_N of genus one; $q^- = 1$, so that we only give q^+:

N	11	14	15	17	19	20	21	27	49
q^+	5	3	4	4	3	2	4	3	2

Corollary 6.14* for the curve X_{11} was proved by Mazur [10] for $l = 5$; in this case the rank of $Y(K_n)$ equals zero for all n.

b) Assertion (45) relates to the behavior of the functions $x_Y^{\pm}$ constructed for the *image* Y of an admissible isogeny. However, observing lengthy tables of the function $x^{\pm}$ for the curve X_{11} compelled us also to suggest some regularity in the behavior mod $q^{\pm}$ of the functions $x_X^{\pm}$ constructed for the *domain* X of the admissible isogeny.

More precisely, the following assertion is fulfilled in the tables ($X = X_{11}$, $q^+ = 5$)

open question!

$$\text{the residue class } x_{11}^{+}\left(\frac{b}{a}\right) \bmod 5 \text{ depends only on } a \tag{47}$$

(*for all $a \not\equiv 0 \bmod 11$ and $(b, a) = 1$*).

The analogous property is observed for $N = 17, 19, 27$; see §8.

Although this assertion seems to have the same nature as property (45), I have not been able to prove it. The assertion is rather striking, since in the computation of $x_{11}^{+}(b/a)$ the denominators of the convergents to b/a are operated on modulo 11, and not modulo 5.

A natural generalization of the conjecture (47) is the conjecture that *the residue classes $x_X^{\pm}(a/b) \bmod q^{\pm}$ are constant with respect to b.*(1) We note that the congruence (46) would also follow from this assertion, which is weaker than (45), because $\Sigma_b \chi(b) = 0$ for any nonprincipal character χ.

Evidence for (47) is noted in the commentary on the tables in §8.

§7. Noncommutative reciprocity law

As the basic result of this section, in 7.3 we formulate a special case of Theorem

(1) *Added in proof.* Drinfel'd has proved an assertion of this type with another interpretation of the numbers $q^{\pm}$. Swinnerton-Dyer has obtained an analogous fact.

9 on the coefficients of parabolic forms, which can be derived from formula (20). The atures of a noncommutative reciprocity law emerge in this special case.

We begin by formulating the necessary concepts.

7.1. **Admissible solutions.** Let $d > 1$ be an integer. A solution of the equation $= \Delta\Delta' + \delta\delta'$ is an ordered quadruple of numbers $(\Delta, \Delta', \delta, \delta')$ satisfying this equa- on. A solution is called *admissible* if it consists of integers satisfying the addition nditions

$$(\Delta, \delta) = (\Delta', \delta') = 1, \qquad \Delta > \delta > 0, \tag{48}$$

id also

$$\text{either } \Delta' > \delta' > 0, \tag{49}$$

$$\text{or else } \delta' = 0,\ \Delta = d,\ \Delta' = 1,\ 0 \leq \delta < \frac{d}{2}. \tag{50}$$

e call the solutions (50) *boundary* solutions.

The *set* of admissible solutions of the equation $d = \Delta\Delta' + \delta\delta'$ determines a finite *mily* of pairs (Δ, δ) which appear in these solutions. We shall later need to sum func- ons of pairs of integers over the terms of this family. Hence for practical purposes it uffices to think of this family of pairs (Δ, δ) as the set of different pairs, each equip- ed with a multiplicity.

We shall also call such pairs (Δ, δ) d-admissible.

7.2. Let X be an elliptic curve over $\mathbf{Q}$ with conductor N which has a Weil uni- ormization in the strong sense. Let $L(X, s)$ be its canonical Dirichlet series, and let a_n be the nth coefficient.

If Δ is an integer, we set $\widetilde{\Delta} = \Delta \bmod N$. If $(\Delta, \delta) = 1$, then $\widetilde{\Delta} : \widetilde{\delta}$ denotes a point f the projective line $\mathbf{P}^1(\mathbf{Z}/(N))$, as in 2.3.

With this notation we have the following

7.3. **Fundamental Theorem.** *Suppose that $L(X, 1) \neq 0$. Then there exists a func- ion $y : \mathbf{P}^1(\mathbf{Z}/(N)) \to \mathbf{Q}$ depending only on X such that the following holds for any rime $l \nmid 2N$:*

$$1 - a_l + l = \sum_{l = \Delta\Delta' + \delta\delta'} y(\widetilde{\Delta} : \widetilde{\delta}), \tag{51}$$

here the summation on the right is over the family of all l-admissible pairs (Δ, δ).

Remarks. a) The function y can be expressed explicitly in terms of the function ε^+ for the curve X (see formula (74) in 7.10).

b) The left side of (51) is the number of $\mathbf{Z}/(l)$-points on the reduction of X mod l, nd the right side is some sum over the solutions of the equation $l = \Delta\Delta' + \delta\delta'$ taken nod N. The general form of this symmetry:

(an equation depending on N, taken mod l)

$\Updownarrow$

(an equation depending on l, taken mod N)

brings to mind a reciprocity law. It relates explicitly to noncommutative extensions, since a_l in (51) is the trace of the Frobenius automorphism of the fields obtained by adjoining to $\mathbf{Q}$ the points of finite order on the curve X (see Shimura [14]).

Another point of view regarding equation (51) is that it gives information on the representations of l by the indefinite quadratic form $\Delta\Delta' + \delta\delta'$. Eichler [5] gave a general technique for obtaining such formulas for representations by positive forms (using theta-functions). It seems that our result has another nature.

7.4. The plan of proof for Theorem 7.3 and its generalization is as follows. Formula (20) gives an expression for $1 - a_l + l$ in terms of integrals over the homology classes $|0, b/l|_N, 0 \leq b \leq l-1$. Formula (16) allows us to represent each class $|0, b/l|_N$ as a sum of distinguished classes $\xi(\widetilde{c} : \widetilde{d})$ whose arguments are (up to sign) the ratios of the denominators mod N of the successive convergents of b/l. Finally, a lemma of Heilbronn [6] allows us to go from continued fractions to solutions of the equation.

We begin the proof by giving Heilbronn's lemma.

7.5. **Formal continued fractions.** Following Heilbronn [6], we introduce the polynomials $Q_i \in \mathbf{Z}[T_1, \cdots, T_n, \cdots]$, $i \geq -1$, by the inductive formulas

$$Q_{-1} = 0, \qquad Q_0 = 1, \qquad Q_n = T_n Q_{n-1} + Q_{n-2} \text{ for } n \geqslant 1.$$

Obviously, $Q_n \in \mathbf{Z}[T_1, \cdots, T_n]$, so that we may write Q_n (and its particular values) as a polynomial in n arguments for $n \geq 1$. We shall also apply this same notation for $n = 0, -1$, but then we do not pay attention to any arguments.

It is easy to verify that

$$Q_n(T_1, \ldots, T_n) = Q_n(T_n, \ldots, T_1). \tag{52}$$

The following formula gives the connection with continued fractions:

$$\frac{Q_{n-1}(T_2, \ldots, T_n)}{Q_n(T_1, \ldots, T_n)} = \cfrac{1}{T_1 + \cfrac{1}{T_2 + \cdots \cfrac{1}{T_n}}}. \tag{53}$$

It remains valid for $n = 0$ if we take the right side equal to zero in this case.

The successive convergents to (53) are defined by the formulas

$$\frac{Q_{n-1}(T_2, \ldots, T_n)}{Q_n(T_1, \ldots, T_n)}, \ \ldots, \ \frac{Q_{m-1}(T_2, \ldots, T_m)}{Q_m(T_1, \ldots, T_m)}, \ \ldots, \ \frac{Q_0}{Q_1}, \ \frac{Q_{-1}}{Q_0} = \frac{0}{1}. \tag{54}$$

The index of a convergent is the index of its denominator. We have

$$Q_{m-1}(T_2, \ldots, T_m) Q_{m-1}(T_1, \ldots, T_{m-1}) - Q_m(T_1, \ldots, T_m) Q_{m-2}(T_2, \ldots, T_{m-1}) = (-1)^{m-1}. \tag{55}$$

The connection with the equation $d = \Delta\Delta' + \delta\delta'$ will be established in 7.7 using the fundamental formula

$$Q_n(T_1, \ldots, T_n) = Q_m(T_1, \ldots, T_m)\,Q_{n-m}(T_{m+1}, \ldots, T_n) + Q_{m-1}(T_1, \ldots, T_{m-1})\,Q_{n-m-1}(T_{m+2}, \ldots, T_n), \tag{56}$$

which makes sense and remains valid for all $0 \le m \le n$. It is proved by induction, decreasing m from the obvious cases $m = n$ and $m = n - 1$.

7.6. **Expansion of rational numbers in continued fractions.** Let $0 < \alpha < \frac{1}{2}$ be a rational number. It uniquely determines an integer $n = n(\alpha) \ge 1$ and positive integers $c_1, \ldots, c_n$ such that $c_1 \ge 2$, $c_n \ge 2$ and

$$\alpha = \frac{Q_{n-1}(c_2, \ldots, c_n)}{Q_n(c_1, \ldots, c_n)} = \cfrac{1}{c_1 + \ldots + \cfrac{1}{c_n}}. \tag{57}$$

The number n is called the length of the (continued fraction) expansion of α, and the numbers $c_1, \ldots, c_n$ are called the partial quotients of α. Substituting $c_1, \ldots, c_n$ for $T_1, \ldots, T_n$ in (54), we obtain the successive convergents of α, and also their numerators and denominators.

7.7. **Heilbronn's Lemma.** *Let $d > 2$ be an integer. The following two families of ordered pairs of integers coincide:*

a) *The pairs of neighboring denominators (from larger to smaller) in the sequence of convergents of all possible rational numbers of the form b/d, $(b, d) = 1$, $1 \le b < d/2$.*

b) *The pairs (Δ, δ) taken for all possible admissible solutions of the equation $d = \Delta\Delta' + \delta\delta'$.*

(Coincidence of families means coincidence of sets and multiplicities: see 7.1.)

Proof. The first family of pairs is indexed by the set consisting of elements of the form

$$\left[\text{the fraction } \alpha = \frac{b}{d}\left((b, d) = 1 \text{ and } 1 \leqslant b < \frac{d}{2}\right);\ \text{the integer } 1 \leqslant m \leqslant n(\alpha)\right]. \tag{58}$$

This element corresponds to the pair [mth denominator, $(m-1)$th denominator of the convergents of α] in the family a).

The second family of pairs is indexed by the set

$$\text{admissible solutions of the equation } d = \Delta\Delta' + \delta\delta'. \tag{59}$$

We shall construct mutually inverse maps of the sets (58) $\leftrightarrow$ (59) which preserve the pairs in the families a) and b).

The map (58) $\to$ (59). Let $(c_1, \ldots, c_n)$ be the partial quotients for α, and let $1 \le m \le n = n(\alpha)$. We set

$$\Delta = Q_m(c_1, \ldots, c_m), \quad \delta = Q_{m-1}(c_1, \ldots, c_{m-1}),$$
$$\Delta' = Q_{n-m}(c_{m+1}, \ldots, c_n), \quad \delta' = Q_{n-m-1}(c_{m+1}, \ldots, c_n). \tag{60}$$

It is clear from (53), (56) and (57) that $d = \Delta\Delta' + \delta\delta'$. Since the c_i are positive, it follows from the recursion relations for Q_n that $\Delta > \delta > 0$ and $\Delta' > \delta' \ge 0$. From (60) we have $(\Delta, \delta) = (\Delta', \delta') = 1$. It remains to verify that the admissible boundary solutions are obtained for $\delta' = 0$. But if $\delta' = 0$, then $m = n$, since $\Delta = d$ and $\Delta' = 1$; finally, $1 \le \delta \Delta d/2$, because $c_n \ge 2$ (apply the recursion relation $\Delta = c_m\delta + Q_{m-2}$).

The map (59) $\to$ (58). Let $(\Delta, \Delta', \delta, \delta')$ be an admissible solution. If it is a boundary solution, we set

$$m = n = \text{the length of the expansion of } \delta/\Delta = \delta/d;$$

we define the numbers $c_1, \ldots, c_n$ by the formula

$$\frac{\delta}{d} = \cfrac{1}{c_n + \ldots + \cfrac{1}{c_1}}, \quad c_n \geqslant 2, \quad c_1 \geqslant 2, \tag{61}$$

and the number α by the formula

$$\alpha = \cfrac{1}{c_1 + \ldots + \cfrac{1}{c_n}}. \tag{62}$$

The denominator of α equals d; this follows from (61), (62) and (52). The numerator of α does not exceed $d/2$; this follows because $\delta/d < \frac{1}{2} \Rightarrow c_n \ge 2$, if we use the recursion relations for Q_n together with (53).

The nonboundary solutions give the pairs (58) with $m < n(\alpha)$. If $(\Delta, \Delta', \delta, \delta')$ is not a boundary solution, we define $c_1, \ldots, c_n$ and m by the formulas

$$\frac{\delta}{\Delta} = \cfrac{1}{c_m + \ldots + \cfrac{1}{c_1}}, \quad c_1 \geqslant 2, \tag{63}$$

$$\frac{\delta'}{\Delta'} = \cfrac{1}{c_{m+1} + \ldots + \cfrac{1}{c_n}}, \quad c_n \geqslant 2, \tag{64}$$

and we set

$$\sigma = \cfrac{1}{c_1 + \ldots + \cfrac{1}{c_n}}.$$

The denominator of α obviously equals d; this follows from (63), (64) and (56). In addition, $0 < \alpha < \frac{1}{2}$, since $c_1 \ge 2$.

It is automatically verified that these set maps are mutually inverse and preserve the pairs which interest us, The lemma is proved.

Remark. It is clear from the proof that if the pair (Δ, δ) corresponds to the pair [mth denominator, $(m-1)$th denominator], then

$$m = \text{the length of the expansion of } \delta/\Delta = n(\delta/\Delta) \tag{65}$$

(see (63)).

7.8. We now proceed to formulate a theorem which contains Theorem 7.3 as a special case. Let $\Phi(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ be a $\Gamma_0(N)$-parabolic form which is an eigenfunction relative to all Hecke operators T_m with $(m, N) = 1$. We suppose that $a_1 = 1$; $\Phi | T_m = a_m \Phi$ for all m, $(m, N) = 1$.

Further, for any point $\tilde{c} : \tilde{d} \in \mathbf{P}^1(N))$ set

$$\eta(\tilde{c} : \tilde{d}) = \xi(\tilde{c} : \tilde{d}) - \xi(\tilde{d} : \tilde{c}), \tag{66}$$

where the classes $\xi(\tilde{c} : \tilde{d}) \in H_1(X_N(\mathbf{C}), \mathbf{R})$ are defined in 2.5. Finally, if

$$\int_0^{i\infty} \Phi(z)\, dz = \int_{\{0, i\infty\}} \omega \neq 0,$$

where ω is the differential of the first kind on $X_N(\mathbf{C})$ corresponding to Φ, then we define the function $y : \mathbf{P}^1(\mathbf{Z}/(N)) \to \mathbf{C}$ by the formula

$$y(\tilde{c} : \tilde{d}) = \int_{\eta(\tilde{c} : \tilde{d})} \omega \Big/ \int_{\{0, i\infty\}} \omega. \tag{67}$$

We note that $\eta(-\tilde{c} : \tilde{d}) = \eta(\tilde{c} : \tilde{d})$, so that y is an even function.

7.9. **Theorem.** *With the notation and assumptions of the last subsection, for any m, $2N) = 1$, we have*

$$\sum_{d|m} d - a_m = \sum_{\substack{d|m \\ d>1}} \tau\left(\frac{m}{d}\right) \sum_{d = \Delta\Delta' + \delta\delta'} y(\tilde{\Delta} : \tilde{\delta}), \tag{68}$$

where $\tau(m)$ is the number of divisors of m, and the (Δ, δ) in the inner sum run through all admissible pairs.

Proof. According to formula (20) of Theorem 3.3,

$$\left(\sum_{d|m} d - a_m\right) \int_{\{0, i\infty\}} \omega = \sum_{d|m} \sum_{b \bmod d} \int_{\left\{0, \frac{b}{d}\right\}} \omega.$$

An irreducible fraction b/d on the right obviously appears $\tau(m/d)$ times in the form $\delta\varepsilon$ for all possible $\delta/(m/d)$. The contribution from the sum with $d = 1$ equals zero, since $\{0, b\} = 0$ for $b \in \mathbf{Z}$. Consequently

$$\left(\sum_{d|m} d - a_m\right) \int_{\{0, i\infty\}} \omega = \sum_{\substack{d|m \\ d>1}} \tau\left(\frac{m}{d}\right) \sum_{\substack{b \bmod d \\ (b,d)=1}} \int_{\left\{0, \frac{b}{d}\right\}} \omega. \tag{69}$$

The inner sum on the right is the integral of ω over the class $\sum_{(b,d)=1} \{0, b/d\}$. Using the fact that

$$\left\{0, \frac{d-b}{d}\right\}_N = \left\{0, -\frac{b}{d}\right\}_N,$$

we represent this class in the form

$$\sum_{\substack{1 \leqslant b < \frac{d}{2} \\ (b,d)=1}} \left(\left\{0, \frac{b}{d}\right\}_N + \left\{0, -\frac{b}{d}\right\}_N\right). \tag{70}$$

Let $d = d_n, \ldots, d_0$ be the successive denominators of the convergents of b/d. According to formula (16) of Theorem 2.7,

$$\left\{0, \frac{b}{d}\right\} = \sum_{k=1}^{n} \xi((-1)^{k-1} \tilde{d}_k : \tilde{d}_{k-1}). \tag{71}$$

Since the class $\{0, b/d\}$ is complex conjugate to $\{0, -b/d\}$, it follows from (12) that

$$\left\{0, -\frac{b}{d}\right\} = -\sum_{k=1}^{n} \xi((-1)^{k-1} \tilde{d}_{k-1} : \tilde{d}_k). \tag{72}$$

Combining (70), (71), (72) and (66), we find, after summing over b, $1 \leq b < d/2$, $(b, d) = 1$, and applying Heilbronn's lemma, that

$$\sum_{\substack{(b,d)=1 \\ 1 \leqslant b \leqslant d}} \left\{C, \frac{b}{d}\right\} = \sum_{d = \Delta\Delta' + \delta\delta'} \eta(\tilde{\Delta} : \tilde{\delta}), \tag{73}$$

where the sum on the right is taken over admissible solutions. The sign $(-1)^{k-1}$ in (72) disappears because η is even.

It is now clear that, combining (69) and (73), we obtain formula (68): we need only divide through both sides of (69) by $\int_{\{0, i\infty\}} \omega$ and recall the definition (67) of the function y. The theorem is proved.

7.10. Remarks. a) Under the conditions of Theorem 7.3, it is not hard to express the function y in terms of x^+. Namely, if $ad - bc = 1$, then

$$y(\tilde{c} : \tilde{d}) = 2\, \frac{x^+\left(\frac{a}{c}\right) - x^+\left(\frac{b}{d}\right)}{x^+(i\infty)}. \tag{74}$$

In fact, then

$$\xi(\tilde{c} : \tilde{d}) = \left\{\frac{b}{d}, \frac{a}{c}\right\} = \left\{\frac{b}{d}, 0\right\} - \left\{\frac{a}{c}, 0\right\}.$$

Using the definition of x^+, we find

$$\eta(\tilde{c} : \tilde{d}) = \left(x^+\left(\frac{b}{d}\right) - x^+\left(\frac{a}{c}\right)\right) \gamma^+.$$

Since, in addition, $\{0, i\infty\} = -\frac{1}{2} x^+(i\infty) \gamma^+$, it hence follows that (74) holds.

b) It is natural to write abelian reciprocity laws in the form $\prod_l S_l = 1$, where the S_l are certain symbols and l runs through the prime numbers and ∞. We can formally

derive an analogous relation from (51). Let $L(X, s) = \Pi_l L_l(X, s)$, where L_l are the local factors of the L-series. We suppose that $\Pi_l L_l(X, 1) = L(X, 1)$ in the sense of some type of (nonabsolute) convergence. For $l \nmid N$ we have $L_l(X, 1) = (1 - a_l + l)/l$. Hence from (51) we find

$$\prod_{l/2N} L_l(X, 1) \prod_{l \nmid 2N} \left(\frac{1}{l} \sum_{l=\Delta\Delta'+\delta\delta'} y(\tilde{\Delta} : \tilde{\delta}) \right) L(X, 1)^{-1} = 1. \tag{75}$$

Here it is natural to associate the factor $L(X, 1)^{-1}$ to the point at infinity in the field $\mathbf{Q}$.

c) It is interesting to connect formula (51) with the Sato-Tate conjecture on the distribution of (a_l) as $l \to \infty$ (see, for example, Serre [13]). The right side of (51) could possibly be treated by an independent statistical investigation.

In fact, the sums $\Sigma_k \phi(d_k, d_{k-1})$, where (d_k) are the successive denominators of the convergents to α, have been studied before. Lévy's book [7] contain facts on the distribution *almost everywhere* of such sums, for irrational α as well (some natural conditions ensuring convergence are imposed on ϕ). We are interested in the mean of such sums over all *rational* α with fixed denominator l and in the distribution of this mean when $l \to \infty$. It was to solve such a problem that Heilbronn [6] proved Lemma 7.7: he was interested in the function $\phi \equiv 1$, and he obtained the principal term of its asymptotic behavior. In our case the principal term is known in advance: it is $l + 1$, and a_l is a "random error."

A natural approach to studying the sums (51) is to expand the function y in terms of some elementary functions. For example, for N prime it would suffice to study the distribution of the sums over admissible solutions of the form

$$\sum_{l=\Delta\Delta'+\delta\delta'} \chi(\Delta)\overline{\chi}(\delta),$$

where χ is any multiplicative character mod N.

d) We would like to note a similarity between the considerations of this section and the constructions in Chapters V and VI of Venkov's book [3]. Comparing these results may lead to a better understanding of them.

e) The condition $\int_0^{i\infty} \Phi(z)dz \neq 0$ is only used to go from continued fractions to the equation $l = \Delta\Delta' + \delta\delta'$. If we do not insist on this, Theorem 3.5 allows us to give explicit formulas for the coefficients of any parabolic forms.

§8. Tables, their computation and use

The basic content of this section is tables of the functions $x^{\pm}(a)$ for $a \in \mathbf{Q}$, constructed for curves X_N of genus 1 for $N = 11$, 17, 19 and 27. Before proceeding to a discussion of the method used to compute these tables and the possibilities for using them, we shall bring together in one place and recall all the notation needed here, which was introduced in various places in the article.

8.1. **Notation and definitions.** The integer $N > 0$ is fixed, H is the complex upper halfplane, $\overline{H} = H \cup \mathbf{Q} \cup (i\infty)$ and $X_N(\mathbf{C}) = \Gamma_0(N)\backslash\overline{H}$. For any $\alpha, \beta \in \overline{H}$ the symbol $\{\alpha, \beta\}_N \in H_1(X_N(\mathbf{C}), \mathbf{R})$ designates the homology class of the path on $X_N(\mathbf{C})$ which is the image of a path on $\overline{H}$ from α to β. Further, $\mathbf{P}^1(\mathbf{Z}/(N)) = \{\text{classes of pairs } \tilde{c} : \tilde{d} \mid = c \bmod N,\ \tilde{d} = d \bmod N,\ (c, d) = 1\}$. The function $\xi_N : \mathbf{P}^1(\mathbf{Z}/(N)) \to H_1(X_N(\mathbf{C}), \mathbf{R})$ is defined by the equation

$$\xi_N(\tilde{c} : \tilde{d}) = \left\{ \frac{b}{d}, \frac{a}{c} \right\}_N \quad \text{for any} \quad ad - bc = 1.$$

Now let the genus of $X_N(\mathbf{C})$ equal 1. Then the subgroup of classes in $H_1(X_N(\mathbf{C}),$ invariant (anti-invariant) relative to conjugation is infinite cyclic; let γ^+ (γ^-) be any generator of this group.

After choosing γ^+ and γ^-, the functions $x_N^{\pm} : \mathbf{Q} \cup (i\infty) \to \mathbf{Q}$ are defined by the equations

$$\{-\alpha, 0\}_N \pm \{\alpha, 0\}_N = x^{\pm}(\alpha)\gamma^{\pm}.$$

The fundamental functions to be tabulated, which we first introduce here, are $\xi_N^{\pm} : \mathbf{P}^1(\mathbf{Z}/(N)) \to \mathbf{Q}$, which are defined by the formulas

$$\xi_N(\tilde{c} : \tilde{d}) \mp \xi_N(\tilde{d} : \tilde{c}) = \xi_N^{\pm}(\tilde{c} : \tilde{d})\gamma^{\pm}. \tag{76}$$

If we have at our disposal a table of the functions $\xi_N^{\pm}$ (their domain of definition consists of $N\Pi_{p|N}(1 + 1/p)$ points, and their range is the rational numbers with rather small numerators and denominators), it is not hard to compute an arbitrarily long table of the functions $x_N^{\pm}$ by using the formula

$$x_N^{\pm}\left(\frac{b}{a}\right) = \mp \sum_{k=1}^{n} \xi^{\pm}((-1)^{k-1}\tilde{a}_k : \tilde{a}_{k-1}), \tag{77}$$

where $a_n = a, a_{n-1}, \cdots, a_0 = 1$ are the denominators of the successive convergents of b/a (equation (77) is derived from the definitions and formula (16)). We further recall that the $x^{\pm}$ have period 1 and that x^+ is even and x^- is odd, so that we may limit ourselves to the arguments $0 < b/a \leq \frac{1}{2}$.

If in addition $\xi_N^+(\tilde{0} : \tilde{1}) \neq 0$ (this holds for all N for which the genus of X_N equals one), then we can tabulate the function $y_N : \mathbf{P}^1(\mathbf{Z}/(N)) \to \mathbf{Q}$, which is defined by the formula

$$y_N(\tilde{c} : \tilde{d}) = 2\frac{\xi_N^+(\tilde{c} : \tilde{d})}{\xi_N^+(\tilde{0} : \tilde{1})} \tag{78}$$

(and so it is proportional to ξ_N^+. Nevertheless, it is instructive to tabulate it separately from ξ_N^+, because it is used for different purposes).

8.2. **Use of the tables.** a) The fundamental function $\xi_N^{\pm}$ in the tables is necessary for computing $x_N^{\pm}$.

b) The functions $x_N^{\pm}$ are used to compute $L(X_N \otimes K, 1)$ over abelian extensions $K \subset \mathbf{Q}$, and also to compute the individual factors of these components corresponding to the different Dirichlet characters. Using the Birch–Swinnerton-Dyer conjecture, we can then make hypothetical estimates from below for the rank of the group $X(K)$ (which, of course, must be verified independently). Thus, for example, we can collect experimental data on questions which remain unsolved in Mazur's theory (the presence of jumps in the rank in a Γ-extension tower; the behavior of the rank for supersingular l, etc.).

c) The function y_N is used to compute the coefficients of $L(X, s)$ in any quantity using formula (51).

In addition, the tables can simply be looked over with the idea of trying to observe anything curious.

8.3. Computation of the tables. The compilation of the tables of the functions $\xi_N^{\pm}$ is in the first place based on Theorem 2.7 (and formula (12), which is necessary to choose γ^+ and γ^-). This theorem alone is sufficient to compute $\xi^{\pm}(\tilde{c} : \tilde{d})$ for all $\tilde{c}$ and $\tilde{d}$ which are not divisors of zero in $\mathbf{Z}/(N)$. In particular, if N is prime, then we obtain in this way all values of $\xi^{\pm}$, except for the values at the points $1 : 0$ and $0 : 1$ (here and later we shall omit the tilde over the numbers, since no ambiguity can arise if N is fixed). To compute the missing values of $\xi^{\pm}$ we must then use Theorems 3.3 and 3.5 (if N is prime Theorem 3.3 suffices) for any prime value of m, $m \nmid N$. For this purpose we must know in advance several coefficients of the canonical L-series.

The general plan is as follows.

a) To compile a list of the points $\mathbf{P}^1(\mathbf{Z}/(N))$.

b) To solve the system of equations (14) and (15), i.e. to find integral linear expressions for the symbols $(\tilde{c} : \tilde{d})$ in terms of independent parameters. The general number of parameters equals

$$2(\text{genus of } X_N) + (\text{number of parabolic points on } X_N) - 1.$$

The parameters must be chosen so that only 2(genus of X_N) parameters appear in the expression for $(\tilde{c} : \tilde{d})$ with $\tilde{c}$ and $\tilde{d}$ not divisors of zero, i.e. 2 parameters appear in the case genus $X_N = 1$, which is the case we shall work with.

For N not very large (less than a hundred), the system (14)–(15) can easily be solved by hand if we successively examine the 3-equations of (15) and the 2-equations of (14) which "link" these 3-equations. Each time, if we solve the next 3-equation in which at least one of the unknowns has already been found using the previous 2-equation, either we obtain a new free parameter or else we obtain a relation among the old parameters; if we use a reasonable procedure, the latter possibility rarely occurs.

c) To choose γ^+ and γ^- from among the linear combinations of the symbols $(\tilde{c} : \tilde{d})$ with $\tilde{c}$ and $\tilde{d}$ not divisors of zero, and to compute $\xi^{\pm}(\tilde{c} : \tilde{d})$ for these points $\tilde{c} : \tilde{d}$.

d) To compile a rather large table of the functions $x^{\pm}(b/a)$ for $(a, N) = (b, N) = 1$, using formula (16). The "extra" parameters which may appear in the separate terms of the sum

(16) because $(a_k, N) > 1$ automatically cancel out in the sum, so that the result is expressed in terms of γ^+ and γ^-.

e) To compute several coefficients of $L(X, s)$, which are necessary in order to apply Theorems 3.3 and 3.5.

f) Using Theorems 3.3 and 3.5, to compute $\xi^{\pm}(\tilde{c} : \tilde{d})$ for the missing values of $\tilde{c} : \tilde{d}$. Here formulas (20) and (22) must be considered as equations for the classes $\{0, i\infty\}_N$ and $\{\alpha, i\infty\}_N$, respectively. The coefficients of these classes are computed using e), and the classes in the right side of (20) and (22) are computed as in d).

The curve X_{11}

Equation: $y^2 = t(t^3 - 20t^2 + 56t - 44)$.

$$\gamma^{\pm} = \left\{-\frac{1}{3}, 0\right\} \pm \left\{\frac{1}{3}, 0\right\}.$$

$P^1(\mathbf{Z}/(11))$	1 : 0	0 : 1	1 : 1	2 : 1	3 : 1	4 : 1	5 : 1	6 : 1	7 : 1	8 : 1	9 : 1	10 : 1
y	−2	2	0	10	5	−5	−10	−10	−5	+5	10	0
ξ^+	$\frac{2}{5}$	$-\frac{2}{5}$	0	−2	−1	1	2	2	1	−1	−2	0
ξ^-	0	0	0	0	1	1	0	0	−1	−1	0	0

α	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{1}{6}$	$\frac{1}{7}$	$\frac{2}{7}$	$\frac{3}{7}$	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{9}$	$\frac{2}{9}$	$\frac{4}{9}$	$\frac{1}{10}$	$\frac{3}{10}$	$\frac{1}{12}$	$\frac{5}{12}$
$x^+(\alpha)$	2	1	−1	−2	3	−2	−1	−1	4	1	1	2	−3	2	0	0	0	5
$x^-(\alpha)$	0	1	1	0	1	0	−1	1	0	−1	1	0	1	0	0	2	0	1

α	$\frac{1}{13}$	$\frac{2}{13}$	$\frac{3}{13}$	$\frac{4}{13}$	$\frac{5}{13}$	$\frac{6}{13}$	$\frac{1}{14}$	$\frac{3}{14}$	$\frac{5}{14}$	$\frac{1}{15}$	$\frac{2}{15}$	$\frac{4}{15}$	$\frac{7}{15}$	$\frac{1}{16}$	$\frac{3}{16}$	$\frac{5}{16}$	$\frac{7}{16}$	$\frac{1}{17}$
$x^+(\alpha)$	2	−3	−3	2	2	2	1	−4	1	−1	−1	−1	4	−2	−2	3	3	−2
$x^-(\alpha)$	0	−1	1	2	2	0	1	0	1	1	−1	1	0	0	0	1	−1	0

α	$\frac{2}{17}$	$\frac{3}{17}$	$\frac{4}{17}$	$\frac{5}{17}$	$\frac{6}{17}$	$\frac{7}{17}$	$\frac{8}{17}$	$\frac{1}{18}$	$\frac{5}{18}$	$\frac{7}{18}$	$\frac{1}{19}$	$\frac{2}{19}$	$\frac{3}{19}$	$\frac{4}{19}$	$\frac{5}{19}$	$\frac{6}{19}$	$\frac{7}{19}$	$\frac{8}{19}$
$x^+(\alpha)$	3	−2	−2	−2	3	3	3	−1	−1	4	1	1	−4	−4	1	1	1	6
$x^-(\alpha)$	−1	0	2	2	1	1	−1	−1	1	2	−1	1	0	0	1	1	1	0

α	$\frac{9}{19}$	$\frac{1}{20}$	$\frac{3}{20}$	$\frac{7}{20}$	$\frac{9}{20}$	$\frac{1}{21}$	$\frac{2}{21}$	$\frac{4}{21}$	$\frac{5}{21}$	$\frac{8}{21}$	$\frac{10}{21}$	$\frac{1}{23}$	$\frac{2}{23}$	$\frac{3}{23}$	$\frac{4}{23}$	$\frac{5}{23}$	$\frac{6}{23}$	$\frac{7}{23}$
$x^+(\alpha)$	1	2	−3	2	2	0	0	0	0	0	0	0	0	0	0	−5	0	0
$x^-(\alpha)$	−1	0	−1	2	0	0	0	0	2	2	0	0	0	−2	0	1	2	2

a	$\frac{8}{23}$	$\frac{9}{23}$	$\frac{10}{23}$	$\frac{11}{23}$	$\frac{1}{24}$	$\frac{5}{24}$	$\frac{7}{24}$	$\frac{11}{24}$	$\frac{1}{25}$	$\frac{2}{25}$	$\frac{3}{25}$	$\frac{4}{25}$	$\frac{6}{25}$	$\frac{7}{25}$	$\frac{8}{25}$	$\frac{9}{25}$
$x^+(\alpha)$	0	5	5	0	2	−3	−3	2	1	1	1	−4	1	1	1	1
$x^-(\alpha)$	2	1	−1	0	0	−1	1	0	1	−1	−1	0	1	1	1	1

a	$\frac{11}{25}$	$\frac{12}{25}$	$\frac{1}{26}$	$\frac{3}{26}$	$\frac{5}{26}$	$\frac{7}{26}$	$\frac{9}{26}$	$\frac{11}{26}$	$\frac{1}{27}$	$\frac{2}{27}$	$\frac{4}{27}$	$\frac{5}{27}$	$\frac{7}{27}$	$\frac{8}{27}$	$\frac{10}{27}$	$\frac{11}{27}$
$x^+(\alpha)$	1	1	−1	4	−1	−1	−1	4	−2	3	−2	−2	−2	−2	3	3
$x^-(\alpha)$	−1	1	1	0	−1	1	1	0	0	1	−2	0	2	2	1	1

a	$\frac{13}{27}$	$\frac{1}{28}$	$\frac{3}{28}$	$\frac{5}{28}$	$\frac{9}{28}$	$\frac{11}{28}$	$\frac{13}{28}$	$\frac{1}{29}$	$\frac{2}{29}$	$\frac{3}{29}$	$\frac{4}{29}$	$\frac{5}{29}$	$\frac{6}{29}$	$\frac{7}{29}$	$\frac{8}{29}$	$\frac{9}{29}$
$x^+(\alpha)$	3	−2	3	−2	3	3	3	−1	−1	−1	−1	−1	−1	−1	−1	4
$x^-(\alpha)$	1	0	1	0	1	1	1	−1	1	1	−1	1	−1	1	1	2

a	$\frac{10}{29}$	$\frac{11}{29}$	$\frac{12}{29}$	$\frac{13}{29}$	$\frac{14}{29}$	$\frac{1}{30}$	$\frac{7}{30}$	$\frac{11}{30}$	$\frac{13}{30}$
$x^+(\alpha)$	−1	−1	4	4	4	1	−4	1	6
$x^-(\alpha)$	1	1	2	0	0	−1	2	1	0

Here we only publish the part of the tables compiled for $\Gamma_0(11)$. The values of $x^{\pm}$ were computed for all 11-integral rational numbers with denominators ≤ 83, and also with denominators 19^2 and 29^2 (19 and 29 are supersingular primes for X_{11}).

In these tables $x^+(b/a) \bmod 5$ always depends only on a. In addition, in the tables $|x^+| \leq 9$ and $|x^-| \leq 5$.

The curve X_{17}

Equation: $y^2 + xy = x^3 - 4x^2 + 4x - 15$.

$$\gamma^{\pm} = \left\{-\frac{1}{3}, 0\right\} \pm \left\{\frac{1}{3}, 0\right\}.$$

$P^1(Z(17))$	1 : 0	0 : 1	1 : 1	2 : 1	3 : 1	4 : 1	5 : 1	6 : 1	7 : 1	8 : 1	9 : 1	10 : 1	11 : 1	12 : 1	13 : 1	14 : 1	15 : 1	16 : 1
y	−1	1	0	4	2	0	2	−2	−2	−4	−4	−2	−2	2	0	2	4	0
ξ^+	$\frac{1}{2}$	$-\frac{1}{2}$	0	−2	−1	0	−1	1	1	2	2	1	1	−1	0	−1	−2	0
ξ^-	0	0	0	0	1	0	1	1	1	0	0	−1	−1	−1	0	−1	0	0

a	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{1}{6}$	$\frac{1}{7}$	$\frac{2}{7}$	$\frac{3}{7}$	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{9}$	$\frac{2}{9}$	$\frac{4}{9}$	$\frac{1}{10}$	$\frac{3}{10}$
$x^+(\alpha)$	2	1	0	1	1	−1	−1	−1	3	−2	2	−2	2	2	−1	−1
$x^-(\alpha)$	0	1	0	1	1	1	1	1	1	0	0	0	0	0	−1	1

a	$\frac{1}{11}$	$\frac{2}{11}$	$\frac{3}{11}$	$\frac{4}{11}$	$\frac{5}{11}$	$\frac{1}{12}$	$\frac{5}{12}$	$\frac{1}{13}$	$\frac{2}{13}$	$\frac{3}{13}$	$\frac{4}{13}$	$\frac{5}{13}$	$\frac{6}{13}$	$\frac{1}{14}$	$\frac{3}{14}$	$\frac{5}{14}$
$x^+(\alpha)$	−1	−1	−1	3	3	1	1	0	0	0	0	0	4	1	1	1
$x^-(\alpha)$	−1	1	1	1	1	−1	1	0	0	0	2	0	0	−1	1	1

a	$\frac{1}{15}$	$\frac{2}{15}$	$\frac{4}{15}$	$\frac{7}{15}$	$\frac{1}{16}$	$\frac{3}{16}$	$\frac{5}{16}$	$\frac{7}{16}$
$x^+(\alpha)$	2	−2	−2	2	0	0	0	4
$x^-(\alpha)$	0	0	0	0	0	2	2	0

In these tables $x^+(b/a) \bmod 4$ depends only on a.

The curve X_{19}

Equation: $y^2 = t(t^3 - 16t^2 + 64t + 76)$.

$$\gamma^{\pm} = \left\{-\frac{1}{4}, 0\right\} \pm \left\{\frac{1}{4}, 0\right\}.$$

$P^1(Z(19))$	1 : 0	0 : 1	1 : 1	2 : 1	3 : 1	4 : 1	5 : 1	6 : 1	7 : 1	8 : 1	9 : 1	10 : 1	11 : 1	12 : 1	13 : 1	14 : 1	15 : 1	16 : 1	17 : 1	18 : 1
y	−2	2	0	6	6	3	−3	−6	0	0	−6	−6	0	0	−6	−3	3	6	6	0
ξ^+	$\frac{2}{3}$	$-\frac{2}{3}$	0	−2	−2	−1	1	2	0	0	2	2	0	0	2	1	−1	−2	−2	0
ξ^-	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	−1	−1	0	0	0

a	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{1}{6}$	$\frac{1}{7}$	$\frac{2}{7}$	$\frac{3}{7}$	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{9}$	$\frac{2}{9}$	$\frac{4}{9}$	$\frac{1}{10}$	$\frac{3}{10}$	$\frac{1}{11}$
$x^+(\alpha)$	2	2	1	−1	2	−2	0	3	0	0	0	−2	1	1	−2	4	0
$x^-(\alpha)$	0	0	1	1	0	0	0	1	0	0	0	0	1	1	0	0	0

a	$\frac{2}{11}$	$\frac{3}{11}$	$\frac{4}{11}$	$\frac{5}{11}$	$\frac{1}{12}$	$\frac{5}{12}$	$\frac{1}{13}$	$\frac{2}{13}$	$\frac{3}{13}$	$\frac{4}{13}$	$\frac{5}{13}$	$\frac{6}{13}$	$\frac{1}{14}$	$\frac{3}{14}$	$\frac{5}{14}$	$\frac{1}{15}$	$\frac{2}{15}$
$x^+(a)$	−3	3	0	3	0	0	−2	−2	1	4	1	4	−1	−1	2	1	−2
$x^-(a)$	1	1	0	1	0	0	0	0	1	0	1	0	−1	1	0	−1	0

a	$\frac{4}{15}$	$\frac{7}{15}$	$\frac{1}{16}$	$\frac{3}{16}$	$\frac{5}{16}$	$\frac{7}{16}$	$\frac{1}{17}$	$\frac{2}{17}$	$\frac{3}{17}$	$\frac{4}{17}$	$\frac{5}{17}$	$\frac{6}{17}$	$\frac{7}{17}$	$\frac{8}{17}$	$\frac{1}{18}$	$\frac{5}{18}$	$\frac{7}{18}$
$x^+(a)$	1	4	2	−1	2	−1	2	−1	−1	−1	5	2	2	2	0	3	3
$x^-(a)$	1	0	0	1	0	1	0	1	0	1	1	0	0	0	0	−1	−1

In these tables $x^+(b/a) \bmod 3$ depends only on a.

The curve X_{27}

Equation: $y^2 = 4x^3 + 1$ (curve with complex multiplication).

$$\gamma^{\pm} = \left\{-\frac{1}{4}, 0\right\} \pm \left\{\frac{1}{4}, 0\right\}.$$

$P^1(Z/(27))$	1 : 0	0 : 1	1 : 1	2 : 1	3 : 1	4 : 1	5 : 1	6 : 1	7 : 1	8 : 1	9 : 1	10 : 1	11 : 1	12 : 1
y	−2	2	0	6	3	3	3	0	−3	0	−1	0	−3	−3
ξ^+	$\frac{2}{3}$	$-\frac{2}{3}$	0	−2	−1	−1	−1	0	1	0	$\frac{1}{3}$	0	1	1
ξ^-	0	0	0	0	$\frac{1}{3}$	1	1	$\frac{2}{3}$	1	0	$\frac{1}{3}$	0	1	$\frac{1}{3}$

$P^1(Z/(27))$	13 : 1	14 : 1	15 : 1	16 : 1	17 : 1	18 : 1	19 : 1	20 : 1	21 : 1	22 : 1	23 : 1
y	−6	−6	−3	−3	0	−1	0	−3	0	3	3
ξ^+	2	2	1	1	0	$\frac{1}{3}$	0	1	0	−1	−1
ξ^-	0	0	$-\frac{1}{3}$	−1	0	$-\frac{1}{3}$	0	−1	$-\frac{2}{3}$	−1	−1

$P^1(Z/(27))$	24 : 1	25 : 1	26 : 1	1 : 3	2 : 3	4 : 3	5 : 3	7 : 3	8 : 3	1 : 9	2 : 9
y	3	6	0	−3	3	0	0	3	−3	1	1
ξ^+	−1	−2	0	1	−1	0	0	−1	1	$-\frac{3}{3}$	$-\frac{1}{3}$
ξ^-	$-\frac{1}{3}$	0	0	$\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{2}{3}$	$\frac{2}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$

a	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{1}{7}$	$\frac{2}{7}$	$\frac{3}{7}$	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{10}$	$\frac{3}{10}$	$\frac{1}{11}$	$\frac{2}{11}$	$\frac{3}{11}$	$\frac{4}{11}$	$\frac{5}{11}$	$\frac{1}{13}$
$x^+(a)$	2	1	1	1	−1	2	2	0	0	0	0	−1	−1	2	2	2	−2
$x^-(a)$	0	1	1	1	1	0	0	0	0	0	0	1	1	0	0	0	0

a	$\frac{2}{13}$	$\frac{3}{13}$	$\frac{4}{13}$	$\frac{5}{13}$	$\frac{6}{13}$	$\frac{1}{14}$	$\frac{3}{14}$	$\frac{5}{14}$	$\frac{1}{16}$	$\frac{3}{16}$	$\frac{5}{16}$	$\frac{7}{16}$	$\frac{1}{17}$	$\frac{2}{17}$	$\frac{3}{17}$	$\frac{4}{17}$	$\frac{5}{17}$	$\frac{6}{17}$
$x^+(a)$	1	1	1	1	1	−2	1	1	−1	−1	2	2	0	0	0	0	0	0
$x^-(a)$	1	1	1	1	1	0	1	1	−1	1	0	0	0	0	0	0	0	0

a	$\frac{7}{17}$	$\frac{8}{17}$	$\frac{1}{19}$	$\frac{2}{19}$	$\frac{3}{19}$	$\frac{4}{19}$	$\frac{5}{19}$	$\frac{6}{19}$	$\frac{7}{19}$	$\frac{8}{19}$	$\frac{9}{19}$	$\frac{1}{20}$	$\frac{3}{20}$	$\frac{7}{20}$	$\frac{9}{20}$	$\frac{1}{22}$
$x^+(a)$	3	3	0	0	0	0	3	0	0	3	3	−1	−1	2	2	1
$x^-(a)$	1	1	0	0	0	0	1	0	0	1	1	−1	1	0	0	−1

a	$\frac{3}{22}$	$\frac{5}{22}$	$\frac{7}{22}$	$\frac{9}{22}$	$\frac{1}{23}$	$\frac{2}{23}$	$\frac{3}{23}$	$\frac{4}{23}$	$\frac{5}{23}$	$\frac{6}{23}$	$\frac{7}{23}$	$\frac{8}{23}$	$\frac{9}{23}$	$\frac{10}{23}$	$\frac{11}{23}$
$x^+(a)$	−2	1	1	1	1	−2	−2	1	1	1	1	1	1	1	4
$x^-(a)$	0	1	1	1	−1	0	0	1	1	1	1	1	1	1	0

a	$\frac{1}{25}$	$\frac{2}{25}$	$\frac{3}{25}$	$\frac{4}{25}$	$\frac{6}{25}$	$\frac{7}{25}$	$\frac{8}{25}$	$\frac{9}{25}$	$\frac{11}{25}$	$\frac{12}{25}$	$\frac{1}{26}$	$\frac{3}{26}$	$\frac{5}{26}$	$\frac{7}{26}$	$\frac{9}{26}$	$\frac{11}{26}$
$x^+(a)$	2	−1	−1	−1	−1	2	2	2	2	2	0	0	0	3	0	3
$x^-(a)$	0	1	1	1	1	1	0	0	0	0	0	0	2	1	0	1

In these tables $x^+(b/a) \bmod 3$ depends only on a.

Received 10/OCT/71

BIBLIOGRAPHY

1. A. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. 185 (1970), 134–160.

2. B. J. Birch, *Diophantine analysis and modular functions*, Internat. Colloq. Algebraic Geometry (Tata Inst. Fund. Res., Bombay, 1968), Oxford Univ. Press, London, 1969, pp. 35–42. MR 41 #3478.

3. B. A. Venkov, *Elementary number theory*, ONTI, Moscow, 1937. (Russian)

4. P. Cartier, *Groupes formels, fonctions automorphes et fonctions zeta des courbes elliptiques*, 1970 (preprint).

5. M. Eichler, *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzeta-funktion*, Arch. Math. 5 (1954), 355–366. MR 16, 116.

6. H. Heilbronn, *On the average [illegible]*
and Analysis (Papers in Honor of Edmund Landau), Plenum, New York, 1969, pp. 87–96. MR 41 #3406.

7. P. Lévy, *Théorie de l'addition des variables aléatoires*, Gauthier-Villars, Paris, 1937.

8. G. Ligozat, *Fonctions L des courbes modulaires*, Séminaire Délange-Pisot-Poitou, 1969/70, Exposé 9, Secrétariat mathématique, Paris, 1970.

9. Ju. I. Manin, *Cyclotomic fields and modular curves*, Uspehi Mat. Nauk 26 (1971), no. 6 (162), 7–71 = Russian Math. Surveys 26 (1971), no. 6 (to appear).

10. B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, 1965 (preprint).

11. ——, *Arithmétique des courbes elliptiques sur les corps cyclotomiques (notes de J. F. Boutot)*, Orsay, 1970.

12. A. Ogg, *Modular forms and Dirichlet series*, Benjamin, New York, 1969. MR 41 #1648.

13. J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968. MR 41 #8422.

14. G. Shimura, *A reciprocity law in non-solvable extensions*, J. Reine Angew. Math. 221 (1966), 209–220. MR 32 #5637.

15. P. Swinnerton-Dyer, *The conjectures of Birch and Swinnerton-Dyer, and of Tate*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 132–157. MR 37 #6287.

16. A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. 168 (1967), 149–156. MR 34 #7473.

Translated by N. KOBLITZ