THE EISENSTEIN MEASURE AND P-ADIC INTERPOLATION

By Nicholas M. Katz

Introduction. This paper grew out of an attempt to understand the arithmetic properties of the Hurwitz numbers [2, 3], particularly the possibility of their "p-adic interpolation" in the style of Kubota-Leopoldt [8]. We are successful precisely "half the time", for those primes $p \equiv 1$ (4). The very nature of our approach, which is an *amalgamation* of the approaches of Serre and Mazur-Swinnerton-Dyer, seems to make it inapplicable to primes $p \equiv 3$ (4).

The basic idea is this. The archtypical case of successful p-adic interpolation is that of the Bernoulli numbers, which in Serre's approach [18] appear as the constant terms of the q-expansions of certain Eisenstein series. On the other hand, the Hurwitz numbers are essentially the *values* of the same Eisenstein series, but at the lemniscatic elliptic curve (multiplication by $\mathbf{Z}[i]$) rather than at $q = 0$, the degenerate "elliptic curve at ∞". The common feature of the lemniscate curve for $p \equiv 1$ (4) and of the "curve at ∞" is that they both have *ordinary* reduction, i.e. their formal groups become isomorphic to the formal multiplicative group at least after a highly non-trivial extension of scalars.

So more generally one might consider "trivialized elliptic curves", namely pairs (E, φ) consisting of an elliptic curve E over a p-adically complete ground-ring together with an isomorphism φ of the formal group of E with the formal multiplicative group. Then any usual modular form (say with p-integral q-expansion) may be viewed as a "function" of trivialized elliptic curves. In this context, it is natural to ask if it is possible to p-adically interpolate the values of the Eisenstein series at *any* trivialized elliptic curve.

We show that this is in fact the case. The main technical tool upon which we rely is the theory of the p-adic Mellin transform ([13], [15]), which assures us that p-adic interpolation of a given sequence of p-adic numbers is equivalent to the existence of a *p-adic measure* on $\mathbf{Z}_p$ such that these numbers are the integrals of the power functions $x \mapsto x^k$. In fact, we

Manuscript received May 30, 1974.

American Journal of Mathematics, Vol. 99, No. 2, pp. 238–311.

simultaneously construct the needed p-adic measures for *all* trivialized elliptic curves by constructed a *single* measure on $\mathbf{Z}_p$ with values in the p-adic Banach space of *all* generalized modular functions (i.e. functions of trivialized elliptic curves), such that the integral of $x \to x^k$ is the k'th Eisenstein series. This measure we propose to call the "Eisenstein measure". (A note to analysts: if one thinks of trivialized elliptic curves as the test objects, then generalized modular functions become the distributions, and the Eisenstein measure becomes a distribution-valued measure.)

Thus we attach a p-adic zeta function to *any* trivialized elliptic curve. In the case of the degenerate elliptic curve at ∞ ($q = 0$), it is the Kubota-Leopoldt p-adic zeta function (and so this paper provides yet another construction of that function). In the case of a complex multiplication curve, (although to fix ideas we treat only the lemniscate curve in detail), we relate the values of our zeta function to the values of the classical "L-series with grossencharacter" at $s = 0$ for the *powers* of the canonical grossencharacter to which the curve gives rise. In the case of a curve over $\mathbf{Q}$ without complex multiplication which admits a Weil parameterization, we do *not* know the classical meaning of our zeta function, and in particular we do *not* know its relation to the p-adic L-series which Mazur and Swinnerton-Dyer [15] and Manin [11] attach to such a curve by their theory of the "modular symbol".

For the sake of completeness, we have worked systematically "with level", especially with $\Gamma_{00}(N)$. This allows us to give an a priori construction of the Kubota-Leopoldt L-series $L(s, \chi)$ with χ *any* Dirichlet character; sticking to level one would have meant restricting χ to have conductor a power of p. In any earlier version, the construction of the Eisenstein measure made use of the existence of the Kubota-Leopoldt zeta function. I owe to Deligne the idea of eliminating this dependence by systematic use of the "Key Lemma" (1.2.1-3). It is a pleasure to record my gratitude to him.

In fact, in a recent (Dec., 1973) unpublished letter of Deligne to Serre, Deligne has explained how to prove the "good" congruences for the Dirichlet L-series of a totally real number field, once one knows the irreducibility mod p of certain moduli problems for abelian varieties with "real multiplication" by that field. In the case of the rational field Q, the moduli problem in question is precisely that of trivialized elliptic curves with $\Gamma_{00}(N)$ structure, and so this paper may be read as an overlong introduction to Deligne's letter.

We have added several appendices. In the first, we recall Hurwitz's form of the functional equation of Dirichlet L-series, which we need (cf.

2.4) to compute the constant terms of the Eisenstein series as *values* of L functions. The second appendix is a brief recapitulation of the entire paper in a context more suitable to the p-adic interpolation of the L-series associated to complex multiplication curves—the point is that $\Gamma(N)$ is to a quadratic imaginary field as $\Gamma_{00}(N)$ is to Q. The final (!) appendix answers the question raised in 2.8 about the modular meaning of Eisenstein series of weight one.

Table of Contents

---

1. Generalized Modular Functions on $\Gamma(N)$ and on $\Gamma_\infty(N)$.

1.1 Basic Definitions. Fix a prime number p, and an integer $N \geq 1$ prime to p. In case $p = 2$ or $p = 3$, we require $N \geq 3$. Let k be a perfect field of characteristic p containing a primitive N'th root of unity ζ_0. Denote by W the Witt vectors of k, and by $\zeta \in W$ the unique N'th root of unity lifting ζ_0.

A trivialized elliptic curve of level N is a triple $(E/B, \varphi, \alpha_N)$ consisting of

an elliptic curve E over a p-adically complete and separated W-algebra B

a "trivialization" of the formal group of E by an isomorphism $\varphi: \hat{E} \xrightarrow{\sim} (\hat{G}_m)_B$

a level N structure $\alpha_N: {}_NE \xrightarrow{\sim} (\mathbf{Z}/N\mathbf{Z})_B{}^2$ of determinant ζ.

A generalized modular function on $\Gamma(N)$ is a rule f which assigns to any trivialized elliptic curve of level N $(E/B, \varphi, \alpha_N)$ a "value" $f(E/B, \varphi, \alpha_N) \in B$, subject to the following two conditions:

1. $f(E/B, \varphi, \alpha_N)$ depends only on the B-isomorphism class of $(E/B, \varphi, \alpha_N)$, and its formation commutes with arbitrary extension of scalars $B \to B'$ of p-adically complete and separated W-algebras.
2. Denote by $W((q))$ the p-adic completion of $W((q))$; then $f(\mathrm{Tate}(q^N)/W((q)), \varphi, \alpha_N)$ lies in the subring $W[[q]]$ of $W((q))$ for

every choice of φ and of α_N. These series are called the q-expansions of f.

(We should remark that the *construction* of the Tate curve makes evident a *canonical* choice φ_{can} of φ, such that any other φ may be uniquely written $a\varphi$ with $a \in \mathbf{Z}_p^{\times}$; thus all φ's are in fact defined over $W((q))$.)

For any p-adically complete W-algebra B_0, we may define the notion of a generalized level N modular function defined over B_0 by restricting attention to trivialized level N curves $(E/B, \varphi, \alpha_N)$ over p-adically complete B_0-algebras B, and requiring that $f(\text{Tate}(q^N)/B_0((q)), \varphi, \alpha_N)$ lie in $B_0[[q]]$ for all choices of φ and α_N.

Let $V(B_0, \Gamma(N))$ denote the p-adically complete ring of all generalized level N modular functions defined over B_0, and let $R^{\cdot}(B_0, \Gamma(N))$ denote the (graded) ring of all "true" modular forms on $\Gamma(N)$ defined over B_0. In a natural way, $R^{\cdot}(B_0, \Gamma(N))$ maps to $V(B_0, \Gamma(N))$: a true modular form f gives rise to the generalized modular function $\tilde{f}$ defined by

$$\tilde{f}(E/B, \varphi, \alpha_N) = f(E/B, \varphi^*(dT/1 + T), \alpha_N)$$

where T is the standard parameter on $\hat{G}_m$, $dT/1 + T$ is the standard invariant differential on $\hat{G}_m$, and where $\varphi^*(dT/1 + T)$ denotes the unique invariant differential on E/B whose restriction to $\hat{E}$ is $\varphi^*(dT/1 + T)$. On the Tate curve, we have $\varphi^*_{\text{can}}(dT/1 + T) = \omega_{\text{can}}$, hence

$$\tilde{f}(\text{Tate}(q^N)/B_0((q)), \varphi_{\text{can}}, \alpha_N) = f(\text{Tate}(q^N)/B_0((q)), \omega_{\text{can}}, \alpha_N).$$

As α_N runs over all level N-structures, the right hand side runs over all the q-expansions of f as true modular form. Thus if we fix the weight of f, it is uniquely determined by $\tilde{f}$ (thanks to the q-expansion principle), in other words $f \mapsto \tilde{f}$ is injective on the space of modular forms of each given weight, but *unless* B_0 is *flat* over W, the ring homomorphism $R^{\cdot}(B_0, \Gamma(N)) \to V(B_0, \Gamma(N))$ will not be injective. (The determination of the kernel for $B_0 = W/p^{\nu}W$, any ν, is the subject of [7].)

The groups $G = SL_2(\mathbf{Z}/N\mathbf{Z})$ and $\mathbf{Z}_p^{\times}$ act on the rings $R^{\cdot}(B_0, \Gamma(N))$ and $V(B_0, \Gamma(N))$ in the following way:

$$[g]f(E/B, \omega, \alpha_N) = f(E/B, \omega, g^{-1} \circ \alpha_N) \qquad g \in G, \quad f \in R^{\cdot}(B, \Gamma(N))$$

$$[a]f(E/B, \omega, \alpha_N) = f(E/B, a^{-1}\omega, \alpha_N) \qquad a \in Z_p^{\times}, \quad f \in R^{\cdot}(B, \Gamma(N))$$

$$[g]f(E/B, \varphi, \alpha_N) = f(E/B, \varphi, g^{-1} \circ \alpha_N) \qquad g \in G, \quad f \in V(B_0, \Gamma(N))$$

$$[a]f(E/B, \varphi, \alpha_N) = f(E/B, a^{-1}\varphi, \alpha_N) \qquad a \in Z_p^{\times}, \quad f \in V(B_0, \Gamma(N))$$

These actions commute with each other, and under them the homomorphism $R^{\cdot}(B_0, \Gamma(N)) \to V(B_0, \Gamma(N))$ is *equivariant*. An element $f \in V(B_0, \Gamma(N))$ is said to have weight $\chi \in \mathrm{Hom}_{\mathrm{contin}}(\mathbf{Z}_p^\times, B_0^\times)$ if it satisfies

$$[a]f = \chi(a)\cdot f \qquad \text{for all} \quad a \in \mathbf{Z}_p^\times.$$

Observe that the image in $V(B_0, \Gamma(N))$ of a true modular forms of usual weight k has weight χ_k, where $\chi_k(a)$ = "a^k viewed as an element of B_0". When B_0 is flat over W, a generalized modular function admits at most *one* weight (though of course most have no weight).

A generalized modular function of level N defined over B_0 is said to be "on $\Gamma_{00}(N)$" if it is *invariant* under the subgroup

$$U = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| \, x \in \mathbf{Z}/N\mathbf{Z} \right\} \quad \text{of} \quad SL(2, \mathbf{Z}/N\mathbf{Z}).$$

In concrete terms, f is on $\Gamma_{00}(N)$ if

$$f(E/B, \varphi, \alpha_N) = f(E/B, \varphi, \alpha_N{}')$$

whenever

$$\alpha_N{}^{-1}(1, 0) = (\alpha_N{}')^{-1}(1, 0).$$

Equivalently, a generalized modular function on $\Gamma_{00}(N)$ is a "function" of triples $(E/B, \varphi, P)$ consisting of a trivialized elliptic curve together with a section P of order exactly N (i.e. order exactly N at every point of $\mathrm{Spec}(B)$), whose q-expansions $f(\mathrm{Tate}(q^N)/B_0((q)), \varphi, P)$ all lie in $B_0[[q]]$. The "standard" q-expansion of a generalized modular function will be its value on $(\mathrm{Tate}(q)/B_0((q)), \varphi_{\mathrm{can}}, \zeta)$, where ζ denotes the point of order exactly N on $\mathrm{Tate}(q)$ obtained from the given N'th root of unity $\zeta \in W$ by viewing $\mathrm{Tate}(q)$ as a suitable quotient of G_m.

We denote by $V(B_0, \Gamma_{00}(N))$ the p-adically complete ring $V(B_0, \Gamma(N))^U$ of generalized modular functions on $\Gamma_{00}(N)$. The action of $\mathbf{Z}_p^\times$ respects $V(B_0, \Gamma_{00}(N))$. The action of the *diagonal* subgroup of $G = SL_2(\mathbf{Z}/N\mathbf{Z})$ respects $V(B_0, \Gamma_{00}(N))$, where it is more conveniently written as an action of $(\mathbf{Z}/N\mathbf{Z})^\times$; defined by

$$[b]f(E, \varphi, P) = f(E, \varphi, bP) \qquad \text{for} \quad b \in (\mathbf{Z}/N\mathbf{Z})^\times.$$

An element f of $V(B_0, \Gamma_{00}(N))$ is said to be of "nebentypus" $\epsilon \in \mathrm{Hom}((\mathbf{Z}/N\mathbf{Z})^\times, B_0^\times)$ if $[b]f = \epsilon(b)f$ for all $b \in (\mathbf{Z}/N\mathbf{Z})^\times$.

Analogously, we denote by $R^{\cdot}(B_0, \Gamma_{00}(N))$ the ring of true modular forms defined over B_0 on $\Gamma_{00}(N)$, defined as the invariants of U in $R^{\cdot}(B_0, \Gamma(N))$. Thus the homomorphism $R^{\cdot}(B_0, \beta(N)) \to V(B_0, \Gamma(N))$ restricts to a $\mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$-equivariant homomorphism $R^{\cdot}(B_0, \Gamma_{00}(N)) \to V(B_0, \Gamma_{00}(N))$.

1.2 Review of the Main Congruence Properties. For any p-adically complete ground-ring B_0, we have $V(B_0, \Gamma(N)) = V(W, \Gamma(N)) \hat{\otimes}_W B_0$ and $V(B_0, \Gamma_{00}(N)) = V(W, \Gamma_{00}(N)) \hat{\otimes}_W B_0$. The important case is $B_0 = W/p^n W$.

Over any p-adically complete ground-ring B_0, any choice of φ, α_N on the Tate curve gives an *injective* q-expansion homomorphism

$$\begin{array}{c} V(B_0, \Gamma(N)) \to B_0[[q]] \\ \cup \\ V(B_0, \Gamma_{00}(N)) \end{array}$$

Applying the results to the rings $B_0 = W/p^n W$, we immediately see that over W, the cokernels $W[[q]]/V(W, \Gamma(N))$ and $W[[q]]/V(W, \Gamma_{00}(N))$ are *flat* over W. In concrete terms, this means that a generalized modular function on $\Gamma(N)$ (resp. on $\Gamma_{00}(N)$) is divisible by p in the ring $V(W, \Gamma(N))$ (resp. in $V(W, \Gamma_{00}(N))$ if and only if at least *one* of its q-expansions is divisible by p in $W[[q]]$. [In particular, if *one* q-expansion is divisible by p, then all are!]

Let $D(W, \Gamma(N))$ (resp. $D(W, \Gamma_{00}(N)))$ denote the subring of $R^{\cdot}(W[1/p], \Gamma(N))$ (resp. of $R^{\cdot}(W[1/p], \Gamma_{00}(N)))$ consisting of elements Σf_i such that for one (and hence for every) choice of q-expansion, $\Sigma f(q)$ lies in $W[[q]]$; the elements of D are the "divided congruences" of [7]. The inclusions $R^{\cdot}(W, \Gamma(N)) \subset V(W, \Gamma(N))$ and $R^{\cdot}(W, \Gamma_{00}(N)) \subset V(W, \Gamma_{00}(N))$ extend to inclusions

$$D(W, \Gamma(N)) \subset V(W, \Gamma(N))$$

$$D(W, \Gamma_{00}(N)) \subset V(W, \Gamma_{00}(N)).$$

Let us recall how these inclusions come about. If Σf_i is a sum of true modular forms over $W[1/p]$ such that for some choice of cusp the q-expansion $\Sigma f_i(q)$ is integral, i.e. lies in $W[[q]]$, then for $n \gg 0$, $\Sigma p^n f_i$ is a sum of true modular forms over W, and gives rise to an element $\Sigma p^n \tilde{f}_i$ of V one of whose q-expansions is divisible by p^n. But then this element is uniquely divisible by p^n in V, and dividing it by p^n gives the desired image in V of the element Σf_i in D.

1.2.1 Key Lemma for $\Gamma(N)$. *Let $\Sigma f_i \in R^{\cdot}(W[1/p], \Gamma(N))$ be a sum of true modular forms on $\Gamma(N)$, defined over $W[1/p]$. Suppose that at some cusp, the q-expansion $\Sigma f_i(q)$ is integral* except *possibly for its constant term, i.e.*

$$\sum f_i(q) \in W[1/p] + W[[q]].$$

Let (a, g) *be any element of* $\mathbf{Z}_p^\times \times SL_2(\mathbf{Z}/N\mathbf{Z})$ *and denote by* $f \mapsto [a, g]f$ *its canonical action on* $R^{\cdot}(W[1/p], \Gamma(N))$. *Then the difference*

$$\sum f_i - [a, g] \sum f_i \in D(W, \Gamma(N)),$$

i.e. $\Sigma f_i - \Sigma [a, g] f_i$ *has* integral *q-expansion.*

Proof. For $n \gg 0$, $\Sigma p^n f_i$ lies in $R^{\cdot}(W, \Gamma(N))$, and there exists a constant $A \in W$ such that $\Sigma p^n f_i - A$ has one of its q-expansions divisible by p^n. Hence $\Sigma p^n f_i - A$ lies in $p^n D$. Applying the automorphism $[a, g]$ of D, we see that $[a, g] \Sigma p^n f_i - [a, g] A = p^n \Sigma [a, g] f_i - A$ lies in $p^n D$. Subtracting, we find that $p^n \Sigma f_i - p^n \Sigma [a, g] f_i$ lies in $p^n D$, and hence that $\Sigma f_i - \Sigma [a, g] f_i$ lies in D.

1.2.2 Key Lemma for $\Gamma_{00}(N)$. *Let* $\Sigma f_i \in R^{\cdot}(W[1/p], \Gamma_{00}(N))$ *be a sum of true modular forms on* $\Gamma_{00}(N)$, *defined over* $W[1/p]$. *Suppose that one of the q-expansions* $\Sigma f_i(q)$ *is integral except possibly for its constant term. Then for any element* $(a, b) \in \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$, *the difference*

$$\sum f_i - [a, b] \sum f_i$$

lies in $D(W, \Gamma_{00}(N))$.

Proof. The same.

1.2.3 Alternate Version of the Key Lemma. *Let* f *be an arbitrary element of* $V(W, \Gamma(N)) \otimes_W W[1/p]$ (*resp. of* $V(W, \Gamma_{00}(N)) \otimes_W W[1/p]$), *and suppose that one of the q-expansions of* f *is integral except possibly for its constant term. Let* (a, g) (*resp.* (a, b)) *be any element of* $\mathbf{Z}_p^\times \times SL_2(\mathbf{Z}/N\mathbf{Z})$ (*resp.* $\mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$). *Then the difference* $f - [a, g]f$ (*resp.* $f - [a, b]f$) *has integral q-expansion and hence lies in* $V(W, \Gamma(N))$ (*resp.* $V(W, \Gamma_{00}(N))$).

Proof. Again the same.

1.3 The Frobenius Endomorphism of $V(B_0, \Gamma_{00}(N))$. Let $(E/B, \varphi)$ be a trivialized elliptic curve. Recall that the *canonical subgroup* E_{can} of E is the kernel of multiplication by p in the formal group $\hat{E}$ of E, which by means of φ is identified with $\boldsymbol{\mu}_p \subset \hat{G}_m$. Let us denote by

$$\pi\colon \quad E \to E/E_{\mathrm{can}}$$

the projection onto the quotient, and by

$$\check{\pi}\colon \quad E/E_{\mathrm{can}} \to E$$

the *dual* isogeny. Then $\check{\pi}$ is *étale*, so in particular induces an isomorphism between the formal groups of E/E_{can} and E.

If in addition we are given a point P on E (i.e. a section of $E \to \operatorname{Spec}(B)$) of order exactly N, then the point $\pi(P)$ on E/E_{can} also has order precisely N, because π is an isogeny of degree p prime to N.

Let's examine what happens with the Tate curve $\operatorname{Tate}(q^N)$. The canonical subgroup *is* μ_p, and the p-th endomorphism of $\mathbf{G}_m$ induces the desired isogeny π: $\operatorname{Tate}(q^N) = \mathbf{G}_m/q^{N\mathbf{Z}} \xrightarrow{x \to x^p} \mathbf{G}_m/q^{pN\mathbf{Z}} = \operatorname{Tate}(q^{Np})$. The dual isogeny $\check{\pi}$ is simply passage to the quotient by the subgroup of $\operatorname{Tate}(q^{Np})$ generated by q^N. It follows that for any trivialization φ of $\operatorname{Tate}(q^N)$, the trivialization $\varphi \circ \check{\pi}$ of $\operatorname{Tate}(q^{Np})$ is the one deduced from φ by the extension of scalars $W((q)) \xrightarrow{q \to q^p} W((q))$. If P is the point $\zeta^n q^m$ on $\operatorname{Tate}(q^N)$, then $\pi(P)$ is the point $\zeta^{np}q^{mp}$ on $\operatorname{Tate}(q^{Np})$, and thus $\pi(P)$ is the point of $\operatorname{Tate}(q^{Np})$ deduced from the point $\zeta^{np}q^m$ of Tate (q^N) by the same extension of scalars $q \mapsto q^p$ of W-algebras. Putting this all together, we find that

$$(\operatorname{Tate}(q^N)/\text{canonical subgroup}, \varphi \circ \check{\pi}, \pi(\zeta^n q^m))$$

is deduced by the extension of scalars $W((q)) \xrightarrow{q \to q^p} W((q))$ from

$$(\operatorname{Tate}(q^N), \varphi, \zeta^{np}q^m)$$

Thus we may define the Frobenius endomorphism

$$\text{Frob:} \quad V(B_0, \Gamma_{00}(N)) \to V(B_0, \Gamma_{00}(N))$$

by defining

$$(\operatorname{Frob} f)(E, \varphi, P) = f(E/E_{\text{can}}, \varphi \circ \check{\pi}, \pi(P)).$$

Its effect on q-expansion is thus given by the formula

$$(\operatorname{Frob} f)(\operatorname{Tate}(q^N), \varphi, \zeta^n q^m)$$
$$= \text{the image under } q \mapsto q^p \text{ of } f(\operatorname{Tate}(q^N), \varphi, \zeta^{np}q^m); \quad (1.3.1)$$

in particular, for the "standard" cusp $(\operatorname{Tate}(q), \varphi, \zeta^n)$, we have

$$(\operatorname{Frob} f)(\operatorname{Tate}(q), \varphi, \zeta^n)$$
$$= \text{the image under } q \to q^p \text{ of } f(\operatorname{Tate}(q), \varphi, \zeta^{np}). \quad (1.3.2)$$

1.4 A Technical Remark. We have viewed the $\Gamma_{00}(N)$ moduli problem, that of "classifying" elliptic curves together with a point of order exactly N, as a quotient of the $\Gamma(N)$ moduli problem, that of classifying elliptic curves together with a level N structure of fixed determinant. As a result, we seem to be stuck with choosing an N'th root of unity before discussing the $\Gamma_{00}(N)$ problem.

In fact, there are *two distinct* moduli problems we can consider which are defined over $\mathbf{Z}$, which both become isomorphic to "our" $\Gamma_{00}(N)$ moduli problem when we adjoin an N'th root of unity and invert N. They are

1. elliptic curves E plus injections $\mathbf{Z}/N\mathbf{Z} \to \mathrm{Ker}(N)$ in E
2. elliptic curves E plus injections $\boldsymbol{\mu}_N \to \mathrm{Ker}(N)$ in E

For purposes of maximizing "rationality", the *second* problem is in fact preferable, simply because the *construction* of the Tate curve $\mathrm{Tate}(q)$ over $\mathbf{Z}((q))$ as a suitable kind of quotient of $\mathbf{G}_m$ makes evident a *canonical* inclusion i_{can}: $\boldsymbol{\mu}_N \to \mathrm{Ker}(N)$ in $\mathrm{Tate}(q)$. Thus the "standard" cusp $(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta)$ on the *first* $\Gamma_{00}(N)$ problem, is defined explicitly in terms of a chosen ζ; it may be "replaced" by the cusp $(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, i_{\mathrm{can}})$ of the *second* $\Gamma_{00}(N)$ moduli problem, which is defined over $\mathbf{Z}_p$. In this way, we may "modularly" interpret an element $f \in V(W, \Gamma_{00}(N))$ whose q-expansion at the standard cusp lies in $\mathbf{Z}_p[[q]]$ as a generalized modular form on $\Gamma_{00}(N)$ in the *second* sense, which is defined over $\mathbf{Z}_p$.

1.5 Modular Forms on $\Gamma_{00}(p^n)$ as Generalized Modular Forms. Let us recall the notion of a modular form on $\Gamma_{00}(p^n)$ of level N ($(p, N)=1$) over $\mathbf{Q}(\zeta_N)$. It is a "function" of quadruples $(E/B, \omega, \rho, \alpha_N)$

B	a $\mathbf{Q}(\zeta_N)$-algebra
E	an elliptic curve
ω	a nowhere vanishing differential on E
ρ	an injection $\boldsymbol{\mu}_{p^n} \to \mathrm{Ker}(p^n)$ in E
α_N	a level N structure of determinant ζ

with values in B which satisfies the usual rules for a modular form (cf. [6], 1.2), namely holomorphic q-expansions and commutation with extensions of scalars $B \to B'$. [As soon as B contains a primitive p^n'th root of unity (i.e. an isomorphism of $(\boldsymbol{\mu}_{p^n})_B \simeq (\mathbf{Z}/p^n\mathbf{Z})_B$, the data of ρ is equivalent to the giving of a point of order exactly p^n on E.]

Now consider the "universal" trivialized elliptic curve with level N structure (E, φ, α_N), whose ground-ring of definition is the p-adic completion of the "finite part" of $V(W, \Gamma_{00}(N))$ (eg, the p-adic completion of $V(W, \Gamma_{00}(N))[1/\Delta]$, where Δ is Ramanujam's cusp form $\Sigma_{n\geq 1} \tau(n)q^n$).

Then the quadruple $(E, \varphi^*(dT/T), \varphi^{-1}|\boldsymbol{\mu}_{p^n} \simeq \hat{E}_{p^n}, \alpha_N)$, viewed over $V(W, \widehat{\Gamma_{00}(N))[1/\Delta]} \otimes_W W[1/p]$ is an admissible point of evaluation for any modular form on $\Gamma_{00}(p^n)$ of level N. Evaluating there, we obtain a ring homomorphism

$$\text{level } N \text{ modular forms on } \Gamma_{00}(p^n), \rightarrow V(W, \widehat{\Gamma(N))[1/\Delta]} \underset{W}{\otimes} W[1/p]$$

defined over $W[1/p]$

which is necessarily injective, because it carries evaluation at (Tate(q^N), φ_{can}, α_N) to evaluation at (Tate(q^N), ω_{can}, $i_{\text{can}} : \mu_{p^n} \rightarrow \text{Ker}(p^n)$, α_N) .

If we restrict to the invariants of the group $U = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \subset SL_2(\mathbf{Z}/N\mathbf{Z})$, we get a ring homomorphism, again injective,

$$\text{modular forms on } \Gamma_{00}(Np^n) \rightarrow V(W, \widehat{\Gamma_{00}(N))[1/\Delta]} \underset{W}{\otimes} W[1/p],$$

defined over $W[1/p]$

which carries evaluation at (Tate(q), φ_{can}, ζ) to evaluation at (Tate(q), φ_{can}, i_{can}: $\boldsymbol{\mu}_{p^n} \rightarrow \text{Ker}(p^n)$, ζ).

LEMMA 1.5.1. *The above homomorphisms actually have values in* $V(W, \Gamma(N)) \otimes W[1/p]$ *and* $V(W, \Gamma_{00}(N)) \otimes W[1/p]$ *respectively. If f is a modular form on $\Gamma_{00}(p^n)$ of level N (resp. on $\Gamma_{00}(Np^n)$) whose q-expansion at one of the cusps (Tate (q^N), ω_{can}, i_{can}, α_N) (resp. (Tate(q), ω_{can}, i_{can}, ζ)) lies in $W[[q]]$, then it defines an element of $V(W, \Gamma(N))$ (resp. of $V(W, \Gamma_{00}(N))$ with the* "same" *q-expansion.*

Proof. Modularly, the formal scheme given by $V(W, \widehat{\Gamma(N))[1/\Delta]}$ is just the open set "the *finite* part" of the formal scheme given by $V(W, \Gamma(N))$. (In the notations of [7], we have

$$V(W, \widehat{\Gamma(N))[1/\Delta]} \underset{W}{\otimes} W/p^mW = \underset{\vec{n}}{\lim} \text{ (the coordinate ring of } T^0_{m,n}).)$$

This implies (just as for $V(W, \Gamma(N))$) that any q-expansion homomorphism

$$V(W, \widehat{\Gamma(N))[1/\Delta]} \rightarrow \widehat{W((q))}$$

is *injective*, and has W-flat cokernel.

By the principle of bounded denominators ([6], p. 161), if we replace f by $p^\nu f$ for $\nu \gg 0$, it will have at least one of its q-expansions in $W[[q]]$. Thus its image in $V(W, \widehat{\Gamma(N))[1/\Delta]} \otimes W[1/p]$ will lie in $V(W, \widehat{\Gamma(N))[1/\Delta]}$. But modularly, this last ring is the ring of all generalized modular functions on

$\Gamma(N)$ which are not necessarily holomorphic at the cusps. By hypothesis, the q-expansions of f all lie in $W[1/p][[q]] \cap \widehat{W((q))} = W[[q]]$, and thus f lands in $V(W, \Gamma(N))$.

The $\Gamma_{00}(N)$ case is immediately deduced, by passing to invariants of the subgroup $U = \left\{\begin{pmatrix}1 & * \\ 0 & 1\end{pmatrix}\right\} \subset SL_2(\mathbf{Z}/N\mathbf{Z})$.

2. Eisenstein Series.

This section provides a leisurely review of Eisenstein series with level, from both an analytic and, where possible, an algebraic, point of view. The principal facts we are aiming at are the following.

2.1 Statement of Results.

2.1.1 Let $k \geq 1$ be an integer. Let f be a periodic function $f\colon \mathbf{Z} \to \mathbf{Z}$ of parity k ($f(-x) = (-1)^k f(x)$) which admits the period N. In the (exceptional) case $k = 2$, suppose also that $f(0) = 0$. Then there is a true modular form $G_{k,f}$ on $\Gamma_{00}(N)$ of weight k whose q-expansion at the standard cusp $(\mathrm{Tate}(q), \omega_{\mathrm{can}}, i_{\mathrm{can}}\colon \boldsymbol{\mu}_N \to \mathrm{Ker}(N))$ is

$$G_{k,f}(q) = \tfrac{1}{2}L(1-k, f) + \sum_{n\geq 1} q^n \sum_{d\mid n} d^{k-1}f(d)$$

where $L(1-k, f)$ denotes the value at $s = 1-k$ of the L-series

$$L(s, f) = \sum_{n\geq 1} f(n)\cdot n^{-s}.$$

2.1.2 If we fix a prime p and an integer $N \geq 1$ prime to p, then for any periodic function $f\colon \mathbf{Z} \to \mathbf{Z}$ of parity k which admits the period Np^n for some $n \geq 0$, there is a generalized p-adic modular form $G_{k,f} \in V(W, \Gamma_{00}(N)) \otimes W[1/p]$ whose q-expansion at the standard cusp $(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta)$ is

$$G_{k,f}(q) = \tfrac{1}{2}L(1-k, f) + \sum_{n\geq 1} q^n \sum_{d\mid n} d^{k-1}f(d)$$

Let us explain briefly how 2.1.2 follows directly from 2.1.1. As we have already explained, a true modular form on $\Gamma_{00}(Np^n)$ "is" a generalized modular form on $\Gamma_{00}(N)$ with the same q-expansion. The only remaining point is that for $k = 2$, we no longer require $f(0) = 0$, i.e. we allow the constant function $f = 1$. This is possible because the series

$$G_2(q) = -\frac{1}{24} + \sum_{n\geq 1} q^n \sum_{d\mid n} d = \tfrac{1}{2}\zeta(-1) + \sum_{n\geq 1} q^n \sum_{d\mid n} d$$

is the q-expansion of a generalized modular form of weight two on $SL_2(\mathbf{Z})$ for any prime p (cf. [6], 4.5.4 for a proof).

2.2 Over C. Let $(E/\mathbf{C}, \omega, P)$ be a triple consisting of an elliptic curve $E/\mathbf{C}$, a non-zero invariant differential ω on E, and a point P on E of finite order. Viewed analytically, this triple is equivalent to a pair (L, ℓ_0) consisting of a *lattice* $L \subset \mathbf{C}$ and an element $\ell_0 \in (L \otimes_{\mathbf{Z}} \mathbf{Q})/L$. The equivalence is given explicitly by

$(L, \ell_0) \mapsto E$: the elliptic curve $\mathbf{C}/L$

ω: the invariant differential dz (z the standard parameter on $\mathbf{C}$)

P: the image of ℓ_0 in $\mathbf{C}/L$

$(E, \omega, P) \mapsto L$: the lattice $\left\{\int_\gamma \omega \mid \gamma \in H_1(E, \mathbf{Z})\right\}$ of *periods* of ω

$$\ell_0\text{: the class modulo } L \text{ of } \int_0^P \omega \text{ taken over } any \text{ path} \tag{2.2.1}$$

On the other hand, we recall that for any $Z[1/6]$-algebra B, if we are given an elliptic curve with nowhere-vanishing differential (E, ω) over B, then there are uniquely determined meromorphic functions $X = X(E, \omega)$ and $Y = Y(E, \omega)$ on E which are holomorphic except for second and third order poles respectively along the identity section "∞", in terms of which (E, ω) is given by a Weierstrass equation as a plane cubic:

$$(E, \omega) = (Y^2 = 4X^3 - g_2X - g_3,\ \omega = dX/Y).$$

Over $\mathbf{C}$, the meromorphic function X on E becomes the Weierstrass $\mathcal{P}$-function on $\mathbf{C}/L$

$$X = \mathcal{P}(z; L) = \frac{1}{z^2} + \sum_{\ell \in L - \{0\}} \left(\frac{1}{(z+\ell)^2} - \frac{1}{\ell^2}\right), \tag{2.2.2}$$

the meromorphic function Y becomes $\mathcal{P}' = \dfrac{d\mathcal{P}}{dz}$;

$$Y = \mathcal{P}'(z, L) = -2 \sum_{\ell \in L} \frac{1}{(z+\ell)^3} \tag{2.2.3}$$

and the differential ω becomes dz:

$$\omega = dX/Y = d\mathcal{P}/\mathcal{P}' = dz. \tag{2.2.4}$$

The Eisenstein series $A_k(L, \ell_0)$ are defined analytically for integers k

≥ 3 by the formulas

$$A_k(L, \ell_0) = \sum_{\substack{w \in L\otimes\mathbf{Q}-\{0\} \\ w \equiv \ell_0 \bmod L}} \frac{1}{w^k}$$

$$= \begin{cases} \displaystyle\sum_{\ell \in L-\{0\}} \frac{1}{\ell^k} & \text{if} \quad \ell_0 \equiv 0 \bmod L \\ \\ \displaystyle\sum_{\ell \in L} \frac{1}{(\ell + \ell_0)^k} & \text{if} \quad \ell_0 \not\equiv 0 \bmod L \end{cases} \tag{2.2.5}$$

In case $\ell_0 \equiv 0 \bmod L$, we sometimes write $A_k(L)$ instead of $A_k(L, \ell_0)$. Notice that $A_k(L, -\ell_0) = (-1)^k A_k(L, \ell_0)$.

These series are closely tied up with the values of the $\mathcal{P}$-function and its derivatives. Explicitly, we have the formula, valid for $k \geq 3$:

$$A_k(L, \ell_0) = \frac{(-1)^k}{(k-1)!} \left(\frac{d}{dz}\right)^{k-2} \mathcal{P}(z, L)\Big|_{z=\ell_0} \qquad \text{if} \quad \ell_0 \not\equiv 0 \bmod L \tag{2.2.6}$$

while the series $A_k(L)$, (which obviously vanish for odd k), enter in the power series expansion of $\mathcal{P}$:

$$\mathcal{P}(z, L) = \frac{1}{z^2} + \sum_{n\geq 1} (n+1)! A_{n+2}(L) \frac{z^n}{n!} \tag{2.2.7}$$

It will in fact be more convenient to deal with the "normalized" Eisenstein series

$$G_k(L, \ell_0) \overset{\text{dfn}}{=\!=} \frac{(-1)^k \cdot (k-1)!}{2} A_k(L, \ell_0) \tag{2.2.8}$$

As above, we will sometimes write $G_k(L)$ instead of $G_k(L, \ell_0)$ when $\ell_0 \equiv 0 \bmod L$.

The formulas become

$$G_k(L, \ell_0) = \frac{1}{2}\left(\frac{d}{dz}\right)^{k-2} \mathcal{P}(z, L)\Bigg|_{z=\ell_0}$$

$$\text{for} \quad k \geq 3, \quad \ell_0 \not\equiv 0 \bmod L$$

and (2.2.9)

$$\mathcal{P}(z, L) = \frac{1}{z^2} + 2\sum_{k\geq 1} G_{2k+2}(L) \frac{z^{2k}}{(2k)!}, \quad G_{\mathrm{odd}}(L) = 0$$

2.3.1 Modular Definition of the G_k over Q. Let (E, ω) be an elliptic curve with differential over a $\mathbf{Q}$-algebra B. Then there is a unique isomorphism of the formal group $\hat{E}$ with the formal additive group $\hat{\mathbf{G}}_a$ under which the differential ι becomes the standard invariant differential dz on $\hat{\mathbf{G}}_a$. In other words, there exists a unique formal parameter $z = z(E, \omega)$ in terms of which $\omega = dz$. The Eisenstein series $G_k(E, \omega)$ are defined as the coefficients of the Laurent series expansion in z of the meromorphic function $X = X(E, \omega)$ on E along the identity section:

$$X = \frac{1}{z^2} + 2 \sum_{n \geq 1} G_{2n+2}(E, \omega) \frac{z^{2n}}{(2n)!} \qquad G_{\mathrm{odd}}(E, \omega) = 0.$$

When $B = \mathbf{C}$, then $X = \mathcal{P}(z, L)$, and $G_k(E, \omega) = G_k(L)$.

2.3.2 Modular Definition of the $G_k(E, \omega, P)$ over $\mathbf{Z}[1/6]$. Let (E, ω, P) be an elliptic curve together with a nowhere vanishing differential and a section P of order exactly N, over a $\mathbf{Z}[1/6N]$-algebra B. Let $D = D_\omega$ be the unique *translation-invariant B-linear derivation* of $\mathcal{O}_E$ which is *dual* to ω. Then we define, for $k \geq 3$

$$G_k(E, \omega, P) = \tfrac{1}{2} D^{k-2}(X)|_P .$$

When $B = \mathbf{C}$, then $D = (d/dz)$, $X = \mathcal{P}(z, L)$, and $G_k(E, \omega, P) = G_k(L, \ell_0)$.

2.3.3 The Magic Triangle. This is a catch-phrase for the fact that two extremely transcendental procedures "cancel" each other, to yield an algebraic one.

$$\begin{tikzcd}
(E, \omega, P) \arrow[r, "\text{integration of } \omega \text{ over } \pi_1"] \arrow[dr, "G_k"', "\text{``purely algebraic''}"'] & (L, \ell_0) \arrow[d, "G_k\text{, an archimedean infinite series}"] \\
 & \mathbf{C}
\end{tikzcd}$$

2.4 q-expansions of Eisenstein Series. We will compute analytically. The Tate curve $(\mathrm{Tate}(q^N), \omega_{\mathrm{can}})$ corresponds to the lattice $2\pi i\mathbf{Z} + 2\pi i N\tau\mathbf{Z}$, a point $P = \zeta^j q^\ell$ of finite order N to $\ell_0 = \dfrac{2\pi i j}{N} + 2\pi i \ell \tau$. We normalize the integers j, ℓ by requiring $0 \leq j, \ell < N$.

$$
\begin{aligned}
&A_k(2\pi i\mathbf{Z} + 2\pi iN\tau\mathbf{Z}, 2\pi ij/N + 2\pi i\ell\tau) \\
&\quad = \frac{1}{(2\pi i)^k} \sum_{n,m} \frac{1}{(n + mN\tau + j/N + \ell\tau)^k} \\
&\quad = \frac{1}{(2\pi i)^k} \sum_{m>0} \sum_{n\in\mathbf{Z}} \frac{1}{(n + mN\tau + j/N + \ell\tau)^k} \\
&\qquad + \frac{1}{(2\pi i)^k} \sum_{n\in\mathbf{Z}} \frac{1}{(n + j/N + \ell\tau)^k} \\
&\qquad + \frac{(-1)^k}{(2\pi i)^k} \sum_{m>0} \sum_{n\in\mathbf{Z}} \frac{1}{(n + mN\tau - j/N - \ell\tau)^k}
\end{aligned}
\tag{2.4.1}
$$

If we now avail ourselves of the formula valid for $\operatorname{Im}(x) > 0$, (both sides converge absolutely for $k \geq 2$)

$$
\sum_{n\in\mathbf{Z}} \frac{1}{(n + x)^k} = \frac{(-1)^k\cdot(2\pi i)^k}{(k-1)!} \sum_{n\geq 1} n^{k-1} e^{2\pi inx}
\tag{2.4.2}
$$

we immediately compute

$$
\begin{aligned}
&A_k(2\pi i\mathbf{Z} + 2\pi iN\tau\mathbf{Z}, 2\pi ij/N + 2\pi i\ell\tau) \\
&\quad = \frac{(-1)^k}{(k-1)!} \sum_{m>0} \sum_{n\geq 1} n^{k-1}(q^{mN+\ell})^n \zeta^{nj} \\
&\qquad + \frac{1}{(k-1)!} \sum_{m>0} \sum_{n\geq 1} n^{k-1}(q^{mN-\ell})^n \zeta^{-nj} \\
&\qquad + \begin{cases} \dfrac{(-1)^k}{(k-1)!} \displaystyle\sum_{n\geq 1} n^{k-1}(q^{\ell}\zeta^{j})^n & \text{if } \ell \neq 0 \\[2ex] \dfrac{1}{(2\pi i)^k} \displaystyle\sum_{n\in\mathbf{Z}} \frac{1}{(n + j/N)^k} & \text{if } \ell = 0 \end{cases}
\end{aligned}
\tag{2.4.3}
$$

Switching to the normalized series $G_k = (-1)^k[(k-1)!/2]A_k$, and adopting the Hurwitz notation

$$
\zeta(s, a) = \sum_{n\geq 0} \frac{1}{(n + a)^s},
\tag{2.4.4}
$$

we have the formulas

$$G_k(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, \zeta^j q^\ell)$$

$$= \frac{1}{2} \sum_{m,n\geq 1} n^{k-1}(q^{mN+\ell})^n \zeta^{nj} + \frac{(-1)^k}{2} \sum_{m,n\geq 1} n^{k-1}(q^{mN-\ell})^n \zeta^{-nj}$$

$$+ \begin{cases} \dfrac{1}{2} \displaystyle\sum_{n\geq 1} n^{k-1} q^{\ell n} \zeta^{nj} & \text{if } \quad \ell \neq 0 \\ \dfrac{(-1)^k (k-1)!}{2(2\pi i)^k} \{\zeta(k, j/N) + (-1)^k \zeta(k, 1 - j/N)\} & \text{if } \quad \ell = 0 \end{cases}$$

(2.4.5)

Thus if $\ell \neq 0$, we have

$$G_k(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, \zeta^j q^\ell) \in \tfrac{1}{2} q\mathbf{Z}[\zeta][[q]] \tag{2.4.6}$$

while in case $\ell = 0$ we have

$$\begin{aligned} &G_k(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \zeta^j) \\ &\quad = \sum_{n\geq 1} q^n \sum_{d\mid n} d^{k-1} \tfrac{1}{2}[\zeta^{jd} + (-1)^k \zeta^{-jd}] \\ &\quad + \frac{(-1)^k N^k (k-1)!}{2(2\pi i)^k} [L(k, \text{char. fct. of } j \bmod N) \\ &\quad + (-1)^k L(k, \text{char. fct. of } -j \bmod N)]. \end{aligned} \tag{2.4.7}$$

where for any function f on $\mathbf{Z}/N\mathbf{Z}$, we note $L(s, f)$ the function

$$L(s, f) = \sum_{n\geq 1} f(n) \cdot n^{-s}$$

In the case of Eisenstein series "without level", the formula above remains valid:

$$G_k(\mathrm{Tate}(q), \omega_{\mathrm{can}}) = \begin{cases} 0 & k \text{ odd} \\ \dfrac{\zeta(k)(k-1)!}{(2\pi i)^k} + \displaystyle\sum_{n\geq 1} q^n \sum_{d\mid n} d^{k-1} & k \text{ even} \end{cases} \tag{2.4.8}$$

Evaluation of the constant term. If we define the Fourier transform $f \mapsto \hat{f}$ on functions on $\mathbf{Z}/N\mathbf{Z}$ by the formula

$$\hat{f}(y) = \frac{1}{N} \sum_{x \bmod N} f(x)\zeta^{-xy} \tag{2.4.9}$$

then the Hurwitz functional equation (cf. Appendix A) for $\zeta(s, a)$ gives the following relation between the integral values of $L(s, f)$:

$$L(1-k, f) = \frac{N^k \cdot (k-1)!(-1)^k}{(2\pi i)^k} L(k, \hat{f}(x) + (-1)^k \hat{f}(-x)), \quad \text{for } k \geq 2 \tag{2.4.10}$$

or equivalently for

$$k \geq 2: \begin{cases} L(1-k, f) = 0 & \text{if } f(-x) = (-1)^{k+1} f(x), \\ \\ L(1-k, f) = \dfrac{2N^k \cdot (k-1)!(-1)^k}{(2\pi i)^k} L(k, \hat{f}) & \text{if } f(-x) = (-1)^k f(x). \end{cases}$$

We introduce some functions on $\mathbf{Z}/N\mathbf{Z}$:

$$\psi_j(x) = \zeta^{jx} \qquad f_j(x) = \begin{cases} 1 & \text{if } x = j \\ 0 & \text{if } x \neq j \end{cases} \tag{2.4.11}$$

They satisfy the identities

$$\begin{cases} f_j(-x) = f_{-j}(x), \qquad \psi_j(-x) = \psi_{-j}(x) \\ f_j = \hat{\psi}_j \\ f_j + (-1)^k f_{-j} = \hat{\psi}_j + (-1)^k \hat{\psi}_{-j} \end{cases} \tag{2.4.12}$$

Thus the functional equation gives

$$\frac{(-1)^k N^k (k-1)!}{2(2\pi i)^k} L(k, f_j + (-1)^k f_{-j}) = \tfrac{1}{4} L(1-k, \psi_j + (-1)^k \psi_{-j}) \tag{2.4.13}$$

and we obtain the q-expansion formula

$$\begin{aligned} G_k(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \zeta^j) &= \tfrac{1}{4} L(1-k, \psi_j + (-1)^k \psi_{-j}) \\ &\quad + \tfrac{1}{2} \sum_{n \geq 1} q^n \sum_{d \mid n} d^{k-1} [\psi_j(d) + (-1)^k \psi_{-j}(d)]. \end{aligned} \tag{2.4.14}$$

2.5 Definition of the Eisenstein series $G_{k,f}$ on $\Gamma_{00}(N)$. For any function f on $\mathbf{Z}/N\mathbf{Z}$, say with values in $\mathbf{Z}$ and any integer $k \geq 3$, we define a modular form $G_{k,f}$ of weight k on $\Gamma_\infty(N)$ over $\mathbf{Q}(\zeta)$ by

$$G_{k,f}(E, \omega, P) = \sum_{d \bmod N} \hat{f}(d) G_k(E, \omega, dP). \tag{2.5.1}$$

Recalling that $G_k(E, \omega, -P) = (-1)^k G_k(E, \omega, P)$, we see that

$$G_{k,f} = 0 \quad \text{if} \quad f(-x) = (-1)^{k+1} f(x)$$

$$\begin{array}{c} G_{k,\psi_d}(E, \omega, P) = G_k(E, \omega, dP) \\ \Big\| \\ G_{k,\frac{1}{2}[\psi_d + (-1)^k \psi_{-d}]} \end{array}$$

The q-expansion at the standard cusp is thus given by

$$G_{k,f}(\mathrm{Tate}(q), \omega_{\mathrm{can}}, f)$$

$$= \begin{cases} 0 & \text{if} \quad f(-x) = (-1)^{k+1} f(x) \\ \frac{1}{2}L(1-k, f) + \sum_{n \geq 1} q^n \sum_{d \mid n} d^{k-1} f(d) & \text{if} \quad f(-x) = (-1)^k f(x) \end{cases} \tag{2.5.2}$$

$$G_{k,f}(q = 0) = \tfrac{1}{2}L(1-k, f) \qquad \text{for any } f$$

At *any* cusp the q-expansion lies in $\mathbf{Q}[\zeta][[q]]$, and is integral except perhaps for its constant term.

LEMMA 2.5.3. *Let $b \in (\mathbf{Z}/N\mathbf{Z})^\times$ act on the space of $\mathbf{Z}$-valued functions on $\mathbf{Z}/N\mathbf{Z}$ by $[b]f(x) = f(bx)$. Then*

$$G_{k,[b]f} = [b]G_{k,f}$$

where $b \in (\mathbf{Z}/N\mathbf{Z})^\times$ acts on modular forms on $\Gamma_{00}(N)$ by

$$[b]G(E, \omega, P) = G(E, \omega, bP)$$

Proof. The point is that $\widehat{[b]f} = [b^{-1}]\hat{f}$; thus

$$\begin{aligned} G_{k,[b]f}(E, \omega, P) &= \sum_{d \bmod N} \widehat{[b]f}(d) G_k(E, \omega, dP) \\ &= \sum_{d \bmod N} \hat{f}(b^{-1}d) G_k(E, \omega, dP) \\ &= \sum_{d \bmod N} \hat{f}(d) G_k(E, \omega, dbP) \\ &= G_{k,f}(E, \omega, bP) \end{aligned}$$

Q.E.D.

2.6 Eisenstein Series of Weight Two. The Eisenstein series of weight two $A_2'(L, \ell_0)$ is defined only for $\ell_0 \not\equiv 0 \bmod L$, by the formula

$$A_2'(L, \ell_0) = \frac{1}{(\ell_0)^2} + \sum_{\ell \in L-\{0\}} \left\{ \frac{1}{(\ell_0 + \ell)^2} - \frac{1}{\ell^2} \right\} = \mathcal{P}(z, L)\big|_{z=\ell_0} \tag{2.6.1}$$

(The sum is absolutely convergent.)

The normalized Eisenstein series $G_2'(L, \ell_0)$ is defined by

$$G_2'(L, \ell_0) = \tfrac{1}{2}A_2'(L, \ell_0) = \tfrac{1}{2}\mathcal{P}(z, L)\big|_{z=\ell_0}. \tag{2.6.2}$$

q-expansion. The q-expansion is readily calculated, just as above:

$$\begin{aligned}
&A_2'(2\pi i\mathbf{Z} + 2\pi i N\tau\mathbf{Z}, 2\pi i j/N + 2\pi i\ell\tau) \\
&= \frac{1}{(2\pi i)^2} \sum_{m,n} \left\{ \frac{1}{(n + mN\tau + j/N + \ell\tau)^2} - \frac{1}{(n + mN\tau)^2} \right\} \\
&= \frac{1}{(2\pi i)^2} \sum_{m>0} \sum_{n\in\mathbf{Z}} \left\{ \frac{1}{(n + mN\tau + j/N + \ell\tau)^2} - \frac{1}{(n + mN\tau)^2} \right\} \\
&\quad + \frac{1}{(2\pi i)^2} \sum_{n\in\mathbf{Z}} \left\{ \frac{1}{(n + j/N + \ell\tau)^2} - \frac{1}{n^2} \right\} \\
&\quad + \frac{(-1)^2}{(2\pi i)^2} \sum_{m>0} \sum_{n\in\mathbf{Z}} \left\{ \frac{1}{(n + mN\tau - j/N - \ell\tau)^2} - \frac{1}{(n + m\tau)^2} \right\}
\end{aligned} \tag{2.6.3}$$

Applying the formula (2.4.2), we find

$$\begin{aligned}
&A_2'(2\pi i\mathbf{Z} + 2\pi i N\tau\mathbf{Z}, 2\pi i j/N + 2\pi i\ell\tau) \\
&= \sum_{m>0} \left(\sum_{n\geq 1} n^{k-1}(q^{mN+\ell})^n \zeta^{nj} - \sum_{n\geq 1} n^{k-1}(q^{mN})^n \right) \\
&\quad + \sum_{m>0} \left(\sum_{n\geq 1} n^{k-1}(q^{mN-\ell})^n \zeta^{-nj} - \sum_{n\geq 1} n^{k-1}(q^{mN})^n \right) \\
&\quad + \begin{cases} \displaystyle\sum_{n\geq 1} n^{k-1}(q^\ell\zeta^j)^n - \frac{1}{(2\pi i)^2} 2\zeta(2) & \text{if } \ell \neq 0 \\[2ex] \displaystyle\frac{1}{(2\pi i)^2} \left(\sum_{n\in\mathbf{Z}} \frac{1}{(n + j/N)^2} - 2\zeta(2) \right) & \text{if } \ell = 0 \end{cases}
\end{aligned} \tag{2.6.4}$$

Thus $A_2'(L, \ell_0)$ has a holomorphic q-expansion. At the cusps (Tate(q),

$\omega_{\mathrm{can}}, \zeta^j)$, the q-expansion is given by

$$G_2'(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \zeta^j) = \sum_{n\geq 1} q^n \sum_{d\mid n} d\cdot\tfrac{1}{2}[\zeta^{jd} + \zeta^{-jd} - 2]$$
$$+ \frac{N^2}{2(2\pi i)^2}[L(2, \text{char. fct. of } j \bmod N)$$
$$+ L(2, \text{char. fct. of } -j \bmod N)] \tag{2.6.5}$$
$$- \frac{1}{(2\pi i)^2}\zeta(2).$$

Using the functional equation for L-series (Appendix A) once again, we may rewrite the constant term. Recalling that $\zeta(-1) = -1/12$, we find

$$\begin{aligned} &G_2'(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \zeta^j) \\ &= \tfrac{1}{4}L(-1, \psi_j + \psi_{-j}) - \tfrac{1}{2}\zeta(-1) \\ &\quad + \tfrac{1}{2}\sum_{n\geq 1} q^n \sum_{d\mid n} d(\psi_j(d) + \psi_{-j}(d) - 2) \\ &= \tfrac{1}{4}L(-1, \psi_j + \psi_{-j}) + \tfrac{1}{2}\sum_{n\geq 1} q^n \sum_{d\mid n} d(\psi_j(d) + \psi_{-j}(d)) \\ &\quad - \left(\frac{-1}{24} + \sum_{n\geq 1} q^n \sum_{d\mid n} d\right) \end{aligned} \tag{2.6.6}$$

2.6.7 Definition of $G'_{2,f}$. For any function f on $\mathbf{Z}/N\mathbf{Z}$ with values in $\mathbf{Z}$ which has total integral zero (i.e. $\sum_{x \bmod N} f(x) = 0$) we define a modular form $G'_{2,f}$ of weight 2 on $\Gamma_\infty(N)$, defined over B, by

$$G'_{2,f}(E, \omega, P) \overset{\mathrm{dfn}}{=\!=} \sum_{\substack{d \bmod N \\ d\neq 0}} \hat{f}(d) G_2(E, \omega, dP). \tag{2.6.8}$$

Recalling that $G_2(E, \omega, -P) = G_2(E, \omega, P)$, we see that

$$G'_{2,f} = 0 \qquad \text{if} \quad f(-x) = -f(x)$$
$$\begin{aligned} G'_{2,\psi_d}(E, \omega, P) &= G_2(E, \omega, dP) \\ \| \\ G'_{2,\frac{1}{2}(\psi_d+\psi_{+d})} \end{aligned} \tag{2.6.9}$$

and the q-expansion of $G'_{2,f}$ at the standard cusp is given by

$$G'_{2,f}(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \zeta)$$

$$= \begin{cases} 0 & \text{if } f(-x) = -f(x) \\ \tfrac{1}{2}L(-1, f) + \sum_{n\geq 1} q^n \sum_{d\mid n} df(d) & \\ \quad - f(0)\left(\dfrac{-1}{24} + \sum_{n\geq 1} q^n \sum_{d\mid n} d\right) & \text{if } f(-x) = f(x). \end{cases} \tag{2.6.10}$$

2.6.11 Definition of $G_{2,f}$ as a generalized modular form. We recall from [6] the fact that for any prime p, there is a generalized modular form $-24G_2$ of weight 2 and defined over $\mathbf{Z}_p$ level *one* whose q-expansion is

$$-24G_2(\mathrm{Tate}(q), \varphi_{\mathrm{can}}) = 1 - 24 \sum_{n\geq 1} q^n \sum_{d\mid n} d. \tag{2.6.12}$$

Thus we may define $G_{2,f} \in V(W, \Gamma_\infty(N)) \otimes W[1/p]$ by the formulas

$$G_{2,f} = \begin{cases} G'_{2,f} + f(0)G_2 & \text{if } \sum_{x \bmod N} f(x) = 0 \\ G_2 & \text{if } f \text{ is the constant function } 1. \end{cases} \tag{2.6.13}$$

For any f, noting by $\int f$ its average value $1/N\ \Sigma_{x \bmod N} f(x)$, we thus have the formula

$$G_{2,f} = G'_{2,f-\int f} + f(0)G_2 \tag{2.6.14}$$

Its q-expansion is given by the expected formula:

$$G_{2,f}(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta)$$

$$= \begin{cases} 0 & f \text{ odd} \\ \tfrac{1}{2}L(-1, f) + \sum_{n\geq 1} q^n \sum_{d\mid n} df(d) & f \text{ even} \end{cases} \tag{2.6.15}$$

2.7 Eisenstein Series of Weight One. Strangely enough, the situation in weight one vis a vis Eisenstein series is *more satisfactory* than it was for weight two. Let us recall the definitions in an analytic context.

The Weierstrass ζ function associated to the lattice L is the meromorphic function on $\mathbf{C}$ defined by the absolutely convergent double sum

$$\zeta(z; L) = \frac{1}{z} + \sum_{\ell \in L - \{0\}} \left(\frac{1}{(z + \ell)} - \frac{1}{\ell} + \frac{z}{\ell^2}\right) \tag{2.7.1}$$

The sum converges absolutely and uniformly on any compact subset of $\mathbf{C} - L$. It is minus the integral of the $\mathscr{P}$ function:

$$d\zeta(z; L) = -\mathscr{P}(z; L)dz \tag{2.7.2}$$

Let us recall its relation to "periods of the second kind" (cf. [9], p. 241). In terms of the coordinates X, Y, we have "the" differentials of the first and second kinds

$$\begin{aligned} \omega &= \frac{dX}{Y} = dz \\ \eta &= X\frac{dX}{Y} = X\,dz = \mathscr{P}(z; L)dz = -d\zeta(z; L) \end{aligned} \tag{2.7.3}$$

which furnish a basis of $H^1(E, \mathbf{C})$.

For any $\ell \in L \simeq H_1(E, \mathbf{Z})$, we denote by $\langle \eta, \ell \rangle$ the complex number obtained by pairing the homology class ℓ and the cohomology class η:

$$\langle \eta, \ell \rangle = \int_\ell \eta = -\int_z^{z+\ell} d\zeta(z, L) = \zeta(z; L) - \zeta(z + \ell; L) \tag{2.7.4}$$

Now suppose given $\ell_0 \in L \otimes \mathbf{Q}$, $\ell_0 \notin L$, and choose an integer N such that $N\ell_0 \in L$. Following Hecke, we define

$$A_1(L, \ell_0) = \zeta(\ell_0; L) + \frac{1}{N}\langle \eta, N\ell_0 \rangle. \tag{2.7.5}$$

It is immediate that for fixed ℓ_0, the number $(1/N)\langle \eta, N\ell_0 \rangle$ is independent of the auxiliary choice of N. If we replace ℓ_0 by $\ell_0 + \ell$, with $\ell \in L$, we find

$$\begin{aligned} A_1(L, \ell_0 + \ell) &= \zeta(\ell_0 + \ell; L) + \frac{1}{N}\langle \eta, N\ell_0 + N\ell \rangle \\ &= \zeta(\ell_0 + \ell; L) + \frac{1}{N}\langle \eta, N\ell_0 \rangle + \langle \eta, \ell \rangle \\ &= \zeta(\ell_0, L) + \frac{1}{N}\langle \eta, N\ell_0 \rangle \\ &= A_1(L, \ell_0). \end{aligned} \tag{2.7.6}$$

The q-expansion of values of the Weierstrass ζ function. For any $z \notin \mathbf{Z} + \mathbf{Z}\tau$, we have

$$\zeta(2\pi iz; 2\pi i\mathbf{Z} + 2\pi i\mathbf{Z}\tau)$$

$$= \frac{1}{2\pi i}\cdot\frac{1}{z} + \frac{1}{2\pi i}\sum_m \sum_n \left(\frac{1}{z+n+m\tau} - \frac{1}{n+m\tau} + \frac{z}{(n+m\tau)^2}\right)$$

$$= \frac{1}{2\pi i}\cdot\frac{1}{z} + \frac{1}{2\pi i}\sum_m \sum_n \left(\frac{1}{z+n+m\tau} - \frac{1}{n+m\tau}\right)$$

$$+ \frac{z}{2\pi i}\sum_m \sum_n \frac{1}{(n+m\tau)^2}$$

$$= \frac{1}{2\pi i}\cdot\frac{1}{z} + \frac{1}{2\pi i}\sum_n \left(\frac{1}{z+n} - \frac{1}{n}\right) + \frac{z}{2\pi i}\sum_m \sum_n \frac{1}{(n+m\tau)^2}$$

$$+ \frac{1}{2\pi i}\sum_{m>0} \sum_n \left(\frac{1}{z+n+m\tau} - \frac{1}{n+m\tau}\right) \tag{2.7.7}$$

$$+ \frac{1}{2\pi i}\sum_{m>0} \sum_n \left(\frac{1}{z+n-m\tau} - \frac{1}{n-m\tau}\right)$$

$$= \frac{1}{2\pi i}\left(\frac{1}{z} + \sum_{n>0}\left(\frac{1}{z+n} + \frac{1}{z-n}\right)\right) + \frac{z}{2\pi i}\sum_m \sum_n \frac{1}{(n+m\tau)^2}$$

$$+ \frac{1}{2\pi i}\sum_{m>0} \sum_n \left(\frac{1}{z+n+m\tau} - \frac{1}{-z+n+m\tau}\right)$$

$$= \frac{1}{2\pi i}\cdot \pi\cot(\pi z) + \frac{z}{2\pi i}\sum_m \sum_n \frac{1}{(n+m\tau)^2}$$

$$- \sum_{m>0}\left(\sum_{n\geq 1} q^{mn}(e^{2\pi inz} - e^{-2\pi inz})\right)$$

The q-expansion of A_1.

$$A_1(2\pi i\mathbf{Z} + 2\pi iN\tau\mathbf{Z}; 2\pi ij/N + 2\pi i\ell\tau)$$

$$= \zeta(2\pi ij/N + 2\pi i\ell\tau) + \frac{1}{N}\zeta(2\pi iz) - \frac{1}{N}\zeta(2\pi iz + 2\pi ij + 2\pi iN\ell\tau)$$

$$= \frac{1}{2\pi i}(\pi\cot(\pi j/N + \pi\ell\tau) + \frac{1}{N}(\pi\cot(\pi z) - \pi\cot(\pi z + \pi j + \pi N\ell\tau))$$

$$- \sum_{m>0}\sum_{n\geq 1} q^{nmN}\Big[(e^{2\pi inj/N + 2\pi in\ell\tau} + \frac{1}{N}e^{2\pi inz} - \frac{1}{N}e^{2\pi inz + 2\pi inN\ell\tau})$$

$$- \text{(same with } n \text{ replaced by } -n)\Big] \tag{2.7.8}$$

Now we may rewrite the coefficient of q^{nmN} as

$$\left(e^{2\pi inj/N}q^{n\ell} + \frac{1}{N}e^{2\pi inz}(1 - q^{nN\ell}) - (\text{same with } n \text{ replaced by } -n)\right).$$

To compute a given coefficient, we may let $z \to 0$; then we see that the coefficient of q^{nmN} is

$$e^{2\pi inj/N}\cdot q^{n\ell} + \frac{1}{N}(1 - q^{nN\ell}) - (\text{same with } n \text{ replaced by } -n).$$

In the particular case $\ell = 0$, then the coefficient of q^{nNm} is $e^{2\pi inj/N} - e^{-2\pi inj/N}$. Thus

$$A_1(2\pi i\mathbf{Z} + 2\pi i\tau\mathbf{Z}, 2\pi ij/N)$$

$$= \frac{\pi\cot(\pi j/N) + \frac{1}{N}(\pi\cot(\pi z) - \pi\cot(\pi(z+j)))}{2\pi i} - \sum_{n\geq 1} q^n \sum_{d|n} (\zeta^{jd} - \zeta^{-jd}) \quad (2.7.9)$$

Because the cotangent function is periodic with period π, the constant term simplifies:

$$A_1(2\pi i\mathbf{Z} + 2\pi i\tau\mathbf{Z}, 2\pi ij/N)$$

$$= \frac{1}{2i}\cot(\pi j/N) - \sum_{n\geq 1} q^n \sum_{d|n} (\zeta^{jd} - \zeta^{-jd}). \quad (2.7.10)$$

We define the normalized series G_1 by the usual formula:

$$G_1 \overset{\text{dfn}}{=\!=} -\tfrac{1}{2}A_1 \quad (2.7.11)$$

Thus

$$G_1(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \zeta^j) = -\frac{1}{2}\frac{\pi\cot(\pi j/N)}{2\pi i} + \sum_{n\geq 1} q^n \sum_{d|n} \tfrac{1}{2}(\zeta^{jd} - \zeta^{-jd}) \quad (2.7.12)$$

LEMMA 2.7.13.

$$\frac{-\pi\cot(\pi j/N)}{2\pi i} = -\frac{1}{2}\left(\frac{\zeta^j + 1}{\zeta^j - 1}\right) = L(0, \tfrac{1}{2}(\psi_j - \psi_{-j}))$$

Proof of lemma. Compute:

$$\cot(\pi j/N) = \frac{\cos(\pi j/N)}{\sin(\pi j/N)} = \frac{\frac{1}{2}(e^{i\pi j/N} + e^{-i\pi j/N})}{\frac{1}{2i}(e^{i\pi j/N} - e^{-i\pi j/N})} = \frac{\frac{1}{2}(\zeta^j + 1)}{\frac{1}{2i}(\zeta^j - 1)}$$

thus

$$\frac{-\pi \cot(\pi j/N)}{2\pi i} = -\frac{1}{2}\frac{(\zeta^j + 1)}{(\zeta^j - 1)}$$

As for $L(0, f)$ for any odd function f, we use Abel summation!

$$L(0, f) \text{ ``$=$'' } \sum_{n=1}^{\infty} f(n) = \sum_{n=1}^{\infty} f(n)T^n \Bigg|_{T=1} = \frac{\sum_{n=1}^{N} f(n)T^n}{1 - T^N}\Bigg|_{N=1}$$

In the last expression, both numerator (f is odd!) and denominator vanish at $T = 1$, so by L'Hopital's rule we have

$$L(0, f) = -\frac{1}{N}\sum_{n=1}^{N} nf(n).$$

The lemma thus reduces to checking that

$$-\frac{1}{N}\sum_{n=1}^{N} n(\zeta^{jn} - \zeta^{-jn}) = -\frac{1}{2}\left(\frac{\zeta^j + 1}{\zeta^j - 1}\right)$$

which we leave to the reader (hint: multiply by $\zeta^j - 1$).

So in weight one as well, we have the "correct" q-expansion

$$\begin{aligned} G_1(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \zeta^j) = {} & \tfrac{1}{2}L(0, \tfrac{1}{2}(\psi_j - \psi_{-j})) \\ & + \tfrac{1}{2}\sum_{n\geq 1} q^n \sum_{d\mid n} \tfrac{1}{2}(\psi_j - \psi_{-j}))d). \end{aligned} \tag{2.7.14}$$

Thus we may define $G_{1,f}$ just as in the case of higher weight by

$$G_{1,f}(E, \omega, P) \stackrel{\text{dfn}}{=\!=} \begin{cases} \sum_{\substack{d \bmod N \\ d \neq 0}} \hat{f}(d)G_1(E, \omega, dP) & \text{if } f \text{ is odd} \\ & \text{if } f \text{ is even.} \end{cases} \tag{2.7.15}$$

We have

$$G_{1,\psi_j} = G_{1,\frac{1}{2}(\psi_j - \psi_{-j})} = G_1(E, \omega, jP) \tag{2.7.16}$$

and hence by linearity we get the desired q-expansion formula for any *odd* function f.

$$G_{1,f}(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \zeta) = \tfrac{1}{2}L(0, f) + \sum_{n \geq 1} q^n \sum_{d \mid n} f(d) \tag{2.7.17}$$

2.8.1 Another technical remark. The Eisenstein series $G_{k,f}$ we have constructed are *intrinsically* modular forms defined over $\mathbf{Q}$(the values of f) on the *second* version of the $\Gamma_{00}(N)$ moduli problem (cf. [1] and 1.4). They are defined, however, with the help of the modular forms (one for each integer d mod N)

$$(E, \omega, P) \to G_k(E, \omega, dP)$$

each of which is intrinsically a modular form defined over $\mathbf{Q}$ on the *first* version of the $\Gamma_{00}(N)$ problem. The modular definition of $G_{k,f}$ is by its "fourier series":

$$G_{k,f}(E, \omega, i\colon \boldsymbol{\mu}_N \to \mathrm{Ker}(N)) = \sum_{\xi \in \boldsymbol{\mu}_N} \hat{f}(\xi) \cdot G_k(E, \omega, i(\xi))$$

The fourier transform $\hat{f}$ of a function f on $\mathbf{Z}/N\mathbf{Z}$ is the function on $\boldsymbol{\mu}_N$ defined by

$$\hat{f}(\xi) = \frac{1}{N} \sum_{d \bmod N} f(d)\xi^{-d}.$$

2.8.2 A question. By the q-expansion principle, the modular forms $G_{1,f}$ we have transcendentally constructed are modular forms on $\Gamma_\infty(N)$, defined over $\mathbf{Q}(\zeta_N)$. How can they be described *purely algebraically*? (See Appendix C for the answer!)

3.1 Measures: generalities. Let X be a compact totally disconnected topological space, and R a p-adically complete ring. We denote by $C(X, R)$ the R-algebra of all continuous R-valued functions on X. Because any element of $C(X, R)$ is a uniform limit of locally constant functions, we have

$$C(X, R) = C(X, \mathbf{Z}_p) \hat{\otimes}_{\mathbf{Z}_p} R = \varprojlim C(X, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} (R/p^n R).$$

A *measure* μ on X with values in R is a (necessarily continuous) R-linear map from $C(X, R)$ to R, or *equivalently* it is a continuous $\mathbf{Z}_p$-linear map from $C(X, \mathbf{Z}_p)$ to R.

Suppose $U \overset{i}{\hookrightarrow} X$ is a compact open subset. Then the characteristic functions of both U and of $X - U$ are continuous functions on X, hence

$$C(X, R) = C(U, R) \oplus C(X - U, R).$$

A measure μ on U gives rise to a measure $i_*\mu$ on X by defining

$$(i_*\mu)(f) = \mu(f|U),$$

and a measure ν on X restricts to a measure $i^*\nu$ on U, defined by

$$(i^*\nu)(g) = \nu(g \text{ extended by 0 to all of } X).$$

A measure ν on X is said to be *supported* in U if $\nu = i_*i^*\nu$, i.e. if

$$\nu(f) = \nu(f|U \text{ extended by 0 to all of } X).$$

The constructions i^*, i_* provide inverse isomorphisms between the spaces of measures on X supported in U and of measures on U.

3.2 Measures and Pseudo-distributions on $\mathbf{Z}_p$. We begin by recalling Mahler's characterization of the continuous p-adic functions on $\mathbf{Z}_p$. For each integer $n \geq 0$, the "binomial coefficient function"

$$x \to \binom{x}{n} = \begin{cases} 1 & \text{for } n = 0 \\ \dfrac{x(x-1)\cdot \ldots \cdot(x-(n-1))}{n!} & \text{for } n > 0 \end{cases}$$

maps the positive integers to themselves, hence by continuity maps $\mathbf{Z}_p$ to $\mathbf{Z}_p$. Thanks to Mahler [21], we know that for any p-adically complete ring R, the continuous R-valued functions for $\mathbf{Z}_p$ "are" the sequences $(a_n)_{n\geq 0}$ of elements of R which tend to 0, via the interpolation expansion

$$f(x) = \sum a_n \binom{x}{n}, \qquad a_n \in R, \qquad a_n \to 0 \quad \text{as} \quad n \to \infty,$$

the a_n's being the higher differences $(\Delta^n f)(0)$.

A measure on $\mathbf{Z}_p$ with values in R is thus uniquely determined by its values on the functions $\binom{x}{n}$. Conversely, given any sequence $(b_n)_{n\geq 0}$ of elements of R, there is a unique measure on $\mathbf{Z}_p$ whose value on $\binom{x}{n}$ is b_n for all $n \geq 0$.

For any finite space T (in the discrete topology!), continuous R-valued functions on $\mathbf{Z}_p \times T$ are exactly the sequences $(a_n)_{n\geq 0}$ of R-valued functions on T which tend to 0, via the expansions

$$f(x, t) = \sum_{n\geq 0} a_n(t) \binom{x}{n}.$$

A *measure* on $\mathbf{Z}_p \times T$ with values in R is uniquely determined by its restriction to the subspace of $C(\mathbf{Z}_p \times T, \mathbf{Z}_p)$ consisting of the finite sums $\Sigma\, a_n(t) \binom{x}{n}$, and its restriction to this subspace is arbitrary.

For any $\mathbf{Z}_p$-algebra R, we define a *pseudo-distribution* on $\mathbf{Z}_p \times T$ with values in R to be a linear form on the R-submodule of $\text{Maps}(\mathbf{Z}_p \times T, \mathbf{Z}_p)$ spanned by all functions $f(x, t) = a(t)x^n$, $n \geq 0$, $a(t)$ any $\mathbf{Z}_p$-valued function on T.

Suppose now that R is $\mathbf{Z}_p$-flat (i.e. $R \subset R \otimes \mathbf{Q}$) and p-adically complete. Then because $\binom{x}{n} = \dfrac{x^n}{n!}$ + lower terms, it follows immediately that an R-valued measure on $\mathbf{Z}_p \times T$ is uniquely determined by the $R \otimes \mathbf{Q}$-valued pseudo-distribution on $\mathbf{Z}_p \times T$ to which it gives rise. Conversely, an $R \otimes Q$-valued pseudo-distribution on $\mathbf{Z}_p \times T$ extends to a *measure* if and only if its values on the functions $a(t) \binom{x}{n}$ ($n \geq 0$, $a(t)$ any $\mathbf{Z}$-valued function on T) all lie in R (rather than in $R \otimes \mathbf{Q}$).

Remark 3.2.1. We have adopted the term "pseudo-distribution" so as to avoid confusion with *distributions* on $\mathbf{Z}_p \times T$ in the sense of [13] and [15], these latter being linear functionals on the space of *locally constant* functions on $\mathbf{Z}_p \times T$. With the exception of the constant functions, the *domains* of distributions and of pseudo-distributions are disjoint! We should also remark that the notion of a pseudo-distribution depends upon the choice of the coordinate x on $\mathbf{Z}_p$, i.e. on the ring structure of $\mathbf{Z}_p$, and not simply on its structure of compact totally disconnected space.

3.3 The Eisenstein pseudo-distribution on $\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}$ and the measures $2\mathbf{H}^{a,b}$. We define a pseudo-distribution $\mathbf{H}$ on $\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}$ with values in $V(W, \Gamma_{00}(N)) \otimes_W W[1/p]$ by the formula

$$\mathbf{H}(x^k f(t)) = G_{k+1,f} \quad \text{for} \quad k \geq 0, f(t) \text{ any } \mathbf{Z}_p\text{-valued function on } \mathbf{Z}/N\mathbf{Z} \tag{3.3.1}$$

For each $(a, b) \in \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$, we define the pseudo-distribution $\mathbf{H}^{a,b}$ on $\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}$ with values in $V(W, \Gamma_{00}(N)) \otimes_W W[1/p]$ by the formula

$$\begin{aligned} \mathbf{H}^{a,b}(x^k f(t)) &= \mathbf{H}(x^k f(t)) - \mathbf{H}(a^{k+1} x^k f(bt)) \\ &= G_{k+1,f} - [a, b] G_{k+1,f} \end{aligned} \tag{3.3.2}$$

THEOREM 3.3.3. *The pseudo-distribution* $2\mathbf{H}^{a,b}$ *has values in* $V(W,$

$\Gamma_\infty(N)$), *and extends to a (unique)* measure *on* $\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}$ *with values in* $V(W, \Gamma_\infty(N))$.

Proof. What must be shown is that if $F(x) \in \mathbf{Q}_p[x]$ is any polynomial which takes values on $\mathbf{Z}_p$ when $x \in \mathbf{Z}_p$, and if $f(t)$ is any $\mathbf{Z}_p$-valued function on $\mathbf{Z}/N\mathbf{Z}$, then $2\mathbf{H}^{a,b}(F(x)f(t)) = 2\mathbf{H}(F(x)f(t)) - 2[a, b]\mathbf{H}(F(x)f(t))$ has *integral* q-expansions. By the "key lemma" (1.2.1), this will certainly be the case if *one* of the q-expansions of $2\mathbf{H}(F(x)f(t))$ is integral except possibly for its constant term. Let's check that this is indeed the case at the standard cusp (Tate(q), φ_{can}, ζ).

We recall that $G_{k,f}$ has q-expansion

$$2G_{k,f}(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta) = \tfrac{1}{2}L(1-k, f(t) + (-1)^k f(-t)) + \sum_{n\geq 1} q^n \sum_{d\mid n} (d^{k-1}f(d) + (-1)^k d^{k-1} f(-d)). \quad (3.3.4)$$

Because of the décalage $k \leftrightarrow k+1$, we obtain

$$2\mathbf{H}(x^k f(t))(\mathrm{Tate}(q). \varphi_{\mathrm{can}}, \zeta) = \text{constant} + \sum_{n\geq 1} q^n \sum_{d\mid n} (d^k f(d) - (-d)^k f(-d)) \quad (3.3.5)$$

By linearity, we obtain

$$2\mathbf{H}(F(x)f(t))(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta) = \text{constant} + \sum_{n\geq 1} q^n \sum_{d\mid n} (F(d)f(d) - F(-d)f(-d)) \quad (3.3.6)$$

Q.E.D.

COROLLARY 3.3.7. *Let B_0 be any p-adically complete W-algebra, and let $F(x, t)$ be a continuous B_0-valued function on $\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}$. Then $2\mathbf{H}^{a,b}(F(x, t))$ lies in $V(V_0, \Gamma_{00}(N))$ and its q-expansion at the standard cusp given by*

$$2\mathbf{H}^{a,b}(F(x,t))(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta) = \text{constant} + \sum_{n\geq 1} q^n \sum_{d\mid n} [F(d,d) - F(-d,-d) - aF(ad, bd) + aF(-ad, +bd)]$$

COROLLARY 3.3.8. *If $g(x)$ is any locally constant function on $\mathbf{Z}_p$, then for $k \geq 0$ we have*

$$2\mathbf{H}^{a,b}(x^k g(x) f(t)) = (1 - [a, b])2G_{k,gf}$$

where gf is viewed as a function on $\mathbf{Z}/p^n N\mathbf{Z}$ for $n \gg 0$.

Additional Properties of the Measures $2\mathbf{H}^{1,b}$.

PROPOSITION 3.3.9. *Let (a, b) and (α, β) be two elements of $\mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$, and let $F(x, t)$ be any continuous function on $\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}$ with values in B_0. Then we have the formulas*

$$2\mathbf{H}^{a,b}(F(x, t)) - 2[\alpha, \beta]\mathbf{H}^{a,b}(F(x, t)) = 2\mathbf{H}^{\alpha,\beta}(F(x, t)) - 2[a, b]\mathbf{H}^{\alpha,\beta}(F(x, t)). \quad (3.3.10)$$

$$2[\alpha, \beta]\mathbf{H}^{a,b}(F(x, t)) = 2\mathbf{H}^{a,b}(\alpha F(\alpha x, \beta t)). \quad (3.3.11)$$

Explicitly, for every "test object" (E, φ, P) of our $\Gamma_{00}(N)$ moduli problem, we have the formulas

$$2\mathbf{H}^{a,b}(F(x, t))(E, \varphi, P) - 2\mathbf{H}^{a,b}(F(x, t))(E, \alpha^{-1}\varphi, \beta P) = 2\mathbf{H}^{\alpha,\beta}(F(x, t))(E, \varphi, P) - 2\mathbf{H}^{\alpha,\beta}(F(x, t))(E, a^{-1}\varphi, bP) \quad (3.3.12)$$

and

$$2\mathbf{H}^{a,b}(F(x, t))(E, \alpha^{-1}\varphi, \beta P) = 2\mathbf{H}^{a,b}(\alpha F(\alpha x, \beta t))(E, \varphi, P). \quad (3.3.13)$$

Proof. We immediately reduce to the case $B_0 = W$, then to the case $F(x, t) = x^k f(t)$. Then $\mathbf{H}^{a,b}(x^k f(t)) = (1 - [a, b])G_{k+1,f}$, and $\mathbf{H}^{a,b}(\alpha F(\alpha x, \beta t)) = (1 - [a, b])\alpha^{k+1}G_{k+1,f(\beta t)} = (1 - [a, b])[\alpha, \beta]G_{k,f}$ (this last equality by (2.5.3)). Thus both sides of the first asserted formula become $2(1 - [\alpha, \beta])(1 - [a, b])G_{k+1,f}$, and both sides of the second reduces to $2[\alpha, \beta](1 - [a, b])G_{k+1,f}$.

Q.E.D.

3.4 Construction of the Eisenstein Measure $J^{a,b}$ on $\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}$. For each $(a, b) \in \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$, we define the measure $2J^{a,b}$ on $\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}$ with values in $V(W, \Gamma_{00}(N))$ by the formula

$$2J^{a,b} = \text{the restriction to } \mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z} \text{ of } 2\mathbf{H}^{a,b} \quad (3.4.1)$$

Let us denote by $F \mapsto [a, b]F$ the action of $\mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$ on functions $F(x, t)$ on $\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}$ given by

$$([a, b]F)(x, t) = aF(ax, bt)$$

The transcription of (3.3.10–11) to the measures $J^{a,b}$ is immediate.

PROPOSITION 3.4.2. *Let (a, b) and (α, β) be elements of $\mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$, and let F be a continuous function on $\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}$ with values in a* *p-adically complete W-algebra B_0. Then we have the formulas*

$$(1 - [\alpha, \beta])(2J^{a,b}(F)) = (1 - [a, b])(2J^{\alpha,\beta}(F)) \tag{3.4.3}$$

$$[\alpha, \beta](2J^{a,b}(F)) = 2J^{a,b}([\alpha, \beta]F). \tag{3.4.4}$$

The q-expansion of $2J^{a,b}(F)$ at the standard cusp is given by formula

$$2J^{a,b}(F)(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta) = \text{constant}$$

$$+ \sum_{n\geq 1} q^n \sum_{\substack{d|n \\ (p,d)=1}} \frac{F(d, d) + F(-d, -d) - F(ad, bd) - F(-ad, -bd)}{d} \tag{3.4.5}$$

3.5 Construction of the Eisenstein series $J_{\chi,f}$. Let χ: $\mathbf{Z}_p{}^\times \to B_0{}^\times$ be a continuous character (B_0 a p-adically complete W-algebra as above), and f: $\mathbf{Z}/N\mathbf{Z} \to B_0$ any function. Recall that χ_k is the character $x \to x^k$ on $\mathbf{Z}_p{}^\times$. We define

$$2J^{a,b}_{\chi,f} \overset{\text{dfn}}{=\!=} 2J^{a,b}(\chi\chi_{-1}f) \tag{3.5.1}$$

Thanks to (3.4.4), we know that $2J^{a,b}_{\chi,f}$ is a generalized modular function of weight χ on $\Gamma_\infty(N)$, defined over B_0. In case f has "parity χ", in the sense that $f(-t) = \chi(-1)f(t)$, the q-expansion of $J^{a,b}_{\chi,f}$ is given

$$2J^{a,b}_{\chi,f}(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta) = \text{constant}$$

$$+ 2 \sum_{n\geq 1} q^n \sum_{\substack{d|n \\ p \nmid d}} \frac{\chi(d)}{d} (f(d) - \chi(a)f(bd)) \tag{3.5.2}$$

while if $f(-t) = -\chi(-1)f(t)$, we have $2J^{a,b}_{\chi,f} = 0$ (this because $(-1, -1) \in \mathbf{Z}_p{}^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$ must operate as the *identity* on $V(B_0, \Gamma_{00}(N))$.

Suppose that B_0 is an *integral domain* with fraction field K, and that the character χ is non-trivial. Then for any $a \in \mathbf{Z}_p{}^\times$ such that $\chi(a) \neq 1$, we define an element

$$J_{\chi,f} \in V(B_0, \Gamma_{00}(N)) \underset{B_0}{\otimes} K \tag{3.5.3}$$

by

$$J_{\chi,f} \overset{\text{dfn}}{=\!=} \frac{1}{1 - \chi(a)} \cdot J^{a,1}_{\chi,f}$$

It is immediate that this definition is independent of the choice of a such that $\chi(a) \neq 1$, for we have the identity

$$(1 - \chi(\alpha))J^{a,1}_{\chi,f} = (1 - [\alpha, 1])J^{a,1}_{\chi,f} = (1 - [a, 1])J^{\alpha,1}_{\chi,f} = (1 - \chi(a))J^{\alpha,1}_{\chi,f}.$$

Further, for any $a, b \in \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$, we have

$$J_{\chi,f}^{a,b} = (1 - [a, b])J_{\chi,f} \quad \text{in} \quad V(B_0, \Gamma_{00}(N)) \otimes K, \tag{3.5.4}$$

because for any α with $\chi(\alpha) \neq 1$, we have the identity

$$\begin{array}{rl} (1 - \chi(\alpha))J_{\chi,f}^{a,b} = (1 - [\alpha, 1])J_{\chi,f}^{a,b} = & (1 - [a, b])J_{\chi,f}^{\alpha,1} \\ & \qquad \| \\ & (1 - [a, b])(1 - \chi(\alpha))J_{\chi,f}. \end{array}$$

In case f has "parity χ", the q-expansion of $J_{\chi,f}$ at the standard cusp is given by

$$J_{\chi,f}(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta) = \frac{\text{elt. of } B_0}{2\cdot(1 - \chi(\alpha))} + \sum_{n\geq 1} q^n \sum_{d\mid n} \frac{\chi(d)}{d} f(d) \tag{3.5.5}$$

(the α written explicitly in the denominator is arbitrary subject to the condition $\chi(\alpha) \neq 1$, though of course the numerator in such a representation of the constant term does depend on α). In case f has parity $-\chi$, $J_{\chi,f}$ vanishes.

Relation of the $J_{\chi,f}$ to the $G_{k,f}$. For any integer $k \neq 0$, we denote by $J_{k,f}$ the Eisenstein series $J_{\chi_k,f}$ where χ_k is the character $\chi_k\colon \mathbf{Z}_p^\times \to \mathbf{Z}_p^\times \subset W^\times$ given by $\chi_k(x) = x^k$. Thus $J_{k,f}$ is an element of $V(W, \Gamma_{00}(N)) \otimes W[1/p]$.

LEMMA 3.5.6. *Let $k \geq 1$ be an integer, and $f\colon \mathbf{Z}/N\mathbf{Z} \to W$ any function. Then*

$$J_{k,f} = G_{k,f} - p^{k-1}\cdot\mathrm{Frob}(G_{k,f}) \quad \text{in} \quad V(W, \Gamma_{00}(N)) \otimes W[1/p]. \tag{3.5.6.1}$$

Proof. It suffices to show that both sides have the same q-expansion at the standard cusp $(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta)$, except possibly for their constant terms. For then their difference would be a *constant* in $W[1/p]$ which has weight $k \neq 0$, hence must vanish. To compute q-expansions, we may assume that f has "parity k", i.e. $f(-t) = (-1)^k f(t)$, for in case f has "parity $k + 1$", both sides of (3.5.6.1) vanish.

Recall that

$$\begin{aligned} &\mathrm{Frob}(G_{k,f})(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta) \\ &\qquad = \text{the image under } q \mapsto q^p \text{ of } G_{k,f}(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta^p) \\ &\qquad = \text{the image under } q \mapsto q^p \text{ of } G_{k,f(pt)}(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta) \end{aligned}$$

and hence

$$\operatorname{Frob}(G_{k,f})(\operatorname{Tate}(q), \varphi_{\mathrm{can}}, \zeta) = \text{constant} + \sum_{n \geq 1} q^{np} \sum_{d \mid n} d^{k-1} f(pd).$$

Hence the q-expansion of the right hand side of (3.5.6.1) is given by

$$\text{constant} + \sum_{n\geq 1} q^n \sum_{d\mid n} d^{k-1}f(d) - \sum_{n\geq 1} q^{np} \sum_{d\mid n} (pd)^{k-1}f(pd)$$

$$= \text{constant} + \sum_{n\geq 1} q^n \sum_{\substack{d\mid n\\(p,d)=1}} d^{k-1}f(d)$$

which agrees with the q-expansion of $J_{k,f}$ up to its constant term.

COROLLARY 3.5.7. *The constant term of the q-expansion of* $J_{k,f}$ *is given by the formula*

$$\begin{aligned} J_{k,f}(q=0) &= G_{k,f}(q=0) - p^{k-1}G_{k,f(pt)}(q=0) \\ &= \tfrac{1}{2}L(1-k,f) - \tfrac{1}{2}p^{k-1}L(1-k,f(pt)). \end{aligned} \tag{3.5.8}$$

In particular, if f is itself a multiplicative function ϵ on $\mathbf{Z}/N\mathbf{Z}$ (meaning $f(xy) = f(x)f(y)$ for all $x, y \in \mathbf{Z}/N\mathbf{Z}$ and $f(1) = 1$) then both $G_{k,\epsilon}$ and $J_{k,\epsilon}$ are of weight k and nebentypus ϵ, and the formula becomes

$$J_{k,\epsilon}(q=0) = \frac{1 - p^{k-1}\epsilon(p)}{2} L(1-k, \epsilon). \tag{3.5.9}$$

Notice that $1 - p^{k-1}\epsilon(p)$ is precisely the value at $1 - k$ of the reciprocal of the p-Euler factor which figures in $L(s, \epsilon)$.

COROLLARY 3.5.10. *If the character* χ *is of the form* $\chi_k\omega$, *where* ω *is a non-trivial character of* $\mathbf{Z}_p^\times$ *of finite order (extended by* 0 *to all of* $\mathbf{Z}_p$), *we have*

$$J_{\chi_k\omega,f} = G_{k,\omega f} - p^{k-1}\operatorname{Frob}(G_{k,\omega f}).$$

In the special case $f = \epsilon$, *a multiplicative function on* $\mathbf{Z}/N\mathbf{Z}$, *and* $\omega\epsilon$ *has parity k, the q-expansion is given at the standard cusp by*

$$J_{\chi_k\omega,\epsilon}(q) = \tfrac{1}{2}L(1-k, \omega\epsilon) + \sum_{n\geq 1} q^n \sum_{d\mid n} d^{k-1}\omega(d)\epsilon(d).$$

(The Euler factor disappears because $(\omega\epsilon)(p) = \omega(p)\epsilon(p) = 0\cdot\epsilon(p) = 0.$*)*

3.6 Applications to the Kubota-Leopoldt p-adic L-function of Q. Let C be a complete algebraically closed overfield of $\mathbf{Q}_p$, and let $\mathcal{O} = \mathcal{O}_C$ denote its ring of integers. Fix an integer N prime to p. The Kubota-Leopoldt L-function is the C-valued function on $\mathrm{Hom}_{\mathrm{contin}}(\mathbf{Z}_p{}^\times \times (\mathbf{Z}/N\mathbf{Z})^\times, C^\times)$—{the trivial character}) defined by

$$\mathscr{L}(\chi, \epsilon) = \frac{1}{1 - \chi(a)\cdot\epsilon(b)} - 2J^{a,b}\left(\frac{(\chi\epsilon)}{``x"}\right)(\mathrm{Tate}(q), \varphi_{\mathrm{can}}, \zeta)\big|_{q=0} \qquad (3.6.1)$$

(the right hand side is independent of the choice of $(a, b) \in \mathbf{Z}_p{}^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$ such that $\chi(a)\epsilon(b) \neq 1$). It has a first order pole at the trivial character, in the sense that for each $(a, b) \in \mathbf{Z}_p{}^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$, the function

$$(\chi, \epsilon) \to (1 - \chi(a)\epsilon(b))\mathscr{L}(\chi, \epsilon)$$

extends to a continuous *$\mathcal{O}$-valued* function on all of $\mathrm{Hom}_{\mathrm{contin}}(\mathbf{Z}_p{}^\times \times (\mathbf{Z}/N\mathbf{Z})^\times, C^\times)$. Because this last function is the restriction of a *measure*, its values satisfy the Kummer congruences:

Whenever a finite C-linear combination $\sum c_{\chi,\epsilon}\chi\cdot\epsilon$ of characters satisfies a congruence

$$\sum c_{\chi,\epsilon}\chi(a)\epsilon(b) \in p^\nu\mathcal{O} \qquad \text{for} \quad \textit{all } (a, b),$$

Then for each (a, b), the values $\mathscr{L}(\chi, \epsilon)$ satisfy the congruence

$$\sum c_{\chi,\epsilon}(1 - \chi(a)\cdot\epsilon(b))\mathscr{L}(\chi, \epsilon) \in p^\nu\mathcal{O}.$$

If we denote by χ_k the character $\chi_k(x) = x^k$ of $\mathbf{Z}_p{}^\times$, we have the formula

$$\mathscr{L}(\chi_k, \epsilon) = (1 - p^{k-1}\epsilon(p))L(1 - k, \omega\epsilon)\begin{cases}\text{valid for } k = 2, \text{ any } \epsilon, \omega \\ \text{valid for } k \geq 1 \text{ only if} \\ \epsilon \text{ is an odd character}\end{cases} \qquad (3.6.3)$$

For any nontrivial character ω: $\mathbf{Z}_p{}^\times \to C$ which is of *finite order* we have the supplementary formula

$$L(\chi_k\cdot\omega, \epsilon) = L(1 - k, \omega\epsilon)\begin{cases}\text{valid for } k \geq 2, \text{ any } \omega, \epsilon \\ \text{valid for } k = 1 \text{ only if} \\ \omega\epsilon \text{ is an odd character}\end{cases} \qquad (3.6.4)$$

(where we view $\omega\epsilon$ as a Dirichlet character of conductor $p^{\mathrm{power}} \times N$).

3.7 The p-adic L-series attached to an ordinary elliptic curve (N = 1 for simplicity). Let C, $\mathcal{O}$ be as above, and suppose given an elliptic curve $E/\mathcal{O}$ together with a nowhere vanishing differential ω. We suppose that E is *ordinary*, in the sense that modulo $\mathscr{Y}$ its Hasse invariant is non-zero. Then E admits a trivialization φ: $\hat{E} \xrightarrow{\sim} \hat{G}_m$ defined over $\mathcal{O}$, and a trivialization φ is uniquely determined by the constant $\lambda \in \mathcal{O}^\times$ defined by $\varphi^*(dT/1 + T) = \lambda\omega$. Indeed, a constant $\lambda \in \mathcal{O}^\times$ comes from a trivialization if and only if the differential $\lambda\omega$ is *formally* logarithmic. In terms of a uniformizing parameter t at the origin ("infinity") on E, the condition is that the power series in t, $\exp\left(\lambda \int_0^t \omega\right)$ have coefficients in $\mathcal{O}$ rather than in C (compare [1a]).

Let us *choose* such a λ (any other would be $a\lambda$, with $a \in \mathbf{Z}_p{}^\times$), and write $(E, \lambda\omega)$ instead of (E, the unique φ such that $\varphi^*\ (dT/1 + T) = \lambda\omega$).

We define the p-adic L-series $\mathscr{L}_{(E,\lambda\omega)}$ as the C-valued function on $\mathrm{Hom}_{\mathrm{contin}}(\mathbf{Z}_p{}^\times, C^\times)$—{the trivial character} given by

$$\mathscr{L}_{(E,\lambda\omega)}(\chi) \overset{\mathrm{dfn}}{=\!=} \frac{1}{1 - \chi(a)} \cdot 2J^a\left(\frac{\chi}{\text{``}\chi\text{''}}\right)(E, \lambda\omega). \tag{3.7.1}$$

It has a first order pole at the trivial character, in the sense that for each $a \in \mathbf{Z}_p{}^\times$, the function

$$\chi \mapsto (1 - \chi(a))\mathscr{L}_{(E,\lambda\omega)}(\chi)$$

extends to a continuous $\mathcal{O}$-valued function on all of $\mathrm{Hom}_{\mathrm{contin}}(\mathbf{Z}_p{}^\times, C^\times)$.

Because this last function is the restriction of a *measure* on $\mathbf{Z}_p{}^\times$, the Kummer congruences are satisfied:

> If a C-linear combination of character $\Sigma\, c_\chi \cdot \chi$ satisfies a congruence
>
> $$\sum c_\chi \cdot \chi(a) \in p^\nu\mathcal{O} \qquad \text{for all} \quad a \in \mathbf{Z}_p{}^\times$$
>
> then for each $a \in \mathbf{Z}_p{}^\times$ the values $\mathscr{L}_{(E,\lambda\omega)}(\chi)$ satisfy
>
> $$\sum c_\chi(1 - \chi(a))\mathscr{L}_{(E,\lambda\omega)}(\chi) \in p^\nu\mathcal{O}.$$

(3.7.2)

We might summarize the situation by saying that $\mathscr{L}_{(E,\lambda\omega)}$ is just as good a function as the Kubota-Leopoldt p-adic L function.

What about special values? By construction, we have, for $k \geq 1$

$$\mathscr{L}_{(E,\lambda\omega)}(\chi_k) = 2J_k(E, \lambda\omega) = 2G_k(E, \lambda\omega) - 2p^{k-1}(\mathrm{Frob}\ G_k)(E, \lambda\omega), \tag{3.7.3}$$

a formula we will be able to unwind only in special cases. But in any case we always have a *limit formula* for $\mathscr{L}_{(E,\lambda\omega)}(\chi_k)$, for $k \neq 0$.

$$\begin{aligned}(1 - a^k)\mathscr{L}_{(E,\lambda\omega)}(\chi_k) &= 2J^a(x \to x^{k-1})(E, \lambda\omega)\\ &= 2\mathbf{H}^a(x \to x^{k-1} \text{ on } \mathbf{Z}_p{}^\times, \text{ extended by } 0)(E, \lambda\omega)\\ &= \lim_{N\to\infty} 2\mathbf{H}^a(x \to x^{k-1+(p-1)p^N} \text{ on } \mathbf{Z}_p)(E, \lambda\omega)\\ &= \lim_{N\to\infty} (1 - a^{k+(p-1)p^N})\cdot 2\cdot G_{k+(p-1)p^N}(E, \lambda\omega)\end{aligned} \tag{3.7.4}$$

Thus

$$\mathscr{L}_{(E,\lambda\omega)}(\chi_k) = \lim_{N\to\infty} 2\cdot\lambda^{k+(p-1)p^N} G_{k+(p-1)p^N}(E, \omega) \tag{3.7.5}$$

3.8 Computation of $\mathscr{L}_{(E,\lambda\omega)}(\chi_k)$ for complex multiplication curves. Suppose *in addition* that there is given an *endomorphism* of E

$$F_p\colon\quad E \to E$$

which modulo $\mathscr{Y}$ is the absolute Frobenius F. This is possibly only when E mod $\mathscr{Y}$ comes from an elliptic curve E_0 defined over the *prime* field $\mathbf{F}_p$, and the curve $E/\mathcal{O}$ is deduced by extension of scalars $\mathbf{Z}_p \to \mathcal{O}$ from the *canonical lifting* of E_0 (cf. [16a], Appendix).

Then the kernel of F_p is just the canonical subgroup E_{can}, and hence F_p may be factored

$$\begin{tikzcd} E \arrow[r, "\pi"] \arrow[rr, bend left, "F_p"] & E/E_{\text{can}} \arrow[r, "A", "\sim"'] & E \end{tikzcd} \tag{3.8.1}$$

Let us denote by

$$V_p\colon\quad E \to E \tag{3.8.2}$$

the *transpose* of F_p (thus $F_pV_p = V_pF_p = p$, and V_p modulo $\mathscr{Y}$ is Verschiebung V). The mapping V is etale, so that

$$\varphi \to \varphi \circ V$$

defines an automorphism of the $\mathbf{Z}_p{}^\times$-torsor $\operatorname{Isom}(\hat{E}, \hat{G}_m)$, which is necessarily of the form

$$\varphi \mapsto \mu\varphi \qquad \text{for some} \quad \mu \in \mathbf{Z}_p{}^\times.$$

The unit $\mu \in \mathbf{Z}_p{}^\times$ is precisely the *image* of V_p in $\operatorname{End}(\hat{E})$,

$$\begin{tikzcd}
\hat{E} \arrow[dd, "V_p"'] \arrow[dr, "\varphi \circ V_p"] & \\
& \hat{G}_m \\
\hat{E} \arrow[ur, "\varphi"'] &
\end{tikzcd} \tag{3.8.3}$$

hence μ is the image of V in $\mathrm{End}(\hat{E} \otimes (\mathcal{O}/\mathcal{Y}))$, which by duality is the image of F_p in $\mathrm{End}(T_p(E \otimes (\mathcal{O}/\mathcal{Y}))$. This makes it clear that μ is none other than the "unit root" of the zeta function of the elliptic curve E_0 over $\mathbf{F}_p$ which gives rise to $E \otimes \mathcal{O}/\mathcal{Y}$ by extension of scalars:

$$\mathrm{Zeta}(E_0/\mathbf{F}_p, T) = \frac{(1 - \mu T)(1 - p\mu^{-1}T)}{(1 - T)(1 - pT)} \tag{3.8.4}$$

Recall now the definition of the Frobenius endomorphism of generalized modular functions in terms of the projection $\pi: E \to E/E_{\mathrm{can}}$

$$\mathrm{Frob}(f)(E, \varphi) = f(E/E_{\mathrm{can}}, \varphi \circ \check{\pi}). \tag{3.8.5}$$

In our situation, we have a commutative diagram

$$\begin{tikzcd}
E \arrow[r, "\pi"] \arrow[rr, bend left, "F_p"] & E/E_{\mathrm{can}} \arrow[r, "A", "\sim"'] \arrow[dr, "\check{\pi}"'] & E \arrow[d, "V_p"] \\
& & E
\end{tikzcd} \tag{3.8.6}$$

so that A defines an *isomorphism* between $(E/E_{\mathrm{can}}, \varphi \circ \check{\pi})$ and $(E, \varphi \circ V_p)$. The formula for Frob becomes

$$\mathrm{Frob}(f)(E, \lambda\omega) = f(E, V^*(\lambda\omega)) = f(E, \mu\lambda\omega). \tag{3.8.7}$$

In particular

$$\mathrm{Frob}(G_k)(E, \lambda\omega) = G_k(E, \mu\lambda\omega) = \mu^{-k}G_k(E, \lambda\omega), \tag{3.8.8}$$

and, referring back to (3.7.3), we obtain the formula

$$\begin{aligned}\mathscr{L}_{(E,\lambda\omega)}(\chi_k) &= 2(1 - p^{k-1}\cdot\mu^{-k})\cdot G_k(E, \lambda\omega) \qquad \text{for} \quad k \geq 1. \\ &= 2(1 - p^{k-1}\mu^{-k})\cdot\lambda^{-k}G_k(E, \omega)\end{aligned}$$

3.9 The Case of the Hurwitz Numbers. The Hurwitz numbers h_n are defined by looking at the power series expansion of the $\mathscr{P}$ function which corresponds to the elliptic curve with differential $\left(E\colon y^2 = 4x^3 - 4x,\ \omega = \dfrac{dx}{y}\right)$:

$$\mathscr{P}(z) = \frac{1}{z^2} + \sum_{n\geq 4} \frac{2^n h_n}{n} \frac{z^{n-2}}{(n-2)!} \tag{3.9.1}$$

Referring to the general formula 2.2.9

$$\mathscr{P}(z; L) = \frac{1}{z^2} + 2\sum_{k\geq 1} G_{2k+2}(L)\frac{z^{2k}}{(2k)!}$$

we see that

$$\frac{2^n h_n}{n} = 2G_n(L) = 2G_n(y^2 = 4x^3 - 4x, dx/y) \in \mathbf{Q}. \tag{3.9.2}$$

Because there is an automorphism of this curve (multiplication by $i = \sqrt{-1}$, defined by $x \to -x$, $y \to iy$) which multiplies the differential dx/y by i, it follows that $h_n = i^n h_n$, and hence

$$h_n = 0 \qquad \text{unless} \quad n \equiv 0(4) \tag{3.9.3}$$

[Hurwitz labels them $E_n \overset{\text{dfn}}{=\!=} h_{4n}$, but we have too many E's already.]

Because of the multiplication by i, the lattice L must be a locally free $Z[i]$ module of rank one, which will in fact be *free* because $\mathbf{Z}[i]$ is a principal ideal ring. By standard considerations, we may generate the lattice L by taking *twice* the integrals of a single-valued branch of ω in the x-plane between the x-coordinates of the finite points of order two (i.e. the zeros of $4x^3 - 4x$, namely ± 1 and 0). Thus L is spanned by the two periods

$$2\int_{-1}^{0} \frac{dx}{\sqrt{4x^3 - 4x}}, \qquad 2\int_{0}^{1} \frac{dx}{\sqrt{4x^3 - 4x}} \tag{3.9.4}$$

the first of which is $\pm i$ times the second. The second is

$$2\int_0^1 \frac{dx}{\sqrt{4x^3-4x}} = 2\int_0^1 \frac{d(t^2)}{\sqrt{4t^6-4t^2}}$$
$$= 2\int_0^1 \frac{dt}{\sqrt{t^4-1}} = -2i\int_0^1 \frac{dt}{\sqrt{1-t^4}}. \qquad (3.9.5)$$

Thus the period lattice of $(y^2 = 4x^3 - 4x,\ dx/y)$ is

$$L = \mathbf{Z}[i]\cdot\Omega$$
$$\Omega = 2\int_0^1 \frac{dt}{\sqrt{1-t^4}} = 2.622057\ldots \qquad (3.9.6)$$

Thus we obtain transcendental formulas for the h_n;

$$h_n = n\cdot 2^{1-n}G_n(L) = n\cdot 2^{-n}\cdot(-1)^n(n-1)!A_n(L)$$
$$= \frac{(-1)^n\cdot n!}{2^n\Omega^n}\sum_{a,b}\frac{1}{(a+bi)^n} \qquad (3.9.7)$$

or equivalently

$$\sum \frac{1}{(a+bi)^{4n}} = \frac{(2\Omega)^{4n}}{(4n)!}h_{4n} \qquad \text{for} \quad n \geq 1. \qquad (3.9.8)$$

Suppose now that $p \equiv 1 \bmod (4)$. Then the curve $y^2 = 4x^3 - 4x$ viewed over $\mathbf{Z}_p$ is *ordinary*, and we may choose a constant λ in $W(\bar{\mathbf{F}}_p)$, the completion of the ring of integers of the maximal unramified extension of $\mathbf{Q}_p$ such that $\lambda\ dx/y$ comes from a trivialization (i.e. $\lambda\ dx/y$ is formally logarithmic).

The values of the p-adic L series associated to $(y^2 = 4x^3 - 4x,\ \lambda\ dx/y)$ at the characters χ_k are thus given by the formula

$$\mathscr{L}_{(y^2=4x^3-4x,\lambda\,dx/y)}(\chi_k)$$
$$= 2(1 - p^{k-1}\mu^{-k})\lambda^{-k}G_k(y^2 = 4x^3 - 4x,\ dx/y) \qquad (3.9.9)$$
$$= (1 - p^{k-1}\mu^{-k})\lambda^{-k}2^k\frac{h_k}{k} \qquad \text{for} \quad k \geq 1$$

where μ is the "unit root". We will recall its precise value below. As a corollary, we obtain the Kummer congruences for the Hurwitz numbers:

$$\left\{\begin{array}{l} \text{Whenever a polynomial } \sum_{k\geq 1} c_k x^k \text{ with} \\ \text{coefficients in } C \text{ satisfies } \sum c_k a^k \in p^\nu \mathcal{O} \\ \text{for all } a \in \mathbf{Z}_p^\times, \text{ then for each } a \in \mathbf{Z}_p^\times \text{ the} \\ \text{Hurwitz numbers satisfy} \\ \qquad \sum (1 - a^k)(1 - p^{k-1}\mu^{-k})\lambda^{-k}\cdot 2^k \dfrac{h_k}{k} \in p^\nu \mathcal{O}. \end{array}\right. \tag{3.9.10}$$

The Relation to L-series with Grössencharacteren. We recall that the numerator of the zeta function of $y^2 = 4x^3 - 4x$ over $\mathbf{F}_p$ is given by

$$\begin{aligned} L_p(T) &= (1 - T)(1 - pT)Z_p(T) \\ &= \begin{cases} 1 + pT^2 & \text{if } \ p \equiv 3 \bmod 4 \\ (1 - \pi T)(1 - \bar{\pi} T) & \text{if } \ p \equiv 1 \bmod 4 \end{cases} \end{aligned} \tag{3.9.11}$$

where π and $\bar{\pi}$ are the unique Gaussian integers satisfying

$$\begin{cases} \pi\bar{\pi} = p \\ \pi, \bar{\pi} \equiv 1 \bmod (2 + 2i). \end{cases} \tag{3.9.12}$$

The L-series of this curve over $\mathbf{Z}[1/2]$ is the Dirichlet series

$$\begin{aligned} L(s) &\overset{\text{dfn}}{=\!=} \prod_{p \neq 2} \frac{1}{L_p(p^{-s})} \\ &= \prod_{p\equiv 3(4)} \frac{1}{1 + p^{1-2s}} \prod_{p\equiv 1(4)} \frac{1}{(1 - \pi p^{-s})(1 - \bar{\pi} p^{-s})} \end{aligned} \tag{3.9.13}$$

which we may more conveniently express as an infinite product over the odd (prime to 2) primes $\mathcal{Y}$ of $\mathbf{Z}[i]$

$$L(s) = \prod_{\mathcal{Y}\ \text{odd}} \left(\frac{1}{1 - \pi(N\mathcal{Y})^{-s}}\right) \qquad \begin{array}{l} \text{where } \pi \text{ is the unique} \\ \text{generator of } \mathcal{Y} \text{ such that} \\ \pi \equiv 1(2 + 2i). \end{array} \tag{3.9.14}$$

We denote by ρ the "identical" grossencharacter of $\mathbf{Z}[i]$, i.e. the ideal-character of conductor $(2 + 2i)$ defined on ideals prime to 2 by

$$\rho(\mathfrak{a}) = \alpha \qquad \text{if} \quad \mathfrak{a} = (\alpha), \qquad \alpha \equiv 1(2 + 2i). \tag{3.9.15}$$

We denote by $\bar{\rho}$ the complex conjugate of ρ.

$$\rho(\mathfrak{a}) = \bar{\alpha} \qquad \text{if} \quad \mathfrak{a} = (\alpha), \qquad \alpha \equiv 1(2 + 2i) \tag{3.9.16}$$

Then the L function $L(s)$ is precisely the L-series with grossencharacter ρ for the field $\mathbf{Q}(i)$:

$$\begin{array}{l} L(s) = L(s, \rho) = \prod_{\mathcal{Y}\,\text{odd}} \left(\dfrac{1}{1 - \rho(\mathcal{Y})\cdot N\mathcal{Y}^{-s}}\right) = \sum_{\mathfrak{a}\,\text{odd}} \dfrac{\rho(\mathfrak{a})}{N\mathfrak{a}^s}. \\ \qquad \| \\ L(s, \bar{\rho}) \end{array} \tag{3.9.17}$$

Now if we return to our prime $p \equiv 1(4)$, and if we *choose* a square root of -1 in $\mathbf{Z}_p$, then we determine an embedding $\mathbf{Z}[i] \to \mathbf{Z}_p$ (send i to the chosen $\sqrt{-1}$) which identifies $\mathbf{Z}_p$ with the $\mathcal{Y}$-adic completion of $\mathbf{Z}[i]$ for one of the prime ideals of $\mathbf{Z}[i]$ lying over p. On the other hand, we have the "unit root" $\mu \in \mathbf{Z}_p^{\times}$; it is given as a "function" of $\mathcal{Y}$ by the equation

$$\mu = \bar{\rho}(\mathcal{Y}) = N\mathcal{Y}/\rho(\mathcal{Y}) \tag{3.9.18}$$

(meaning that $\mu \in \mathbf{Z}_p$ is the image of the gaussian integer $\bar{\rho}(\mathcal{Y})$ under embedding corresponding to $\mathcal{Y}$).

Thus when we view $\mathbf{Z}_p$ as the $\mathcal{Y}$-adic completion of $\mathbf{Z}[i]$, we may write

$$\mathcal{L}_{(y^2=4x^3-4x,\lambda\, dx/y)}(\chi_k) = (1 - N\mathcal{Y}^{k-1}/\bar{\rho}^k(\mathcal{Y}))\lambda^{-k}2^k \frac{h_k}{k}. \tag{3.9.19}$$

Looking at the Euler factor $(1 - N\mathcal{Y}^{k-1}/\bar{\rho}^k(\mathcal{Y}))$, it is unavoidable to suppose that we are "really" looking at

$$L(1-k, (\bar{\rho})^{-k}) = \sum_{\mathfrak{a}\,\text{odd}} \frac{1}{N\mathfrak{a}^s\bar{\rho}(\mathfrak{a})^k}\Bigg|_{s=1-k} \tag{3.9.20}$$

which is "joined" by the functional equation with

$$L(0, (\rho)^{-k}) = \sum_{\mathfrak{a}\,\text{odd}} \frac{1}{\rho(\mathfrak{a})^k} \tag{3.9.21}$$

This last value is easily computed in the case of interest to us, namely $k = 4n$, $n \geq 1$:

$$\begin{aligned} L(0, (\rho)^{-4n}) &= \frac{1}{4} \sum_{\substack{\alpha\in\mathbf{Z}[i] \\ (\alpha,2)=1}} \frac{1}{\alpha^{4n}} \\ &= \frac{1}{4}\left(1 - \frac{1}{(1+i)^{4n}}\right) \sum_{\substack{\alpha\in\mathbf{Z}[i] \\ \alpha\neq 0}} \frac{1}{\alpha^{4n}} \\ &= \frac{1}{4}\left(1 - \left(\frac{-1}{4}\right)^n\right) \cdot \frac{(2\Omega)^{4n}}{(4n)!} h_{4n}. \end{aligned} \tag{3.9.22}$$

To summarize:

There is a constant $\lambda \in \mathbf{C}$ such that

$$\frac{2^{-4k}\lambda^{4k}\mathscr{L}(\chi_{4k})}{(1-p^{4k-1}\mu^{-4k})} = \frac{h_{4k}}{4k}$$

and there is a constant $\Omega \in \mathbf{C}$ such that (3.9.23)

$$\frac{(2\Omega)^{-k}\cdot L(0,(\rho)^{-4k})}{\left(1-\frac{-1}{4}\right)^{k}} = \frac{h_{4k}}{4k}$$

—the constants λ and Ω^{-1} are *analogous*, in the sense that

$\lambda\omega$ is formally logarithmic

$\Omega^{-1}\omega$ has integral periods on the real points of the curve, whose connected component is S^1, the compact form of $\mathbf{G}_m$.

Appendix A. Hurwitz's Form of the Functional Equation for L-series

We define $\zeta(s, a)$ be the series, convergent for $\mathrm{Re}(s) > 1$,

$$\zeta(s,a) = \sum_{n=0}^{\infty} \frac{1}{(n+a)^s} \qquad \text{(we'll take } 0 < a \leq 1) \tag{A.1}$$

It has a meromorphic continuation to the entire s-plane, which satisfies Hurwitz's functional equation:

$$\zeta(s,a) = \frac{2\Gamma(1-s)}{(2\pi)^{1-s}}\left\{\sin\left(\frac{s\pi}{2}\right)\sum_{n\geq 1}\frac{\cos(2\pi an)}{n^{1-s}} + \cos\left(\frac{s\pi}{2}\right)\sum_{n\geq 1}\frac{\sin(2\pi an)}{n^{1-s}}\right\} \tag{A.2}$$

for $\mathrm{Re}(s) < 0$.

Thus for $\mathrm{Re}(s) > 1$ we have

$$\begin{aligned}\zeta(1-s,a) = \Bigg\{&\frac{2\Gamma(s)}{(2\pi)^s}\sin\left(\frac{(1-s)\pi}{2}\right)\sum_{n\geq 1}\frac{\cos(2\pi an)}{n^s}\\ &+\cos\left(\frac{(1-s)\pi}{2}\right)\sum\frac{\sin(2\pi an)}{n^2}\Bigg\}\end{aligned} \tag{A.3}$$

If $s = 2k$ is an even integer, then

$$\sin\left((1-2k)\frac{\pi}{2}\right) = \sin\left(\frac{\pi}{2} - k\pi\right) = (-1)^k \sin\left(\frac{\pi}{2}\right) = (-1)^k$$

$$\cos\left((1-2k)\frac{\pi}{2}\right) = \cos\left(\frac{\pi}{2} - k\pi\right) = (-1)^k \cos\left(\frac{\pi}{2}\right) = 0$$

$$\begin{aligned}\zeta(1-2k, a) &= \frac{2\Gamma(2k)}{(2\pi)^{2k}}(-1)^k \sum_{n\geq 1} \frac{\cos(2\pi an)}{n^{2k}} \\ &= \frac{2\cdot(2k-1)!}{(2\pi)^{2k}}(-1)^k \sum_{n\geq 1} \frac{\frac{1}{2}(e^{2\pi ian} + e^{-2\pi ian})}{n^{2k}} \\ &= \frac{2\cdot(2k-1)!}{(2\pi)^{2k}}(i)^{2k} L(2k, \tfrac{1}{2}(\psi_a + \psi_{-a}))\end{aligned} \tag{A.4}$$

if $s = 2k + 1$ is an odd integer then

$$\sin\left((1-1-2k)\frac{\pi}{2}\right) = \sin(-k\pi) = 0$$

$$\cos\left((1-1-2k)\frac{\pi}{2}\right) = \cos(-k\pi) = (-1)^k$$

$$\begin{aligned}\zeta(1-(2k+1), a) &= \frac{2\Gamma(sk+1)}{(2\pi)^{2k+1}}(-1)^k \sum \frac{\sin(2\pi an)}{n^{2k+1}} \\ &= \frac{2(2k)!\,i^{2k}}{(2\pi)^{2k+1}} \sum \frac{\frac{1}{2i}(e^{2\pi ian} - e^{-2\pi ian})}{n^{2k+1}} \\ &= \frac{2(2k)!\,i^{2k-1}}{(2\pi)^{2k+1}} L(2k+1, \tfrac{1}{2}(\psi_a - \psi_{-a}))\end{aligned} \tag{A.5}$$

where we denote by ψ_a the function

$$\psi_a(x) = e^{2\pi iax}$$

Thus

$$\left\{\begin{aligned}\zeta(1-2k, a) &= \frac{2(2k-1)!}{(2\pi i)^{2k}} L(2k, \tfrac{1}{2}(\psi_a + \psi_{-a})) \\ \zeta(1-(2k+1), a) &= \frac{2(2k)!\,i^{2k+1}i^{2k-1}}{(2\pi i)^{2k+1}} L(2k+1, \tfrac{1}{2}(\psi_a - \psi_{-a})) \\ &= \frac{2(2k)!}{(2\pi i)^{2k+1}} L(2k+1, \tfrac{1}{2}(\psi_a - \psi_{-a}))\end{aligned}\right. \tag{A.6}$$

so in all cases, for integers $k \geq 2$, we have

$$\zeta(1-k, a) = \frac{2(k-1)!}{(2\pi i)^k} L(k, \tfrac{1}{2}(\psi_a + (-1)^k \psi_{-a}) \tag{A.7}$$

Now if $a = A/N$, with $A, N \in \mathbf{Z}$, and if we define

$$\begin{cases} f_A = \text{the characteristic function of } A \bmod N \text{ as function on } \mathbf{Z}/N\mathbf{Z} \\ \psi_A: \quad x \to e^{2\pi i A x/N} \text{ as function on } \mathbf{Z}/N\mathbf{Z} \end{cases} \tag{A.8}$$

then

$$\begin{aligned} \zeta(1-k, a) &= \sum_n (n+a)^{k-1} \\ &= \sum_n \left(\frac{nN+A}{N}\right)^{k-1} = N^{1-k} L(1-k, f_A) \end{aligned} \tag{A.9}$$

Thus we obtain

$$L(1-k, f_A) = \frac{2(k-1)!N^{k-1}}{(2\pi i)^k} L(k, \tfrac{1}{2}(\psi_A + (-1)^k \psi_{-A})) \tag{A.10}$$

This shows in particular that

$$\begin{aligned} L(1-k, f_A) &= (-1)^k L(1-k, f_{-A}) \\ &= L(1-k, \tfrac{1}{2}(f_A + (-1)^k f_{-A})) \end{aligned} \tag{A.11}$$

If we define the Fourier transform on $\mathbf{Z}/N\mathbf{Z}$ by

$$\hat{f}(y) = \frac{1}{N} \sum f(x) \zeta^{-xy} \qquad \zeta = e^{2\pi i/N} \tag{A.12}$$

then

$$\begin{cases} f_A = \hat{\psi}_A \\ \hat{f}_A = \dfrac{1}{N} \psi_{-A} \end{cases} \tag{A.13}$$

We may now rewrite (A.10–11) in two equivalent forms:

For any function F on $\mathbf{Z}/N\mathbf{Z}$ of parity $k(F(-x) = (-1)^k F(x))$, we have

$$L(1-k, \hat{F}) = \frac{2(k-1)!N^{k-1}}{(2\pi i)^k} L(k, F) \qquad \text{for} \quad k \geq 2 \tag{A.14}$$

For any function F on $\mathbf{Z}/N\mathbf{Z}$, and any integer $k \geq 2$, we have

$$L(1-k, F) \tag{A.15}$$
$$\begin{cases} \dfrac{2(k-1)!N^k(-1)^k}{(2\pi i)^k} L(k, \hat{F}) & \text{if} \quad F(-x) = (-1)^k F(x) \\ \\ 0 & \text{if} \quad F(-x) = -(-1)^k F(x) \end{cases}$$

Appendix B. A slight generalization of our measures, adapted to complex multiplication curves

B.1 Let's continue to work over the same ground ring W, but no longer *fix* a primitive N'th root of unity $\zeta \in W$. Then for each choice of ζ, we have the ring $V(W, \zeta, \Gamma(N))$ which we had previously denoted simply $V(W, \Gamma(N))$. We define

$$\mathbf{V}(W, \Gamma(N)) = \bigoplus_{\zeta} V(W, \zeta, \Gamma(N))$$

the sum taken over the $\varphi(n)$ primitive N'th roots of unity ζ in W. The ring $\mathbf{V}(W, \Gamma(N))$ is exactly the ring of all generalized modular functions on $\Gamma(N)$ as defined in 1.1, save that we no longer fix the determinant of the e_N pairing.

The group $GL_2(\mathbf{Z}/N\mathbf{Z})$, rather than "just" $SL_2(\mathbf{Z}/N\mathbf{Z})$, operates on $\mathbf{V}(W, \Gamma(N))$ in the obvious manner $([g]f)(E, \varphi, \alpha_N) = f(E, \varphi, g^{-1} \circ \alpha_N)$. The ring $V(W, \Gamma_\infty(N))$ may be viewed in this context as the subring of *invariants* of the subgroup

$$\left\{ \begin{pmatrix} 1 & x \\ 0 & \alpha \end{pmatrix} \middle| \; x \in \mathbf{Z}/N\mathbf{Z}, \alpha \in (\mathbf{Z}/N\mathbf{Z})^\times \right\} \subset GL_2(\mathbf{Z}/N\mathbf{Z})$$

in $\mathbf{V}(W, \Gamma(N))$.

Another "advantage" is that the Frobenius endomorphism operates on $\mathbf{V}(W, \Gamma(N))$, through the rule

$$(\text{Frob}\, f)(E, \varphi, \alpha_N) = f(E/E_{\text{can}}, \varphi \cdot \check{\pi}, \pi(\alpha_N))$$

where

$E_{\text{can}} \subset E$ is the *canonical* subgroup

π: $E \to E/E_{\text{can}}$ is the projection, $\check{\pi}$ its (etale) dual

$\pi(\alpha_N)$ is the unique level N structure on E/E_{can} making the diagram

$$\begin{tikzcd} & (\mathbf{Z}/N\mathbf{Z})^2 & \\ {}_N E \arrow[ur, "\alpha_N"] \arrow[rr, "\pi", "\sim"'] & & {}_N(E/E_{\text{can}}) \arrow[ul, "\pi(\alpha_N)"'] \end{tikzcd}$$

[It is clumsy (though possible!, cf. [6]) to formulate the Frobenius endomorphism of $V(W, \Gamma(N))$ as a σ-linear endomorphism, the difficulty being that $\det(\pi(\alpha_N)) = (\det(\alpha_N))^p$,]

We may carry over the proof of the "Key Lemma" to our new situation, and we get:

KEY LEMMA FOR $\mathbf{V}(W, \Gamma(N))$. *Let f be an arbitrary element of $\mathbf{V}(W, \Gamma(N)) \otimes W[1/p]$. Suppose that on* each *of the $\varphi(N)$ components of $\mathbf{V}(W, \Gamma(N))$, there is at least one cusp at which the q-expansion is integral, except possibly for its constant term. Then for any element $(a, h) \in \mathbf{Z}_p^\times \times SL_2(\mathbf{Z}/N\mathbf{Z})$, the difference $f - [a, h]f$ lies in $\mathbf{V}(W, \Gamma(N))$.*

B.2 We may now define the Eisenstein measure on $\mathbf{Z}_p \times (\mathbf{Z}/N\mathbf{Z})^2$, as follows. For $(a, h) \in \mathbf{Z}_p^\times \times SL_2(\mathbf{Z}/N\mathbf{Z})$, we define $2\mathbf{H}^{a,h}$ as the pseudodistribution on $\mathbf{Z}_p \times (\mathbf{Z}/N\mathbf{Z})^2$, with values in $\mathbf{V}(W, \Gamma(N))$, whose value on $x^k \cdot F$ is

$$(1 - [a, h]) \cdot 2G_{k+1,F}$$

where $G_{k,F}$ is the Eisenstein series in $\mathbf{V}(W, \Gamma(N)) \otimes W[1/p]$ defined by

$$G_{k,F}(E, \omega, \alpha_N) = \begin{cases} \displaystyle\sum_{a,b \bmod N} F(a, b) G_k(E, \omega, \alpha_N{}^{-1}(a, b)) & F \text{ of parity } (-1)^k \\ \\ 0 & F \text{ of parity } (-1)^{k+1} \end{cases}$$

The Key Lemma (applicable thanks to all our q-expansion computations) assures us that this pseudo-distribution, which a priori takes values in $\mathbf{V}(W, \Gamma(N)) \otimes W[1/p]$, in fact takes values in $\mathbf{V}(W, \Gamma(N))$, and therefore extends to a *measure* $2\mathbf{H}^{a,h}$ with values in $\mathbf{V}(W, \Gamma(N))$. We might also observe that our present construction for $\Gamma(N)$ is compatible with the previous one for $\Gamma_{00}(N)$, in the following sense: For any function f on $\mathbf{Z}/N\mathbf{Z}$, if we define

$$F_f(a, b) = \begin{cases} \dfrac{1}{\mathrm{N}} \hat{\mathrm{f}}(\mathrm{a}) & \text{if } b = 0 \\ \\ 0 & \text{if } b \neq 0 \end{cases}$$

then we obtain the identity

$$G_{k,F_f} = G_{k,f}.$$

B.3 The transcendental expression for $G_{k,F}$ is, for $k \geq 3$,

$$G_{k,F}\left(L, \text{basis } e_1, e_2 \text{ of } \frac{1}{N}L\right) = \frac{(-1)^k(k-1)!}{2} \sum_{a,b \bmod N} F(a,b)A_k(L, ae_1 + be_2).$$

If we use $\frac{1}{N} \circ \alpha_N \colon L/NL \xrightarrow{\sim} \frac{1}{N}L/L \to (\mathbf{Z}/N\mathbf{Z})^2$ to *identify* $\hat{F}$ with a function (still noted $\hat{F}$) on L/NL, then we have

$$G_{k,F}\left(L, \frac{1}{N}L/L \xrightarrow{\sim} (\mathbf{Z}/N\mathbf{Z})^2\right) = \frac{(-1)^k(k-1)!N^k}{2} \sum_{\ell \in L-\{0\}} \frac{F(\ell)}{\ell^k}$$

B.4 Variances (compare 3.4.2). We make the group $\mathbf{Z}_p^\times \times GL_2(\mathbf{Z}/N\mathbf{Z})$ operate on the continuous functions on $\mathbf{Z}_p \times (\mathbf{Z}/N\mathbf{Z})^2$ by the action:

$$([b, g]\mathbf{F})(x, y) = b\mathbf{F}(bx, g^{-1}y) \qquad x \in \mathbf{Z}_p, y \in (\mathbf{Z}/N\mathbf{Z})^2$$

As noted, this group operates on $\mathbf{V}(W, \Gamma(N))$ by the rule

$$([b, g]f)(E, \varphi, \alpha_N) = f(E, b^{-1}\varphi, g^{-1} \circ \alpha_N)$$

It follows immediately from the definition of $G_{k,F}$

$$G_{k,F}(E, \varphi, \alpha_N) = \sum_y G_k(E, \varphi, \alpha_N{}^{-1}(y)) \cdot F(y)$$

that

$$[b, g]G_{k,F} = b^k G_{k,[g]F}$$

and hence, for any $(a, h) \in \mathbf{Z}_p^\times \times SL_2(\mathbf{Z}/N\mathbf{Z})$, we have

$$\begin{aligned}
[b, g] \cdot 2\mathbf{H}^{a,h}(x^k F(y)) &= [b, g]2G_{k+1,F} - [b, g][a, h]2G_{k+1,F} \\
&= b^{k+1}2(G_{k+1,[g]F} - a^{k+1}G_{k+1,[ghg^{-1}][g]F}) \\
&= b^{k+1}2\mathbf{H}^{a,ghg^{-1}}(x^k([g]F)(y)) \\
&= 2\mathbf{H}^{a,ghg^{-1}}([b, g](x^k \cdot F))
\end{aligned}$$

An obvious limiting argument then gives

Variance Formulas. For $(a, h) \in \mathbf{Z}_p^\times \times SL_2(\mathbf{Z}/N\mathbf{Z})$, $(b, g) \in \mathbf{Z}_p^\times \times GL_2(\mathbf{Z}/N\mathbf{Z})$, and $\mathbf{F}$ a continuous function on $\mathbf{Z}_p \times (\mathbf{Z}/N\mathbf{Z})^2$ we have an identity in $\mathbf{V}(W, \Gamma(N))$:

$$[b, g](2\mathbf{H}^{a,h}(\mathbf{F})) = 2\mathbf{H}^{a,ghg^{-1}}([b, g](\mathbf{F}))$$

B.5 We may also define the $\mathbf{V}(W, \Gamma(N))$-valued measure $2J^{a,h}$ on $\mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^2$ by the formula

$$2J^{a,h} = \text{the restriction to } \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^2 \text{ of } 2\mathbf{H}^{a,b}.$$

For any continuous character $\chi\colon \mathbf{Z}_p^\times \to B_0^\times$, we define

$$2J^{a,h}_{\chi,F} = 2J^{a,g}(\chi\cdot\chi_{-1}F)$$

(where χ_{-1} is the character $x \to x^{-1}$ on $\mathbf{Z}_p^\times$), which we know to be an element of $\mathbf{V}(B_0, \Gamma(N))$ of *weight* χ.

When B_0 is an integral domain with fraction field K, and χ is non-trivial, we can define

$$J_{\chi,F} = \frac{1}{1-\chi(a)} J^{a,1}_{\chi,F} \in \mathbf{V}(B_0, \Gamma(N)) \otimes K$$

by choosing $a \in \mathbf{Z}_p^\times$ where $\chi(a) \neq 1$.

The analogue of 3.5.6 is

LEMMA 3.5.6. *Let $k \geq 1$ an integer, F any function on $(\mathbf{Z}/N\mathbf{Z})^2$; then $J_{k,F} = G_{k,F} - p^{k-1}\,\mathrm{Frob}(G_{k,F})$ in $\mathbf{V}(W, \Gamma(N)) \otimes W[1/p]$.*

Proof. Imitating the proof of 3.5.6, it suffices to check that at one cusp on each component of $\mathbf{V}(W, \Gamma(N))$, both sides have the same q-expansions.

Let's use the cusps $(\mathrm{Tate}(q^N), q, \zeta^j)$, $\zeta = e^{2\pi i/N}$, $j \in (\mathbf{Z}/N\mathbf{Z})^\times$, whose given level N structures have all possible determinants. We may and will suppose F is the characteristic function of (a, b). Then

$$\begin{aligned} G_{k,F}(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, (q, \zeta^j)) &= G_k(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, q^a\zeta^{bj}) \\ &= \tfrac{1}{2} \sum_{\substack{n\geq 1\\ m\geq 0}} n^{k-1}(q^{mN+a})^n)^{nbj} \qquad \text{(by 2.4.5)} \\ &\quad + \frac{(-1)^k}{2} \sum_{m,n\geq 1} n^{k-1}(q^{mN-a})^n\zeta^{-nbj} \end{aligned}$$

Because the restriction of the function x^k to $\mathbf{Z}_p^\times$ (reextended by zero to all of $\mathbf{Z}_p$) is uniformly approximated by the functions $x^{k+(p-1)p^r}$, we have

$$\begin{aligned} J_{k,F} &= \tfrac{1}{2} \sum_{\substack{n\geq 1\\ m\geq 0\\ (p,n)=1}} n^{k-1}(q^{mN+a})^n\zeta^{nbj} \\ &\quad + \frac{(-1)^k}{2} \sum_{\substack{m,n\geq 1\\ (p,n)=1}} n^{k-1}(q^{mN-a})^n\zeta^{-nbj} \end{aligned}$$

Thus it remains to check that

$$\begin{aligned}
&\mathrm{Frob}(G_{k,F})(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, (q, \zeta^j)) \\
&\quad = \tfrac{1}{2} \sum_{\substack{n\geq 1\\ m\geq 0}} p^{k-1}n^{k-1}(q^{mN+a})^{np}\zeta^{npbj} \\
&\qquad + \frac{(-1)^k}{2} \sum_{m,n\geq 1} p^{k-1}n^{k-1}(q^{mN-a})^{np}\zeta^{-npbj} \\
&\quad = G_{k,F}(\mathrm{Tate}(q^{Np}), \omega_{\mathrm{can}}, q^{ap}\cdot\zeta^{pbj}).
\end{aligned}$$

But this is easily seen to be the case, for the canonical subgroup of $\mathrm{Tate}(q^N) = \mathbf{G}_m/q^{N\mathbf{Z}}$ is $\boldsymbol{\mu}_p$. The quotient is $\mathrm{Tate}(q^{Np}) = \mathbf{G}_m/q^{pN\mathbf{Z}}$, and the projection map is the one deduced from the p'th power map on $\mathbf{G}_m$ by passage to quotients. Thus

$$\begin{aligned}
\mathrm{Frob}(G_{k,F})(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, (q, \zeta^j)) &= G_{k,F}(\mathrm{Tate}(q^{Np}), \omega_{\mathrm{can}}, q^p, \zeta^{pj}) \\
&= G_k(\mathrm{Tate}(q^{Np}), \omega_{\mathrm{can}}, q^{ap}\zeta^{pjb})
\end{aligned}$$

which was the desired formula.

Application to complex multiplication curves

B.6 Let D be the ring of integers in a fixed quadratic imaginary extension of $\mathbf{Q}$, and fix an isomorphism of abelian groups

$$(\mathbf{Z}/N\mathbf{Z})^2 \xrightarrow{\sim} D/ND.$$

This determines an inclusion of groups

$$(D/ND)^\times \hookrightarrow GL_2(\mathbf{Z}/N\mathbf{Z})$$

which makes the diagram below commute.

$$\begin{tikzcd}
(D/ND)^\times \arrow[rr, hook] \arrow[dr, "\mathrm{Norm}"'] & & GL_2(\mathbf{Z}/N\mathbf{Z}) \arrow[dl, "\det"] \\
& (\mathbf{Z}/N\mathbf{Z})^\times &
\end{tikzcd}$$

For any $(a, d_1) \in \mathbf{Z}_p^\times \times$ (elements of Norm 1 in $(D/ND)^\times$), we obtain $\mathbf{V}(W, \Gamma(N))$-valued measures $2\mathbf{H}^{a,d_1}$ on $\mathbf{Z}_p \times D/ND$ and $2J^{a,d_1}$ on $\mathbf{Z}_p^\times \times D/ND$ by "transport of structure". The transcription of the formula (3.4.3–4) becomes

Variance Formula. For $(a, d_1) \in \mathbf{Z}_p^\times \times$ (elements of norm 1 in $(D/ND)^\times$), $(b, d) \in \mathbf{Z}_p^\times \times (D/ND)^\times$, and $\mathbf{F}$ a continuous function on $\mathbf{Z}_p \times D/ND$ (resp. on $\mathbf{Z}_p^\times \times D/ND$), we have the following identities on $\mathbf{V}(W, \Gamma(N))$:

$$[b, d](2\mathbf{H}^{a,d_1}(\mathbf{F})) = 2\mathbf{H}^{a,d_1}([b, d](\mathbf{F}))$$

(resp.)
$$[b, d](2J^{a,d_1}(\mathbf{F})) = 2J^{a,d_1}([b, d](\mathbf{F}))$$

[One must remember that $(b, d) \in \mathbf{Z}_p^\times \times (D/ND)^\times$ acts on functions $\mathbf{F}$ on $\mathbf{Z}_p \times D/ND$ by the formula $[b, d]\mathbf{F}(x, y) = b\mathbf{F}(bx, d^{-1}y)$.]

B.7 Let ψ be a Dirichlet character of D of conductor N; we may view ψ as a group homomorphism

$$\psi\colon \quad (D/ND)^\times \to C^\times$$

which is extended by zero to all of D/ND.

Let (E, ω) be an elliptic curve as in 3.7, and fix a level N structure α_N on E. In the notations of 3.7, we define the p-adic L-series $\mathscr{L}_{(E,\lambda\omega,\alpha_N)}$ as the C-valued function on $\mathrm{Hom}_{\mathrm{contin}}(\mathbf{Z}_p^\times \times (D/ND)^\times, C^\times)$—{characters trivial on $\mathbf{Z}_p^\times \times$ (elts of norm 1)} by the formula

$$\mathscr{L}_{(E,\lambda\omega,\alpha_N)}(\chi \times \psi) = \frac{1}{1 - \chi(a)/\psi(d_1)} \cdot 2J^{a,d_1}_{\chi,\psi}(E, \lambda\omega, \alpha_N)$$

(this is easily seen to be independent of the choice of point (a, d_1) where χ/ψ is $\neq 1$). It has at worst a first order pole at the excluded characters (which are precisely those which factor through the composite

$$\mathbf{Z}_p^\times \times (D/ND)^\times \xrightarrow{pr_2} (D/ND)^\times \xrightarrow{\text{Norm}} (\mathbf{Z}/N\mathbf{Z})^\times)$$

in the sense that for any point $(a, d_1) \in \mathbf{Z}_p^\times \times$ (elts of norm 1), the function

$$\chi\cdot\psi \to (1 - \chi(a)/\psi(d_1))\mathscr{L}_{(E,\lambda\omega,\alpha_N)}(\chi\cdot\psi)$$

extends to a continuous $\mathscr{O}$-valued function on all of $\mathrm{Hom}_{\mathrm{contin}}(\mathbf{Z}_p^\times \times (D/ND)^\times, C^\times)$.

The Kummer congruences are also satisfied:

$$\begin{cases} \text{Whenever a } C\text{-linear combination of characters } \sum c_{\chi\psi}\chi\psi \text{ satisfies} \\ \sum c_{\chi\psi}\cdot\chi(b)\psi(d) \in p^\omega\cdot\mathscr{O} \qquad \text{for all} \quad (b, d) \in \mathbf{Z}_p^\times \times)d/ND)^\times, \\ \text{then for any } (a, d_1) \in \mathbf{Z}_p^\times \times \text{(elts of norm 1), we have} \\ \sum c_{\chi\psi}(1 - \chi(a)/\psi(d_1))\mathscr{L}_{(E,\lambda\omega,\alpha_N)}(\chi\psi) \in p^\nu\mathscr{O}. \end{cases}$$

B.8 Suppose now that the curve E has D as its *endomorphism ring*, and that the hypothesis of 3.8, the existence of $F_p \in D$ lifting absolute Frobenius, is fulfilled. We further suppose that the composed isomorphism

$$N^E \xrightarrow[\sim]{\alpha_N} (\mathbf{Z}/N\mathbf{Z})^2 \xrightarrow{\sim} D/ND$$

is an isomorphism of D/ND-modules.

Then we may carry through the computations of section 3.8, which show that, in the notations of that section we have

$$\begin{array}{rl} \mathrm{Frob}(G_{k,\psi})(E, \lambda\omega, \alpha_N) = & G_{k,\psi}(E, \mu\lambda\omega, \alpha_N \cdot F_p{}^{-1}) \\ & \qquad \| \\ & \psi(F_p)^{-1} \cdot \mu^{-k} G_{k,\psi}(E, \lambda\omega, \alpha_N), \end{array}$$

(Notice that $\mu = p/F_p$ in D.) Combining this with the formula (3.5.6 vis A.6) we obtain the explicit formula

$$\begin{aligned} \mathscr{L}_{(E,\lambda\omega,\alpha_N)}(\chi_k\psi) &= 2(1 - p^{k-1}/\mu^k\psi(F_p))G_{k,\psi}(E, \lambda\omega, \alpha_N) \\ &= 2(1 - p^{k-1}/\mu^k\psi(F_p))\cdot\lambda^{-k}G_{k,\psi}(E, \omega, \alpha_N) \end{aligned}$$

An explicit look at the Lemniscate curve $y^2 = 4x^3 - 4x$ ($D = \mathbf{Z}[i]$, $p \equiv 1(4)$).

B.9 The presence of the automorphism i of this curve E dictates that we have

$$\mathscr{L}_{(y^2=4x^3-4x,\lambda\, dx/y,\alpha_N)}(\chi_k\psi) = 0 \qquad \text{unless} \quad \psi(i) = i^k,$$

so let us henceforth assume that $\psi(i) = i^k$. Then

$$\mathscr{L}_{(y^2=4x^3-4x,\lambda\, dx/y.\alpha_N)}(\chi_k\psi) = 2(1 - p^{k-1}/\mu^k\psi(F_p))\lambda^{-k}G_{k,\psi}(E, \omega, \alpha_N)$$

When we view $G_{k,\psi}(E, \omega, \alpha_N)$ as a *complex* number, it is given by

$$\begin{aligned} &G_{k,\psi}(\Omega\cdot\mathbf{Z}[i], \alpha_N) \\ &\quad = \frac{(-1)^k(k-1)!}{2}\Omega^{-k}N^k \sum_{a+bi\neq 0} \frac{\psi(a+bi)}{(a+bi)^k} \\ &\quad = \frac{(-1)^k(k-1)!}{2}\Omega^{-k}N^k\cdot 4\left(\frac{1}{1-(\psi(1+i)/(1+i)^k)}\right)\sum_{\mathfrak{a}} \psi(\mathfrak{a})\rho(\mathfrak{a})^{-k}. \end{aligned}$$

where the sum is taken over all *ideals* of $\mathbf{Z}[i]$ which are prime to $2N$, and where $\psi\rho^{-k}$ is the grossencharacter of (not necessarily exact) conductor $(2 + 2i)N$ defined by

$$\psi\rho^{-k}(\mathfrak{a}) = \psi(\alpha)/\alpha^k \qquad \text{if} \quad \mathfrak{a} = (\alpha) \qquad \text{with} \quad \alpha \equiv 1 \bmod (2 + 2i).$$

So we may summarize our findings in the following "equality" of a p-adic and a complex expression for the same algebraic number $G_{k,\psi}(E, \omega, \alpha_N)$

$$G_{k,\psi}(y^2 = 4x^3 - 4x, dx/y, \alpha_N)$$

$$= \frac{\lambda^k}{2}\left(\frac{1}{1 - p^{k-1}/\mu^k\psi(F_p)}\right)\mathscr{L}_{(y^2=4x^3-4x,\lambda\, dx/y,\alpha_N)}(\chi_k\psi)$$

$$\frac{(-1)^k(k-1)!}{2}\,\Omega^{-k}N^k 4\left(\frac{1}{1 - \dfrac{\psi(1+i)}{(1+i)^k}}\right)L(0, \psi\rho^{-k}).$$

From the point of view of p-adically interpolating values of L-series with grossencharacter, the hypothesis that $\psi(i) = i^k$ is not very natural because for $k \geq 3$ and *any* ψ, the value $L(0, \psi\rho^{-k})$ is given by its absolutely convergent Euler product, hence is *non-zero*. So let us explain how our methods apply to *all* these values.

Let us denote by ϵ the following $\mathbf{Z}$-valued function on the Gaussian integers $\mathbf{Z}[i]$:

$$\epsilon(a+bi) = \begin{cases} 1 & \text{if } \ a + bi \equiv 1 \bmod 2 + 2i \\ 0 & \text{if } \ \text{not} \end{cases}$$

Then the product $\epsilon\psi$ is a function on $\mathbf{Z}[i]/(4N)$,

$$\epsilon\psi(a+bi) = \begin{cases} \psi(a+bi) & \text{if } \ a + bi \equiv 1(2+2i) \\ 0 & \text{if } \ \text{not} \end{cases}$$

which by transport of structure (B.8) becomes a function on $(\mathbf{Z}/4N\mathbf{Z})^2$.

Consider the Eisenstein series of level $4N$ and weight k, $G_{k,\epsilon\psi}$. It's value on the lattice $L = \mathbf{Z}[i]$ with basis $1/4N$, $i/4N$ of $(1/4N)L/L$ is the archimedean series

$$\frac{(-1)^k(k-1)!(4N)^k}{2}\sum_{a+bi\neq 0}\frac{\epsilon\psi(a+bi)}{(a+bi)^k}$$

$$= \frac{(-1)^k(k-1)!(4N)^k}{2}\sum_{a+bi\equiv 1(2+2i)}\frac{\psi(a+bi)}{(a+bi)^k}$$

$$= \frac{(-1)^k(k-1)!(4N)^k}{2}\sum_{\mathfrak{a}\text{ odd}}(\psi\rho^{-k})(\mathfrak{a})$$

$$= \frac{(-1)^k(k-1)!(4N)^k}{2}L(0, \psi\rho^{-k}).$$

From an algebraic point of view, the lattice $\Omega\cdot\mathbf{Z}[i]$ with level $4N$-structure given by $\Omega/4N$, $i\Omega/4N$ is none other than the curve $(y^2 = 4x^3 -$

$4x$, dx/y) with one of its level $4N$-structures α_{4N} (all of which are defined over the "ray-class field of conductor $4N$ over $\mathbf{Z}[i]$"):

$$\frac{(-1)^k(k-1)!(4N)^k\Omega^{-k}}{2} L(0, \psi\rho^{-k}) = G_{k,\epsilon\psi}(y^2 - 4x^3 - 4x, dx/y, \alpha_{4N}).$$

From the p-adic point of view, if we introduce the previously chosen p-adic transcendental unit λ such that $\lambda\ dx/y$ is formally logarithmic, we may reinterpret the algebraic value $G_{k,\epsilon\psi}(y^2 = 4x^3 - 4x, dx/y, \alpha_{4N})$ p-adically.

$$G_{k,\epsilon\psi}(y^2 = 4x^3 - 4x, dx/y, \alpha_{4N}) = \lambda^k \cdot G_{k,\epsilon\psi}(y^2 = 4x^3 - 4x, \lambda\ dx/y, \alpha_{3N}).$$

We next express this in terms of $J_{k,\epsilon\psi} = G_{k,\epsilon\psi} - P^{k-1}\ \mathrm{Frob}(G_{k,\epsilon\psi})$. Recall that for this curve, the Frobemus endomorphism F_p when viewed in $\mathbf{Z}[i]$, is the unique generator of $\mathcal{Y}$ satisfying $F_p \equiv 1 \bmod (2 + 2i)$; it follows from the definition of ϵ and the multiplicativity of ψ that we have the transformation equation

$$(\epsilon\psi)(F_p y) = \psi(F_p)\cdot(\epsilon\psi)(y) \qquad \text{for all} \quad y \in \mathbf{Z}[i]/(4N).$$

Thus we have (compare 3.8)

$$\mathrm{Frob}(G_{k,\epsilon})(y^2 = 4x^3 - 4x, \lambda\ dx/y, \alpha_{4N}) = \frac{1}{\mu^k\psi(F_p)} G_{k,\epsilon\psi}(y^2 = 4x^3 - 4x, \lambda\ dx/y, \alpha_{4N}),$$

and hence

$$J_{k,\epsilon\psi}\left(y^2 = 4x^3 - 4x, \frac{\lambda\ dx}{y}, \alpha_{4M}\right) = \left(1 - \frac{p^{k-1}}{\mu^k\psi(F_p)}\right)\lambda^{-k}G_{k,\epsilon\psi}(y^2 = 4x^3 - 4x, dx/y, \alpha_{4N}).$$

If we choose any $a \in \mathbf{Z}_p^\times$ and any $d \in (\mathbf{Z}[i]/(4N))^\times$ of norm *one* which is $\equiv 1 \bmod (2 + 2i)$, we can express the generalized modular function $J_{k,\epsilon\psi}$ in terms of the Eisenstein measure $J^{a,d}$ on $\mathbf{Z}_p^\times \times \mathbf{Z}[\mathrm{o}]/(4N)$:

$$J_{k,\epsilon\psi} = \frac{1}{1 - a^k/\psi(d)} J^{a,d}(x^{k-1}\epsilon\psi)$$

Evaluating at the lemniscate curve gives the equality of values

$$J_{k,\epsilon\psi}(y^2 = 4x^3 - 4x, \lambda\ dx/y, \alpha_{4N}) = \frac{1}{1 - a^k/\psi(d)} J^{a,d}(x^{k-1}\epsilon\psi)(y^2 = 4x^3 - 4x, \lambda\ dx/y, \alpha_{4N}).$$

So for each (a, d) as above, we may define a measure $\mu^{(a,d)}$ on $\mathbf{Z}_p^\times \times \mathbf{Z}[i]/(N)$, with values in $\mathcal{O}_C$, by decreeing that

$$\binom{x}{n} F \xrightarrow{\mu^{(a,d)}} J^{a,d}\left(\binom{x}{n} \epsilon F\right)(y^2 = 4x^3 - 4x, \lambda\, dx/y, \alpha_{4N})$$

This "lemniscate measure" $\mu^{(a,d)}$ is related to the problem of interpolating the classical L-series values $L(0, \psi\rho^{-k})$ by following two formulas valid for any character ψ of $(\mathbf{Z}[i]/(N))^\times$ and any integer $k \geq 3$:

$$\mu^{(a,d)}(x^{k-1}\psi)$$
$$= (1 - a^k/\psi(d))(1 - p^{k-1}/\mu^k\psi(F_p))\lambda^{-k}G_{k,\epsilon\psi}(y^2 = 4x^3 - 4x, dx/y, \alpha_{4N})$$

$$G_{k,\epsilon\psi}(y^2 = 4x^3 - 4x, dx/y, \alpha_{4N}) = \frac{(-1)^k(k-1)!(4N)^k\Omega^{-k}}{2} L(0, \psi\rho^{-k}).$$

Appendix C. Modular Definition of Eisenstein Series of Weight One, and Their Relation to the Universal Extension

In this final appendix, we answer the question raised before (2.8.2). The answer is completely classical. It was crystallized by the reading of Lang's book [9], esp. pp. 240–241, a conversation with Mazur, and yet another reading of Whittaker and Watson [20]!

C.1 The Universal Extension. Let S be an arbitrary scheme, and E/S an elliptic curve. We will freely identify E with its "Picard variety" $\mathrm{Pic}^0_{E/S}$. Recall that as functor on S-schemes, $\mathrm{Pic}^0_{E/S}$ is the f.p.p.f. sheaf associated to the presheaf

$T \mapsto$ isomorphism classes of invertible sheaves $\mathcal{L}$ on $E \times_S T$ which point by point on T are of degree zero.

The identification

$$E \xrightarrow{\sim} \mathrm{Pic}^0_{E/S}$$

is given by

$P \in E(T) \mapsto$ the invertible sheaf $I^{-1}(P) \otimes I(0)$, where $I^{-1}(P)$ is the inverse of the ideal sheaf which defines the section P of $E \times_S T$, and $I(0)$ is the ideal sheaf of the zero-section of $E \times_S T$.

Now let $E^\dagger$ be the "universal extension" of E by a vector group. It is a smooth commutative S-group scheme which sits in an exact sequence of S-groups

$$0 \to \omega_{E/S} \to E^{\dagger} \xrightarrow{\pi} E \to 0$$

in which we have written $\omega_{E/S}$ for the "vector group" whose T-valued points are given by

$$\omega_{E/S}(T) = H^0(E \underset{S}{\times} T, \Omega^1_{E \underset{S}{\times} T/T}).$$

The group $E^{\dagger}$, as functor on S-schemes, is the f.p.p.f. sheaf associated to the presheaf

$T \mapsto$ isomorphism classes of pairs $(\mathscr{L}, \nabla)$ consisting of an invertible sheaf $\mathscr{L}$ on $E \underset{S}{\times} T$ which has degree zero over each point of T, and of a (necessarily integrable) T-connection ∇ on $\mathscr{L}$.

When T is an S-scheme which is (absolutely) affine, then the long exact f.p.p.f. cohomology sequence gives a short exact sequence of abelian groups

$$0 \to H^0(E \underset{S}{\times} T, \Omega^1_{E \underset{S}{\times} T/T}) \to E^{\dagger}(T) \to E(T) \to 0$$

(the next term would be $H^1_{\text{fppf}}(T, (\omega_{E/S})_T)$, which vanishes because T is affine and ω is quasi-coherent).

LEMMA C.1.1. *Let n be an integer which is invertible on S, and let $P \in E(S)$ be a point of (not necessarily exact) order n. Then there is a* unique *point*

$$P^{\text{can}} \in E^{\dagger}(S)$$

which lies over P, and which has (not necessarily exact) order n in $E^{\dagger}(S)$.

Proof. Unicity is clear, for the difference of any two would be a section of the $\mathcal{O}_S$-module $\omega_{E/S}$ which is killed by n. Further, for any S-scheme T which is absolutely affine, we can find *some* point $\tilde{P} \in E^{\dagger}(T)$ which maps onto P in $E(T)$. But $n\tilde{P}$ maps onto $0 \in E(T)$, hence $n\tilde{P} = \omega$ is a section of ω over T. Since n is invertible on T, the section $(1/n)\omega$ of ω makes sense, and $\tilde{P} - (1/n)\omega$ is point of $E^{\dagger}(T)$ lying over P and having order n. So we have the desired $P_T{}^{\text{can}} \in E^{\dagger}(T)$ for all absolutely affine S-schemes T. By the unicity, it follows that these $P_T{}^{\text{can}}$ *descend* to give the desired element $P^{\text{can}} \in E^{\dagger}(S)$.

We now recall the dictionary between connections on invertible sheaves on curves and "differentials of the third kind" (compare [5], sections 7.2–7.4).

LEMMA C1.2. *Let S be any scheme, X/S a smooth curve, $P_i \in X(S)$ a finite number of* disjoint *sections, and n_i some integers. Then an S-connection on the invertible sheaf $\otimes \quad I(P_i)^{\otimes n_i}$ is given by any element of $H^0(X, \Omega^1_{X/S} \otimes I^{-1}(P_1) \otimes \ldots \otimes I^{-1}(P_m))$ (a differential one-form on X/S having at worst first order poles along the P_i and holomorphic elsewhere) whose* residue *along each P_i is the image of the integer $-n_i$ in $\Gamma(S, \mathcal{O}_S)$.*

Proof. The correspondence is as follows. The differential ω gives the connection

$$\nabla_\omega : \quad \otimes I(P_i)^{\otimes n_i} \to \otimes I(P_i)^{\otimes n_i} \otimes \Omega^1_{X/S}$$

defined by

$$\nabla_\omega(f) = df + f\omega.$$

Let's check this indeed defines a connection. For f a local invertible section, we may write

$$\nabla_\omega(f) = f\left(\frac{df}{f} + \omega\right)$$

and the hypothesis on the residues of ω assures that $(df/f) + \omega$ is a local section of $\Omega^1_{X/S}$. Any local section may be written fg with g a local section of $\mathcal{O}_X$, and the product rule gives

$$\nabla_\omega(fg) = f\,dg + g\,\nabla_\omega(f)$$

which shows that ∇_ω does indeed map $\otimes I(P_i)^{\otimes n_i}$ to $\otimes I(P_i)^{\otimes n_i} \otimes \Omega^1_{X/S}$.

Conversely, any connection is of the form $f \to df + f\omega$, and taking f to be a local invertible section shows that ω must have a worst first order pole at the P_i with the prescribed residues.

REMARK C.1.3. *Suppose that $S = Spec(k)$ with k a field. Let $P \in E(k)$ be a point of order N, with N prime to the characteristic of k. Then by Abel's theorem we can find a rational function f_P on E whose divisor is* $N[P] - N[0]$. *The function f_P is only unique up to $k^\times$-multiples, but df_P/f_P is unique. Moreover, the differential*

$$\frac{1}{N} \cdot df_P / f_P \stackrel{\text{dfn}}{=\!=} \omega_P^{\text{can}}$$

is independent *of the choice of the integer N prime to char(k) which kills P. It is a section of* $\Omega^1_{E/k} \otimes I^{-1}(P) \otimes I^{-1}(0)$ *with residue* 1 *at P and residue* -1 *at* 0, *hence corresponds to a* connection *on* $I^{-1}(P) \otimes I(0)$, *i.e. it corresponds to a point of* $E^\dagger(k)$. This point is none other than the point P^{can} of Lemma C.1.1. To see this, it suffices to check that the connection ω_P^{can} on $I^{-1}(P) \otimes I(0)$ is of order N. Its N'th "power" is the connection $df_P/f_P = N\cdot\omega_P^{\text{can}}$ on $I^{-n}(P) \otimes I^n(0)$, which is mapped isomorphically by "multiplication by f_P" to $\mathcal{O}_E$ with its trivial connection d, which is the zero-element of $E^\dagger(k)$.

C.2 Construction of a rational cross-section of $E^\dagger \to E$ when 6 is invertible. Henceforth, we will assume that S is a scheme on which 6 is invertible, in order to be able to make free use of Weierstrass normal form. Given an elliptic curve E/S, we denote by E^{aff}/S the complement of the zero section. If we are also given a nowhere-vanishing invariant differential ω on E, we may write a unique Weierstrass equation

$$(E, \omega) = (y^2 = 4x^3 - g_2x - g_3\,,\ \omega = dx/y) \qquad g_2\,, g_3 \in \Gamma(S, \mathcal{O}_S)$$

in which the zero section becomes the point at infinity. In this picture E^{aff} is exactly the affine curve of equation $y^2 = 4x^3 - g_2x - g_3$. We will now construct a cross section of the projection $E^\dagger \xrightarrow{\pi} E$ over E^{aff}.

LEMMA C.2.1. *Let* (E, ω) *be an elliptic curve with differential over the* $\mathbf{Z}[1/6]$*-scheme* S, *and let* $P \in E^{\text{aff}}(S)$ *be a point with Weierstrass coordinates* $x = a$, $y = b$. *Then the differential*

$$\frac{1}{2}\cdot\frac{y+b}{x-a}\cdot\frac{dx}{y} \overset{\text{dfn}}{=\!=} \omega_P$$

lies in $H^0(E, \Omega^1_{E/S} \otimes I^{-1}(P) \otimes I^{-1}(0))$, *and has residues* $+1$ *at P and* -1 *at* 0. (*Thus it provides* (*C.*1.2) *a* connection *on* $I^{-1}(P) \otimes I(0)$.)

Proof. The question being local on S, we may suppose S affine $=$ Spec(A). By reduction to the universal case, we may further assume A finitely generated over $\mathbf{Z}$, hence noetherian. Localizing further, we may assume A a noetherian local ring, then (by faithful flatness of the completion) a complete noetherian local ring, and finally (by "holomorphic functions") we may assume A an artin local ring.

Near the zero section "∞", $\omega_P = \frac{1}{2}[1 + (b/y)]\, dx/x - a$, and as the function $x - a$ has a double pole at "∞", and $1/y$ a triple zero there, it follows that ω_P has a first order pole at ∞ with residue -1.

If $b \in A$ is *nilpotent*, then P modulo the maximal ideal of A is a point of order exactly two, and the section P is locally defined by the uniformizing parameter $y - b$.

$$\omega_P = \frac{1}{2} \cdot \frac{y+b}{x-a} \cdot \frac{dx}{y} = \frac{y+b}{x-a} \cdot \frac{dy}{f'(x)} \quad \text{where} \quad f(x) = 4x^3 - g_2 x - g_3$$

$$= \frac{y^2 - b^2}{(x-a)f'(x)} \cdot \frac{dy}{y-b}$$

$$= \frac{f(x) - f(a)}{(x-a)f'(x)} \cdot \frac{d(y-b)}{y-b}$$

As $f'(a)$ is invertible, it follows that

$$\frac{f(x) - f(a)}{(x-a)f'(x)} = 1 + a \text{ function vanishing at } x = a$$

which shows that ω_P has a first order pole at P, with residue $+1$. To check that ω_P is holomorphic in $E^{\text{aff}} - P$, it suffices to check that both $(x-a)\omega_P$ and $(y-b)\omega_P$ are holomorphic in E^{aff} (because P is globally defined in E^{aff} by the ideal $(x-a, y-b)$. But

$$(x-a)\omega_P = \tfrac{1}{2}(y+b)\frac{dx}{y} \qquad \text{is holomorphic on } E^{\text{aff}}$$

$$(y-b)\omega_P = \frac{1}{2} \cdot \frac{y^2 - b^2}{x-a} \cdot \frac{dx}{y}$$

$$= \frac{1}{2}\left(\frac{f(x) - f(a)}{x-a}\right)\frac{dx}{y} \qquad \text{is holomorphic on } E^{\text{aff}}.$$

If $b \in A$ is *invertible*, then the function $x - a$ has simple zeroes at P ($x = a, y = b$) and at $-P$ ($x = a, y = -b$), but the function $y + b$ has a zero at $-P$. Thus $y + b/x - a$ is holomorphic on $E^{\text{aff}} - P$, and has a first order pole at P. Thus ω_P's only finite pole is a simple one at P, and near P we have

$$\omega_P = \frac{1}{2}\frac{1 - b + 2b}{y - b + b}\frac{d(x-a)}{(x-a)}$$

$$= \frac{1 + \dfrac{y-b}{2b}}{1 + \dfrac{y-b}{b}} \cdot \frac{d(x-a)}{x-a}$$

$$= (1 + \text{function vanishing at } P)\,\frac{d(x-a)}{x-a}$$

so that ω_P has residue $+1$ at P.

REMARK. *The differential ω_P constructed above is* independent *of the auxiliary choice of ω. For if we replace ω by $\lambda\omega$, $\lambda \in \Gamma(S, \mathcal{O}_S)^\times$, then we replace x by $\lambda^{-2}x$, y by $\lambda^{-3}y$, and the new coordinates of P become $(\lambda^{-2}a, \lambda^{-3}b)$, whence*

$$\frac{1}{2}\cdot\frac{y+b}{x-a}\cdot\frac{dx}{y} = \frac{1}{2}\cdot\frac{\lambda^{-3}y + \lambda^{-3}b}{\lambda^{-2}x - \lambda^{-2}a}\cdot\frac{d(\lambda^{-2}x)}{\lambda^{-3}y}$$

Thus we may define a cross section

$$\begin{tikzcd} E^\dagger \arrow[d, "\pi"'] & \\ E & E^{\mathrm{aff}} \arrow[l, phantom, "\supset"] \arrow[ul, bend right, "\mathcal{S}_0"'] \end{tikzcd}$$

as follows. For any S-scheme T, and any point $P \in E^{\mathrm{aff}}(T)$, we define $\mathcal{S}_0(P)$ = the connection given by ω_P on $I^{-1}(P) \otimes I(0) \in E(T)$.

C.3 Construction of a rational map $E^\dagger \to \omega_{E/S}$ when 6 is invertible. We will define a morphism

$$\mathbf{E}: \quad \pi^{-1}(E^{\mathrm{aff}}) \to \omega_{E/S}$$

simply by defining for $z \in \pi^{-1}(E^{\mathrm{aff}}(T))$

$$\mathbf{E}(z) = \mathcal{S}_0(\pi z) - z \in \omega_{E/S}(T)$$

In down to earth terms, a point of $\pi^{-0}(E^{\mathrm{aff}})(T) \subset E^\dagger(T)$ with values in T is a pair

$$(P \in E^{\mathrm{aff}}(T), \omega \in H^0(E_T, \Omega^1_{E_{T/T}} \otimes I^{-1}(P) \otimes I^{-1}(0) \text{ with residues 1 at } P, -1 \text{ at } 0).$$

Its image $\boldsymbol{\omega}_{E/S}(T) = H^0(E_T, \Omega^1_{E_T/T})$ is the differential

$$\omega_P - \omega.$$

We summarize this in the following diagram.

$$\begin{tikzcd}
0 \arrow[d] & & \\
\boldsymbol{\omega}_{E/S} \arrow[d] & & \\
E^{\dagger} \arrow[d] & \supset & \pi^{-1}(E^{\mathrm{aff}}) \arrow[ull, "\mathbf{E}\ \text{(not a section of anything)}"'] \arrow[d, dash] \\
E \arrow[d] & \supset & E^{\mathrm{aff}} \arrow[u, bend right=60, "\mathscr{S}_0\ \ \text{(a section of } \pi\text{)}"'] \\
0 & &
\end{tikzcd}$$

C.4 The construction of a modular form of weight one when 6 is invertible. Let N be an integer ≥ 2. We will construct a modular form A_1 of weight one on $\Gamma_{00}(N)$ over $\mathbf{Z}[1/6N]$ as follows. Given a ring R in which $6N$ is invertible, and a triple (E, ω, P) consisting of an elliptic curve with differential over A and a point of order *exactly* N, the value at (E, ω, P) of A_1 is defined by

$$A_1(E, \omega, P) = \frac{\mathbf{E}(P^{\mathrm{can}})}{\omega}$$

(Recall that $P^{\mathrm{can}} \in E^{\dagger}(R)$ is the unique point of order N lying over P, and that as P has exact order $N \geq 2$, P^{can} lies in $\pi^{-1}(E^{\mathrm{aff}})$, so that $\mathbf{E}(P^{\mathrm{can}})$ is a well-defined element of $\boldsymbol{\omega}_{E/R}(R) = H^0(E, \Omega^1_{E/R})$, a free R-module of which ω is a basis. Thus the ratio is a well-defined element of R.)

It is clear that the formation of $A_1(E, \omega, P)$ is compatible with arbitrary extension of scalars, and that it has degree -1 in ω. That it has holomorphic q-expansions will result from the theorem we will later prove, identifying it with the A_1 of 2.7.

C.5 The transcendental expression of the universal extension $E^{\dagger}$. Let (E, ω) be an elliptic curve with differential over $\mathbf{C}$, corresponding to the lattice $L \subset \mathbf{C}$ of *periods* of ω:

$$L = \left\{ \int_{\gamma} \omega \ \middle|\ \gamma \in H_1(E, \mathbf{Z}) \right\} \subset \mathbf{C},\ z \text{ a standard variable on } \mathbf{C}$$

$$E = \mathbf{C}/L,\ \omega = dz$$

$$(E, \omega) = (y^2 = 4x^3 - g_2 x - g_3,\ dx/y)$$

$$x = \mathcal{P}(z)$$

$$y = \mathcal{P}'(z)$$

$$\omega = dz$$

We have the Weierstrass ζ function

$$\zeta(z) = \frac{1}{z} + \text{holomorphic near } 0$$

$$\zeta'(z) = -\mathcal{P}(z)$$

which is not doubly-periodic, but satisfies

$$\zeta(z + \ell) - \zeta(z) = -\eta(\ell) \qquad \text{for} \quad \ell \in L$$

where

$$\eta(\ell) = \int_{\ell} x \frac{dx}{y} = \int_{\ell} \mathcal{P}(z)\, dz$$

is the "period of the second kind".

The differentials

$$\omega = \frac{dx}{y} \qquad \eta = \frac{x\, dx}{y}$$

form a *basis* of $H^1(E, \mathbf{C}) = \mathrm{Hom}_{\mathbf{Z}}(\mathbf{H}_1(\mathbf{E}, \mathbf{Z}), \mathbf{C}) = \mathrm{Hom}_{\mathbf{Z}}(\mathbf{L}, \mathbf{C})$ when we view them as the linear forms on L defined by

$$\omega(\ell) = \int_{\ell} \omega, \qquad \eta(\ell) = \int_{\ell} \eta$$

By Legendre's relation (cf. [6], A.1.3.13), we have a formula for their *cup-*

product:

$$\langle \omega, \eta \rangle = 2\pi i \qquad \text{(topological cup-product).}$$

We may view any element $\ell \in L = H_1(E, \mathbf{Z})$ as an element of $H^1(E, \mathbf{C})$, namely the unique element $\gamma(\ell) \in H^1(E, \mathbf{C})$ such that under cup-product we have

$$\int_\ell \omega = \langle \omega, \gamma(\ell) \rangle$$
$$\int_\ell \eta = \langle \eta, \gamma(\ell) \rangle$$

The image of L under γ is none other than $H^1(E, \mathbf{Z}) = \mathrm{Hom}_{\mathbf{Z}}(H_1(E, \mathbf{Z}), \mathbf{Z}) = \mathrm{Hom}_{\mathbf{Z}}(L, \mathbf{Z})$. If we remember that

$$\langle \omega, \eta \rangle = 2\pi i = -\langle \eta, \omega \rangle, \qquad \langle \omega, \omega \rangle = \langle \eta, \eta \rangle = 0,$$

then we immediately find the formula

$$2\pi i \gamma(\ell) = \left(\int_\ell \omega\right) \cdot \eta - \left(\int_\ell \eta\right) \cdot \omega$$

(both sides have the same cup-products with ω and η).

If we view $\ell \in L \subset \mathbf{C}$ as a *complex number*, it's exactly the complex number $\int_\ell \omega$, so that in our earlier $\eta(\ell)$ notation we may rewrite this last formula

$$2\pi i \gamma(\ell) = \ell \cdot \eta - \eta(\ell)\omega \quad \text{in} \quad H^1(E, \mathbf{C})$$

Now let's recall that $E^\dagger(\mathbf{C})$ is the group of isomorphism classes of invertible sheaves on E with integrable connections (the existence of the connection implies that the *degree* is zero, when we are over $\mathbf{C}$). By GAGA, $E^\dagger(\mathbf{C})$ is equivalently the group of isomorphism classes of analytic invertible sheaves with connection on E^{an}, which group is just the group

$$\mathrm{Hom}(\pi_1(E), \mathbf{C}^\times)$$

(A line bundle with connection gives rise to a representation of the fundamental group by considering the effect of analytic continuation on the local horizontal sections of the *dual* line bundle with its dual connection.)

Thus we have

$$E^\dagger(\mathbf{C}) = \mathrm{Hom}(\pi_1(E), \mathbf{C}^\times) = H^1(E, \mathbf{C}^\times) \underset{\exp}{\xleftarrow{\sim}} H^1(E, \mathbf{C})/2\pi i H^1(E, \mathbf{Z}).$$

In terms of the *basis* η, ω of $H^1(E, \mathbf{C})$, we have

$$H^1(E, \mathbf{C}) = \text{pairs } (a, b) \text{ of complex numbers} \leftrightarrow a\eta + b\omega$$

$$2\pi i H^1(E, \mathbf{Z}) = \text{the subgroup consisting of all pairs } (\ell, -\eta(\ell)),\ \ell \in L.$$

The analytic description sits in the commutative diagram

$$\begin{tikzcd}
0 \arrow[d] & & \\
\omega(\mathbf{C}) \arrow[r, equal] & H^0(E, \Omega^1_{E/\mathbf{C}}) & \mathbf{C} \arrow[l, "\sim", "\text{basis } \omega"'] \arrow[d, "b \to (0,\, b)"] \\
E^{\dagger}(\mathbf{C}) \arrow[d] & H^1(E, \mathbf{C})/2\pi i H^1(E, \mathbf{Z}) \arrow[l, "\sim"] & \mathbf{C}^2/\{(\ell, -\eta(\ell)\} \arrow[l, "\sim", "\text{basis } \eta,\omega"'] \arrow[dl, "pr_1"] \\
E(\mathbf{C}) \arrow[d] \arrow[r, dash, "\sim"] & \mathbf{C}/L & \\
0 & &
\end{tikzcd}$$

C.6 The comparison theorem: statement.

THEOREM C.6.

(1) *Under the isomorphism* $\mathbf{C}^2/\{\ell, -\eta(\ell)\} \xrightarrow{\sim} E^{\dagger}$, *the class of the point* $(a, b) \in \mathbf{C}^2$ *gives the point* a *mod* L *in* $\mathbf{C}/L = E(\mathbf{C})$ *and the connection on the divisor* $[a] - [0]$ *(meaning: on the invertible sheaf* $I^{-1}(a \bmod L) \otimes I(0))$ *given by the differential*

$$(\zeta(z - a) - \zeta(z) + b)\, dz$$

(2) *The section* $\mathscr{S}_0\colon E^{\mathrm{aff}}(\mathbf{C}) \to \pi^{-1}(E^{\mathrm{aff}}(\mathbf{C}))$ *is given analytically by*

$$a \in \mathbf{C}/L \to \text{the class of } (a, \zeta(a)) \text{ in } \mathbf{C}^2/\{\ell, -\eta(\ell))\}$$

(3) *The morphism* $\mathbf{E}\colon \pi^{-1}(E^{\mathrm{aff}}(\mathbf{C})) \to \boldsymbol{\omega}(\mathbf{C})$ *is given analytically by*

$$(a, b) \to (\zeta(a) - b)\, dz$$

Before the proof, let's give the corollary which motivated this whole appendix.

COROLLARY C.4. *Let P be a point of order exactly $N \geq 3$ on $E(\mathbf{C}) \simeq \mathbf{C}/L$, represented as $(1/N)\ell$ for some $\ell \in L$. Then the modular form A_1 defined in C.4 is given by*

$$A_1(E, \omega, P) = \zeta\left(\frac{1}{N}\ell\right) + \frac{1}{N}\eta(\ell)$$

Proof of the corollary. The point $P^{\mathrm{can}} \in E^{\dagger}(\mathbf{C})$ is the unique point of order N in $E^{\dagger}(\mathbf{C})$ lying over $P = (1/N)\ell$, so we must have

$$P^{\mathrm{can}} = \frac{1}{N}(\ell, -\eta(\ell)) \qquad \text{in} \quad E^{\dagger}(\mathbf{C}) \simeq \mathbf{C}^2/\{(\ell, -\eta(\ell)\}.$$

By definition of A_1, we have

$$A_1(E, \omega, P) = \frac{\mathbf{E}(P^{\mathrm{can}})}{\omega} = \frac{\mathbf{E}\left(\frac{1}{N}\ell, -\frac{1}{N}\eta(\ell)\right)}{dz}$$

By (3) of C.6, $\mathbf{E}(a, b) = (\zeta(a) - b)dz$, whence

$$A_1(E, \omega, P) = \frac{\mathbf{E}\left(\frac{1}{N}\ell, -\frac{1}{N}\eta(\ell)\right)}{dz} = \zeta\left(\frac{1}{N}\ell\right) + \frac{1}{N}\eta(\ell)$$

Q.E.D.

C.7 Proof of the theorem. We begin with the proof of (1). Let $(a, b) \in \mathbf{C}^2$. We wish to compute which connection on $I^{-1}(a \bmod L) \otimes I(0)$ it corresponds to, or equivalently which differential $\omega_{a,b}$ on E with only first order poles at $a \bmod L$ and at 0, residues $+1$ at a, -1 at 0, it corresponds to. The differential $\omega_{a,b}$ gives the connection

$$f \to df + f\omega_{a,b}$$

on $I^{-1}(a \bmod L) \otimes I(0)$. The *dual* connection is the connection on $I(a \bmod L) \otimes I^{-1}(0)$ given by

$$g \to dg - g\omega_{a,b}.$$

A local horizontal section of this dual connection is thus a meromorphic function $\psi_{a,b}$ on $\mathbf{C}$, *not* doubly periodic, such that

$$\frac{d\psi_{ab}}{\psi_{ab}} = \omega_{a,b}$$

The corresponding representation $\rho_{a,b}$ of $\pi_1(E) = L$ in $\mathbf{C}^\times$ is given by

$$\psi_{a,b}(z + \ell) = \rho_{a,b}(\ell)\psi_{a,b}(z)$$

(since $d \log \psi_{a,b}$ is doubly-periodic, translating $\psi_{a,b}$ by $\ell \in L$ only changes it by a scalar factor!)

On the other hand, we know explicitly in terms of (a, b) *which* representation $\rho_{a,b}$ is, for under our isomorphisms, we have

$$\begin{tikzcd}[column sep=small]
(a, b) \in \mathbf{C}^2 \sim a\eta + b\omega \in H^1(E, \mathbf{C}) \sim \ell \to a\eta(\ell) + b\ell \in \operatorname{Hom}(L, \mathbf{C}) \arrow[d, "\exp"] \\
\ell \to e^{a\eta(\ell)+b\ell} \in \operatorname{Hom}(L, \mathbf{C}^\times)
\end{tikzcd}$$

Thus

$$\rho_{a,b}(\ell) = e^{a\eta(\ell)+b\ell}$$

So in order to prove (1), it suffices to exhibit a function $\psi_{a,b}$, meromorphic on $\mathbf{C}$, such that

$$\begin{cases} d\psi_{a,b}/\psi_{a,b} = (\zeta(z - a) - \zeta(z) + b)\, dz \\ \psi_{a,b}(z + \ell)/\psi_{a,b}(z) = e^{a\eta(\ell)+b\ell} \end{cases}$$

But this is just what the Weierstrass σ function is all about; it satisfies

$$\begin{cases} d\sigma(z)/\sigma(z) = \zeta(z) \\ d(z + \ell)/\sigma(z) = f(\ell)\cdot e^{-\eta(\ell)(z+\frac{1}{2}\ell)} \end{cases}$$

where $f(\ell)$ is a certain ± 1-valued function on $L/2L$. So if we define $\psi_{a,b}$ by the formula

$$\psi_{a,b}(z) = \frac{\sigma(z - a)}{\sigma(z)} \exp(bz)$$

then we clearly have the requisite properties, to wit

$$d\psi_{a,b}/\psi_{a,b} = \zeta(z-a) - \zeta(z) + b$$

and

$$\psi_{a,b}(z+\ell)/\psi_{a,b}(z) = \frac{\sigma(z-a+\ell)\sigma(z+\ell)\exp(bz+b\ell)}{\sigma(z-a)\sigma(z)\exp(bx)}$$

$$= \frac{f(\ell)e^{-\eta(\ell)(z-a+\frac{1}{2}\ell)}}{f(\ell)e^{-\eta(\ell)(z+\frac{1}{2}\ell)}} \cdot e^{b\ell}$$

$$= e^{a\eta(\ell)+b\ell}$$

This proves (1).

To prove (2), we must show that the point $(a, \zeta(a))$ gives the differential

$$\frac{1}{2}\frac{\mathcal{P}'(z)+\mathcal{P}'(a)}{\mathcal{P}(z)-\mathcal{P}(a)}\,dz.$$

As we have just proven,

$$\omega_{a,b} = (\zeta(z-a) - \zeta(z) + b)dz$$

so we must check that

$$\frac{1}{2}\frac{\mathcal{P}'(z)+\mathcal{P}'(a)}{\mathcal{P}(z)-\mathcal{P}(a)} = \zeta(z-a) - \zeta(z) + \zeta(a)$$

or equivalently, replacing a by $-a$ and remembering that ζ and $\mathcal{P}'$ are odd functions while $\mathcal{P}$ is an even function, we must check that

$$\frac{1}{2}\frac{\mathcal{P}'(z)-\mathcal{P}'(a)}{\mathcal{P}(z)-\mathcal{P}(a)} = \zeta(z+a) - \zeta(z) - \zeta(a)$$

This last formula is well-known (Whittaker and Watson, p. 451, example 2); it is the value at $t = a$ of the result of applying $\partial/\partial z + \partial/\partial t$ to the logarithms of both sides of the formula

$$-\mathcal{P}(z) + \mathcal{P}(t) = \frac{\sigma(z+t)\sigma(z-t)}{\sigma^2(z)\sigma^2(t)}.$$

To prove (3), simply recall that, by definition, we have

$$\begin{aligned} E(a,b) &= \omega_{a,\zeta(a)} - \omega_{a,b} \\ &= [\zeta(z-a) - \zeta(z) + \zeta(a) - (\zeta(z-a) - \zeta(z) + b)]\,dz \\ &= (\zeta(a) - b)\,dz \end{aligned}$$

Q.E.D.

C.8 A philosophical remark. The section

$$\begin{tikzcd} E^{\dagger} \arrow[d, "\pi"'] & \\ E & \supset \; E^{\mathrm{aff}} \arrow[ul, bend right, "\mathscr{S}_0"'] \end{tikzcd}$$

whose transcendental expression is

$$a \to (a, \zeta(a)) = \left(\int_0^a dz, -\int_{a \text{ zero of } \zeta}^a \mathscr{P}(z)\, dz\right)$$

is the "Abel-Jacobi map" for periods of the first *and* second kind. So we may summarize the comparison theorem by saying that "the Abel-Jacobi map for periods of the second kind is *algebraic*".

C.9 Reformulation of a Conjecture (compare [5], 7.5). Let E be an elliptic curve over $\mathbf{Z}[1/N]$ such that $E_{\mathbf{Q}}$ has a rational point of order two. Let E_p denote $E \otimes \mathbf{F}_p$. Then (cf. [5], 7.5) for $p \geq 7$, $p \nmid N$, the group $E(\mathbf{F}_p) = E_p(\mathbf{F}_p)$ is of order prime to p. Now let $P \in E(\mathbf{Z}[1/N]) = E(\mathbf{Q})$ be a point in $E^{\mathrm{aff}}(\mathbf{Q})$. Then at the expense of enlarging N, we may assume that $P \in E^{\mathrm{aff}}(\mathbf{Z}[1/N])$. Let $P_p \in E(\mathbf{F}_p)$ denote the reduction mod p of P; it is a rational point on $E_{\mathbf{F}_p}$ of finite order *prime* to p. Thus the modular form A_1 is defined at $(E_{\mathbf{F}_p}, P_p)$;

$$A_1(E_{\mathbf{F}_p}, P_p) \in \boldsymbol{\omega}_{E_{\mathbf{F}_p}}(\mathbf{F}_p) = H^0(E_p, \Omega^1_{E_p/\mathbf{F}_p})$$

It is natural to consider the map

$$E(\mathbf{Q}) \to \prod_p H^0(E_p, \Omega^1_{E_p})/H^0(E, \Omega^1_{E/\mathbf{Z}[1/N]})$$

which is a *group homomorphism*, and to ask whether its kernel lies in the *torsion subgroup*.

C.10 Effect on Tangent Spaces. Recall that if A is an abelian scheme over any affine scheme S, then the universal extension of $\mathrm{Pic}^0_{A/S}$, noted $A^{\dagger}$, sets in an exact sequence of S-groups

$$0 \to \boldsymbol{\omega}_{A/S} \to A^{\dagger} \to \mathrm{Pic}^0_{A/S} \to 0.$$

Its tangent space along the identity section, $tg(A^{\dagger})$, is canonically equal to $H^1_{DR}(A/S)$, and the short exact sequence of tangent spaces

$$\begin{tikzcd} 0 \arrow[r] & \boldsymbol{\omega}_{A/S} \arrow[r] \arrow[d, equal] & H^1_{DR}(A/S) \arrow[r] & tg(\mathrm{Pic}^0_{A/S}) \arrow[r] \arrow[d, equal] & 0 \\ & H^0(A, \Omega^1_{A/S}) & & H^1(A, \mathcal{O}_A) & \end{tikzcd}$$

is the Hodge filtration on $H^1_{DR}(A/S)$.

Suppose now that $A = E$, an elliptic curve. Then $H^1_{DR}(E/S)$ is selfdual under the cup-product pairing (e.g. in the Weierstrass model the DR cup-product $\langle \omega, \eta \rangle = 1$). Thus there is a unique isomorphism

$$ctg(E^\dagger) \xrightarrow{\sim} H^1_{DR}(E/S)$$

under which the canonical pairing

$$ctg(E^\dagger) \times tg(E^\dagger) \to \mathcal{O}_S$$

becomes the cup-product pairing on $H^1_{DR}(E/S)$.

We recall from ([6], p. 163) that the inclusion of complexes $(\mathcal{O}_E \to \Omega^1_{E/S}) \to (I^{-1}(0) \to \Omega^1_{E/S} \otimes I^{-2}(0))$ though not a quasi-isomorphism, gives rise to an isomorphism

$$H^1_{DR}(E/S) \xrightarrow{\sim} \mathbf{H}^1(E, I^{-1}(0) \to \Omega^1_{E/S} \otimes I^{-2}(0)) \xrightarrow{\sim} H^0(E, \Omega^1_{E/S} \otimes I^{-2}(0)).$$

THEOREM C.10.1. *Consider the composite map*

$$\begin{tikzcd} H^0(E, \Omega^1_{E/S} \otimes I^{-2}(0)) \arrow[r, "\sim"] & H^1_{DR}(E/S) \arrow[r, "\sim"] & ctg(E^\dagger) \subset H^0(E^\dagger, \Omega^1_{E^\dagger/S}) \arrow[d, "\text{restriction to } \pi^{-1}(E^{\mathrm{aff}})"] \\ & & H^0(\pi^{-1}(E^{\mathrm{aff}}), \Omega^1_{E^\dagger/S}) \arrow[d, "\mathscr{S}_0{}^*"] \\ & & H^0(E^{\mathrm{aff}}, \Omega^1_{E/S}) \arrow[d, equal] \\ & & \bigcup_{n \geq 1} H^0(E, \Omega^1_{E/S} \otimes I^{-n}(0)). \end{tikzcd}$$

It is simply the inclusion of

$$H^0(E, \Omega^1_{E/S} \otimes I^{-2}(0)) \textit{ in } \cup_{n\geq 1} H^0(E, \Omega^1_{E/S} \otimes I^{-n}(0)).$$

Proof. By "reduction to the universal case", it suffices to check the case when S is the spectrum of a finitely generated subring R of $\mathbf{C}$. Further localizing on S, we may also suppose that $H^0(E, \Omega^1_{E/S} \otimes I^{-n}(0))$ is free of rank n for $n = 2$, and 3—it will then automatically be true for all $n \geq 2$. Then our assertion is that two maps between free R-modules are equal. For this, it suffices that they become equal after any injective extension of scalars $R \to R'$. Choosing $R' = \mathbf{C}$, we are reduced to the case $S = \operatorname{Spec}(\mathbf{C})$, which we will check transcendentally.

$$\begin{cases} E^\dagger(\mathbf{C}) = H^1(E, \mathbf{C})/2\pi i H^1(E, \mathbf{Z}) \xrightarrow{\sim} \mathbf{C}^2/\{(\ell, -\eta(\ell))\} \\ tgE^\dagger = H^1(E, \mathbf{C}) \xrightarrow{\sim} \mathbf{C}^2, \text{ via the basis } \eta, \omega \end{cases}$$

Taking coordinates (a, b) on $\mathbf{C}^2$, the invariant differentials are da, db and da, db is the basis of $ctg(E^\dagger)$ *dual* to the basis η, ω of $tg(E^\dagger)$. Using the DeRham cup-product on $H^1(E, \mathbf{C})$, we have

$$\langle \omega, \eta \rangle_{DR} = 1 = -\langle \eta, \omega \rangle_{DR}$$

and thus the dual basis to (η, ω) is $(\omega, -\eta)$, hence the isomorphism

$$ctg(E^\dagger) \xrightarrow{\sim} H^1_{DR}(E/S)$$

is given by

$$\begin{cases} da \leftrightarrow \omega \\ db \leftrightarrow -\eta \end{cases}$$

Now the section $\mathscr{S}_0$ is given by

$$z \to (z, \zeta(z));$$

Thus

$$\begin{cases} \mathscr{S}_0{}^*(da) = dz = \omega \\ \mathscr{S}_0{}^*(db) = d\zeta(z) = -\wp(z)\, dz = -\eta \end{cases}$$

as desired.

Q.E.D.

C.11 Relation with Mazur's modular form. He begins with an elliptic curve E over a field k, and a point $P \in E^{\text{aff}}(k)$ of order N prime to char(k). The divisor

$$N^*([P] - [0]) = \sum_{Ny=P} [y] - \sum_{Nz=0} [z]$$

is easily seen to be principal, by Abel's theorem, for it has degree zero, and it sums to zero on E. (If we choose one point y_0 such that $Ny_0 = P$, then

$$\sum_{Ny=P} y - \sum_{Nz=0} z = \sum_{Nz=0} (y_0 + z) - \sum_{Nz=0} z = N^2 y_0 = NP = 0.)$$

So there is a function g on E, unique up to a $k^\times$-multiple, such that

$$(g) = N^*([P] - [0])$$

Clearly, the divisor of (g) is *invariant* by translation by points of order N, hence the function g itself only changes by a $k^\times$-multiple under such translation, and hence the differential dg/g is *invariant* by such translations. Hence there is a unique differential, noted $\omega_P{}^{\mathrm{can}}$, such that

$$dg/g = N^*(\omega_P{}^{\mathrm{can}}).$$

LEMMA C.11.1. *Let f be any function such that $(f) = N[P] - N[0]$. Then*

$$\omega_P{}^{\mathrm{can}} = \frac{1}{N} df/f$$

Proof. We must check that $N^*(\omega_P{}^{\mathrm{can}}) = N^*((1/N)\ df/f)$, i.e. that $N \cdot dg/g = N^*(df/f)$, i.e. that $dg^N/g^N = N^*(df/f)$. So it suffices to show that $(g^N) = N^*(f)$, or equivalently that $N(g) = N^*(f)$. But $(g) = N^*([P] - [0])$, and $(f) = N[P] - N[0]$.

Q.E.D.

Thus the differential $\omega_P{}^{\mathrm{can}}$ is precisely the connection on $I^{-1}(P) \otimes I(0)$ which *is* the point $P^{\mathrm{can}} \in E^\dagger(k)$ (cf. C.1.3).

Mazur's modular form is defined as follows. If P and Q are two *distinct* points of $E^{\mathrm{aff}}(k)$, both of finite order N prime to char(k), then Mazur defines

$$M(E, \omega, P, Q) = \frac{\omega_P{}^{\mathrm{can}}}{\omega}(Q).$$

Over any base scheme S where N is invertible, we may define $\omega_P{}^{\mathrm{can}} \in H^0(E/S,\ \Omega^1_{E/S} \otimes I^{-1}(P) \otimes I^{-1}(0))$ as the element giving the connection on $I^{-1}(P) \otimes I(0)$ which is $P^{\mathrm{can}} \in E^\dagger(S)$. So over any base where N is invertible, whenever we are given two *disjoint* sections $P, Q \in E^{\mathrm{aff}}(S)$ of order N, we may define

$$M(E, \omega, P, Q) = \frac{\omega_P{}^{\mathrm{can}}}{\omega}(Q),$$

the value along the section Q of the function

$$\frac{\omega_P{}^{\mathrm{can}}}{\omega} \in H^0(E, I^{-1}(P) \otimes I^{-1}(0)).$$

We now express M in terms of the Eisenstein series A_1.

LEMMA C.11.2. *Over* $\mathbf{C}$, *if* $(E, \omega) \leftrightarrow$ *the lattice* $L \subset \mathbf{C}$, *and* $P = (1/N)\ell$, *then*

$$\omega_P{}^{\mathrm{can}} = \left(\zeta\left(z - \frac{1}{N}\ell\right) - \zeta(z) - \frac{1}{N}\eta(\ell)\right) dz$$

Proof. The point $P^{\mathrm{can}} \in E^{\dagger}(\mathbf{C})$ is $[(1/N)\ell, -(1/N)\eta(\ell)]$, which by (2) of C.6 is the connection given by the differential

$$\left(\zeta\left(z - \frac{1}{N}\ell\right) - \zeta(z) - \frac{1}{N}\eta(\ell)\right) dz$$

An alternate proof would be to remark that the elliptic function

$$f = \frac{\left(\sigma\left(z - \frac{1}{N}\ell\right)\right)^N}{(\sigma(z))^{N-1}\sigma(z - \ell)}$$

has divisor $(f) = N[P] - N[0]$, and then simply to compute

$$\begin{aligned}\omega_P{}^{\mathrm{can}} = \frac{1}{N} df/f &= \left(\zeta\left(z - \frac{1}{N}\ell\right) - \left(\frac{N-1}{N}\right)\zeta(z) - \frac{1}{N}\zeta(z - \ell)\right) dz \\ &= \left(\zeta\left(z - \frac{1}{N}\ell\right) - \zeta(z) + \frac{1}{N}[\zeta(z) - \zeta(z - \ell)]\right) dz \\ &= \left(\zeta\left(z - \frac{1}{N}\ell\right) - \zeta(z) - \frac{1}{N}\eta(\ell)\right) dz.\end{aligned}$$

PROPOSITION C.11.3. *Let* S *be any scheme where* $6N$ *is invertible,* (E, ω) *an elliptic curve with differential over* S, *and* $P, Q \in E^{\mathrm{aff}}(S)$ *two disjoint sections* (*meaning* $P - Q \in E^{\mathrm{aff}}(S)$), *both of* (*not necessarily exact*) *order* N. *Then*

$$M(E, \omega, P, Q) = A_1(E, \omega, Q - P) - A_1(E, \omega, Q)$$

Proof. By standard reductions, it suffices to check the case $S = \mathrm{Spec}(\mathbf{C})$. Then (E, ω) corresponds to a lattice $L \subset \mathbf{C}$, P is $(1/N)\ell$, Q is

$(1/N)\ell'$, and

$$\frac{\omega_P{}^{\text{can}}}{\omega} = \frac{\left(\zeta\left(z - \frac{1}{N}\ell\right) - \zeta(z) - \frac{1}{N}\eta(\ell)\right) dz}{dz}$$

Thus

$$\begin{aligned} M(E, \omega, P, Q) &= \frac{\omega_P{}^{\text{can}}}{\omega}(Q) \\ &= \zeta\left(\frac{1}{N}\ell' - \frac{1}{N}\ell\right) - \zeta\left(\frac{1}{N}\ell'\right) - \frac{1}{N}\eta(\ell) \\ &= \zeta\left(\frac{1}{N}\ell' - \frac{1}{N}\ell\right) + \frac{1}{N}\eta(\ell' - \ell) - \zeta\left(\frac{1}{N}\ell'\right) - \frac{1}{N}\eta(\ell') \\ &= A_1(E, \omega, Q - P) - A_1(E, \omega, Q). \end{aligned}$$

Q.E.D.

PRINCETON UNIVERSITY.

REFERENCES.

[0] Cartier, P.: Bernoulli Numbers from Ancient to Modern Times, lectures at Haverford College, Fall, 1973.

[1] Deligne, P., and Rapoport, M.: Les schémas de modules de courbes elliptiques. Proceedings of the 1972 Antwerp International Summer School on Modular Functions, Springer Lecture Notes in Mathematics 349 (1973), 143–317.

[1a] Dwork, B.: P-adic cycles, Pub. Math. I.H.E.S. (37), 1969, 327–415.

[2] Hurwitz, A.: Über die Entwicklungskoffizienten der lemniskatischen Functionen. Nachrichten von der k. Gesselschaft der Wissenschaften zu Göttigen, Mathematisch phys. Klasse, 1897, 273–276.

[3] ———: Über die Entwicklungskoffizienten der lemniskatischen Functionen, Mathem. Annalen, Bd. 51 (1899), 196–226.

[4] Iwasawa, K.: *Lectures on p-adic L functions.* Annals of Mathematics Studies 74, Princeton University Press (1972).

[5] Katz, N. M.: Algebraic solutions of differential equations (p-curvature and the Hodge filtration), Invent. Math. 18 (1972), 1–118.

[6] ———: P-adic properties of modular schemes and modular forms, Proceedings of the 1972 Antwerp International Summer School on Modular Functions, Springer Lecture Notes in Mathematics 350 (1973), 70–189.

[7] ———: Higher congruences between modular forms, to appear.

[8] Kubota, T., and Leopoldt, W.: Eine p-adische Theorie der Zetawerte, I, Jour. Reine und Angew. Math. 214/215 (1964), 328–339.

[9] Lang, S.: *Elliptic functions,* Reading, Addison-Wesley (1973).

[10] Manin, J. I.: Parabolic points and zeta functions of modular curves, Izv. Akad. Nauk. 36 (1972), 19–66.

[11] ———: Periods of parabolic forms and p-adic Hecke series (in Russian), Math. Sbornik V.93 (134), No. 3 (11), 1973.

[12] Mazur, B.: Courbes elliptiques et symboles modulaires, Exposé 414, Séminaire Bourbaki 1971/72, Springer Lecture Notes in Mathematics 317 (1973), 277–294.

[13] ———: Analyse p-adique; secret Bourbaki rédaction, 1973.

[14] ——— and Messing, W.: Universal extensions and one-dimensional crystalline cohomology, Springer Lecture Notes in Mathematics 370 (1974).

[15] ——— and Swinnerton-Dyer, H. P. F.: Arithmetic of Weil Curves, Inv. Math. 25 (1974), 1–61.

[16] Messing, W.: The universal extension of an abelian variety by a vector group, *Symposia Mathematica,* Vol. XI, Instituto Nazionale di Alta Mathematica, Academic Press (1973).

[16a] ———: The crystal associated to Barsotti-Tate groups, with applications to abelian schemes, Springer Lecture Notes in Mathematics 264 (1972).

[17] Serre, J.-P.: Congruences et formes modulaires, Exposé 416, Séminaire N Bourbaki 1971/72, Springer Lecture Notes in Mathematics 317 (1973), 319–338.

[18] ———: Formes modulaires et fonctions zeta p-adiques, Proceedings of the 1972 Antwerp International Summer School on Modular Functions, Springer Lecture Notes in Mathematics 350 (1973).

[19] Swinnerton-Dyer, H. P. F.: On ℓ-adic representations and congruences for coefficients of modular forms, Proceedings of the 1972 Antwerp International Summer School on Modular Functions, Springer Lecture Notes in Mathematics 350 (1973), 1–55.

[20] Whittaker, E. T. and Watson, G. N.: *A course of modern analysis,* Cambridge, Cambridge University Press, 1962.

[21] Mahler, K.: An interpolation series for a continuous function of a p-adic variable. J. Reine Ang. Math. 199 (1958), 23–34.