Iwasawa theory for the symmetric square of an elliptic curve

by

J.Coates*, C.-G.Schmidt**

*University of Cambridge
Department of Mathematics
16, Mill Lane
Cambridge CB2 1SB
England

**Max-Planck-Institut
für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3
Germany

MPI/86-34

Introduction. Up until the present time, most work in Iwasawa theory has dealt with either the cyclotomic theory or descent theory on abelian varieties. We began work on the material in this paper several years ago in an effort to formulate precise questions of Iwasawa theory for more general L-functions which are of arithmetic interest. It seemed to us that the first case to consider was the L-function attached to the symmetric square of the Tate module of an elliptic curve defined over $\mathbb{Q}$. The aim of the present paper is to present the rather fragmentary results we have obtained in this direction, as well as several precise conjectures. Throughout, we have only considered primes p such that the elliptic curve has good ordinary reduction at p - the case of all other primes remains shrouded in mystery at present. Finally, we wish to express our thanks to R. Greenberg, whose many suggestions over the last year have greatly helped us. Indeed, Greenberg has now gone a long way towards formulating precise conjectures of Iwasawa theory for the L-function attached to an arbitrary ℓ-adic representation and a prime p which is ordinary for this ℓ-adic representation.

Notation. We write $\bar{\mathbb{Q}}$ for the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. If L/K is a Galois extension of fields, we write $G(L/K)$ for the Galois group of L/K. For simplicity, we put

$$G = G(\bar{\mathbb{Q}}/\mathbb{Q}) .$$

For each integer $m \geq 1$, let μ_m denote the group of m-th roots of unity. Let ℓ be a prime number, and write $\mathbb{Q}_\ell$ (resp. $\mathbb{Z}_\ell$) for the field of ℓ-adic numbers (resp. the ring of ℓ-adic integers). Put

$$T_\ell(\mu) = \varprojlim \mu_{\ell^n} , \quad V_\ell(\mu) = T_\ell(\mu) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell .$$

For an integer $n \geq 0$, we write $V_\ell(\mu)^{\otimes n}$ for the n-fold tensor product of $V_\ell(\mu)$ with itself. For negative n, $V_\ell(\mu)^{\otimes n}$ denotes the $(-n)$-fold tensor product of $\mathrm{Hom}(V_\ell(\mu), \mathbb{Q}_\ell)$ with itself. Throughout, E will denote an elliptic curve defined over $\mathbb{Q}$. For each integer $n \geq 1$, E_{ℓ^n} will signify the group of ℓ^n-division points on E. We put

$$T_\ell(E) = \varprojlim E_{\ell^n}, \quad V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell .$$

All these modules are endowed with their natural G-structure. In general, if A and B are G-modules, we endow $\mathrm{Hom}(A,B)$ with its natural structure as a G-module, i.e. $(\sigma f)(a) = \sigma f(\sigma^{-1}a)$, for $\sigma \in G$, $a \in A$ and $f \in \mathrm{Hom}(A,B)$. Also, for a field F and a discrete $G(\bar{F}/F)$-module M, we denote by $H^i(F,M)$ the ordinary Galois cohomology groups of the $G(\bar{F}/F)$-module M. For each integer $N \geq 1$, $\Gamma_0(N)$ denotes the subgroup of $SL_2(\mathbb{Z})$ consisting of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where N divides c. We write c_ψ for the conductor of a Dirichlet character ψ. The symbol $[r]$ stands for the integral part of $r \in \mathbb{R}$. Now fix a prime number $p > 2$ and denote by $\mathbb{Q}_\infty$ the cyclotomic $\mathbb{Z}_p$-extension over $\mathbb{Q}$ with Galois group $\Gamma = G(\mathbb{Q}_\infty/\mathbb{Q})$. Put

$$\Theta = G(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}), \quad \Delta = G(\mathbb{Q}(\mu_p)/\mathbb{Q}) .$$

Let κ denote the cyclotomic character

$$\kappa : \Gamma \longrightarrow 1+p\mathbb{Z}_p ,$$

giving the action of Γ on μ_{p^∞} via the canonical isomorphism $\Theta \cong \Gamma \times \Delta$. Let ω denote the Teichmüller character

$$\omega : \Delta \longrightarrow \mathbb{Z}_p^* ,$$

given by the action of Δ on μ_{p^∞}. Finally we write

$$\Lambda = \mathbb{Z}_p[[\Gamma]]$$

for the completed group ring of the pro-p-group Γ over $\mathbb{Z}_p$.

§ 1. Complex L-function attached to the symmetric square of the Tate module

Our aim in this section is to recall the standard conjectures (see [16]) about the complex L-function attached to the symmetric square of $T_\ell(E)$, and also to explicitly calculate the Euler factors at the bad primes.

1.1 Definition of the complex L-function. Put

$$H^1_\ell(E) = \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(E), \mathbb{Q}_\ell) ,$$

so that $H^1_\ell(E)$ has dimension 2 over $\mathbb{Q}_\ell$, and is endowed with its natural action of $G = G(\bar{\mathbb{Q}}/\mathbb{Q})$. Let τ denote the involution of the tensor product of $H^1_\ell(E)$ with itself over $\mathbb{Q}_\ell$ which sends $x \otimes y$ into $y \otimes x$. As usual, we write $\mathrm{Sym}^2(H^1_\ell(E))$ for the 3-dimensional subspace on which τ acts as the identity, and $\mathrm{Alt}^2(H^1_\ell(E))$ for the 1-dimensional subspace on which τ acts like minus the identity. Then both subspaces are clearly invariant under the action of G, and we have

$$H^1_\ell(E) \otimes_{\mathbb{Q}_\ell} H^1_\ell(E) = \mathrm{Sym}^2(H^1_\ell(E)) \oplus \mathrm{Alt}^2(H^1_\ell(E)) .$$

Now it is well known that the Weil pairing implies that

$$\mathrm{Alt}^2(H^1_\ell(E)) \xrightarrow{\sim} \mathrm{Hom}(V_\ell(\mu), \mathbb{Q}_\ell)$$

as G-modules. In the following, we shall only be concerned with the 3-dimensional ℓ-adic representation $\mathrm{Sym}^2(H^1_\ell(E))$, and, for brevity, we write

$$\Sigma_\ell(E) = \mathrm{Sym}^2(H^1_\ell(E)) . \tag{1.1}$$

We also denote the action of G on $\Sigma_\ell(E)$ by

$$\rho_\ell : G \longrightarrow \mathrm{Aut}(\Sigma_\ell(E)) \quad . \tag{1.2}$$

Note that $\Sigma_\ell(E)$ plainly remains unchanged if we replace E by its twist by any quadratic character of $\mathbb{Q}$.

We now explain the standard manner (see [16]) to attach an Euler product to the ℓ-adic representation (1.2). For each rational prime r , let $D_r \supset I_r$ denote a decomposition group and its inertia subgroup for r , in G . Write Frob_r for the element of D_r/I_r given by $x \longmapsto x^r$. Now pick any prime ℓ different from r , and define the Euler factor at r by

$$\mathcal{D}_r(X) = \det(1-\rho_\ell(\mathrm{Frob}_r^{-1})X \mid \Sigma_\ell(E)^{I_r}) \quad . \tag{1.3}$$

It is easy to see (in fact, we shall compute this Euler factor for every r a little later in this section) that $\mathcal{D}_r(X)$ is a polynomial in X with rational coefficients, which does not depend on the choice of ℓ , nor on the choice of the decomposition group D_r . This then leads us to the definition of the primitive symmetric square as the Euler product

$$\mathcal{D}(E,s) = \prod_{r \text{ finite}} \mathcal{D}_r(r^{-s})^{-1} \quad . \tag{1.4}$$

It is also explained in [16] what conjecturally should be the functional equation for $\mathcal{D}(E,s)$. Here is the precise result. Let C denote the conductor of the ℓ-adic representation (1.2). By definition, for each prime r , we have $\mathrm{ord}_r(C) = \varepsilon_r + \delta_r$, where ε_r and δ_r are given as follows. We have

$$\varepsilon_r = 3 - \dim_{\mathbb{Q}_\ell}(\Sigma_\ell(E)^{I_r})$$

for any $\ell \neq r$. Also, for $\ell \neq r$,

$$\delta_r = \sum_{i=1}^{\infty} \frac{\#(G_i)}{\#(G_0)} \dim_{\mathbb{F}_\ell} (M/M^{G_i}) ,$$

where $M = \mathrm{Sym}^2(\mathrm{Hom}(E_\ell, \mathbb{F}_\ell))$, and

$$G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots$$

denote the series of higher ramification groups for the extension of local fields $\mathbb{Q}_r(E_\ell)/\mathbb{Q}_r$. It is easy to see that ε_r and δ_r do not depend on the choice of ℓ . Moreover, as the inertia group G_0 for this extension acts trivially on μ_ℓ , the Weil pairing shows that we can replace M in the definition of δ_r by $\mathrm{Sym}^2(E_\ell)$. Finally, the $\mathbb{R}$-Hodge structure of the complex vector space

$$\mathrm{Sym}^2(H^1(E,\mathbb{C})) \subset H^2(E \times E, \mathbb{C})$$

shows that the Γ-factor in the functional equation should be

$$\Gamma(\mathcal{D},s) = \pi^{-s/2} \Gamma(\tfrac{s}{2}) (2\pi)^{-s} \Gamma(s) .$$

Conjecture 1.1. The function

$$\Lambda(\mathcal{D},s) = C^{s/2} \Gamma(\mathcal{D},s) \mathcal{D}(E,s)$$

has a holomorphic continuation over the whole complex plane, and satisfies the functional equation

(1.5) $$\Lambda(\mathcal{D},s) = \Lambda(\mathcal{D},3 - s) .$$

In the next section, we shall prove this conjecture when E is a modular elliptic curve over $\mathbb{Q}$. We remark also that the general conjectures do not directly imply that the sign in the functional equation (1.5) is always $+1$.

We now explicitly calculate the Euler factors appearing in $\mathcal{D}(E,s)$. These will be used later on in the paper, and also have some

interest in their own right.

Case 1. Let r be a prime number such that E has good reduction at r. By the criterion of Néron-Ogg-Safarevic, this is equivalent to the assertion that I_r acts trivially on $T_\ell(E)$ for $\ell \neq r$. Hence

$$\mathcal{D}_r(X) = \det(1 - \rho_\ell(\mathrm{Frob}_r^{-1})X \mid \Sigma_\ell(E)) \quad (\ell \neq r) .$$

Let $\alpha_r, \beta_r \in \mathbb{C}$ be defined by

$$(1.6) \qquad (1-\alpha_r X)(1-\beta_r X) = \det(1-\rho'_\ell(\mathrm{Frob}_r^{-1})X \mid H^1_\ell(E)) ,$$

where $\rho'_\ell : G \longrightarrow \mathrm{Aut}(H^1_\ell(E))$ denotes the action of G on $H^1_\ell(E)$. Then it is easy to see that

$$(1.7) \qquad \mathcal{D}_r(X) = (1-\alpha_r^2 X)(1-\beta_r^2 X)(1-rX) ,$$

where we have used the fact that $\alpha_r \beta_r = r$.

Case 2. Let r be a prime number such that $\mathrm{ord}_r(j_E) < 0$, where j_E denotes the j-invariant of E. Then there exists a quadratic extension $K/\mathbb{Q}_r$ such that E becomes isomorphic over K to the Tate curve $E_q = \mathbb{G}_m/q^{\mathbb{Z}}$, where $q \in r\,\mathbb{Z}_r$ is given by the expansion

$$j_E = \frac{1}{q} + 744 + 196884q + \ldots .$$

Lemma 1.2. If $\mathrm{ord}_r(j_E) < 0$, we have

$$\mathcal{D}_r(X) = 1 - X .$$

Proof. It is easy to see that the ℓ-adic representation $\Sigma_\ell(E)$ does not change when we replace E by a quadratic twist. In particular, we have a D_r-isomorphism

$$\Sigma_\ell(E) \xrightarrow{\sim} \Sigma_\ell(E_q) ,$$

and so we can use the latter representation to compute $\mathcal{D}_r(X)$. Now it is well known that we have the exact sequence

(1.8) $0 \longrightarrow V_\ell(\mu) \longrightarrow V_\ell(E_q) \longrightarrow \mathbb{Q}_\ell \longrightarrow 0$,

which does not split as an exact sequence of I_r-modules. Now, for any elliptic curve A over $\mathbb{Q}_r$, the Weil pairing shows that

$$\mathrm{Sym}^2(H^1_\ell(A)) = \mathrm{Sym}^2(V_\ell(A)) \otimes V_\ell(\mu)^{\otimes(-2)} .$$

Using this observation, and the fact that (1.8) does not split as an sequence of I_r-modules, a straightforward argument of linear algebra shows that

$$\mathrm{Sym}^2(H^1_\ell(E_q))^{I_r} = \mathbb{Q}_\ell .$$

The assertion of Lemma 1.2 is now clear.

Case 3. Let r be a prime number such that E has bad reduction at r , but $\mathrm{ord}_r(j_E) \geq 0$. This is the case of potential good reduction, in which the inertia group I_r acts on $V_\ell(E)$ $(\ell \neq r)$ by a finite quotient. In fact, in the case of elliptic curves, rather precise information is known about which finite groups can occur as the image of inertia. We shall exploit this knowledge in the subsequent calculations.

For each integer $m \geq 3$ with $(r,m) = 1$, let Φ_r denote the inertia subgroup of the extension $\mathbb{Q}_r(E_m)/\mathbb{Q}_r$. It is known (see [17], p. 312) that Φ_r is independent of m , and has one of the following structures as a group (in fact, all possibilities occur):-

(a). $r > 3$. Then Φ_r is cyclic of order 2,3,4, or 6;

(b). $r = 3$. Then, if Φ_r is abelian, it is cyclic of order 2,3,4, or 6. If Φ_r is not abelian, it is the non-abelian semi-direct product of $\mathbb{Z}/4$ and $\mathbb{Z}/3$, with $\mathbb{Z}/3$ as normal subgroup;

(c). $r = 2$. Then, if Φ_r is abelian, it is cyclic of order 2,3,4, or 6. If Φ_r is non-abelian, it is either isomorphic to the quaternion group of order 8 or $SL_2(\mathbb{F}_3)$.

We first dispose of the essentially trivial case when Φ_r is cyclic of order 2.

Lemma 1.3. Assume Φ_r is of order 2. Then there exist complex numbers α_r, β_r, with absolute values $\sqrt{r}$ and $\alpha_r\beta_r = r$, such that

$$\mathcal{D}_r(X) = (1-\alpha_r^2 X)(1-\beta_r^2 X)(1-rX) .$$

Proof. The hypothesis that Φ_r is of order 2 implies that there exists a quadratic twist E' of E such that E' has good reduction at r. Since $\Sigma_\ell(E)$ is isomorphic to $\Sigma_\ell(E')$ as a Galois module, the lemma follows immediately from (1.7).

Lemma 1.4. Assume Φ_r is of order >2. If Φ_r is not cyclic, then $\mathcal{D}_r(X) = 1$. If Φ_r is cyclic, we have

$$\mathcal{D}_r(X) = \begin{cases} 1 - rX & \text{if } \mathbb{Q}_r(E_\ell)/\mathbb{Q}_r \text{ is abelian} \\ 1 + rX & \text{if } \mathbb{Q}_r(E_\ell)/\mathbb{Q}_r \text{ is not abelian,} \end{cases}$$

here ℓ denotes any prime number distinct from 2 and r.

We need a preliminary lemma. We assume $\ell \neq 2, r$.

Lemma 1.5. Put $H = \mathbb{Q}_r(E_\ell)$. Then $H/\mathbb{Q}_r$ is abelian if and only if $\mathbb{Q}_r(E_{\ell^\infty})/\mathbb{Q}_r$ is abelian.

Proof. Let M denote the maximal unramified extension of $\mathbb{Q}_r$ in $\bar{\mathbb{Q}}_r$. Assuming $H/\mathbb{Q}_r$ is abelian, it follows that the compositum $N = HM$ is abelian over $\mathbb{Q}_r$. It therefore suffices to show that $\mathbb{Q}_r(E_{\ell^\infty}) \subset N$. Since the inertia group of $\mathbb{Q}_r(E_{\ell^n})/\mathbb{Q}_r$ maps isomorphically under restriction to the inertia group of $H/\mathbb{Q}_r$ (see the above definition of Φ_r), we see that $\mathbb{Q}_r(E_{\ell^n})/H$ is unramified for all $n \geq 1$, as required.

Part (i). Assume Φ_r is cyclic of order >2, and let τ denote a generator of Φ_r. Put $F = \mathbb{Q}_r(E_{\ell^\infty})$. We can then identify Φ_r with the inertia subgroup of F over $\mathbb{Q}_r$. Let $d = \#(\Phi_r)$, and write

$$V = H^1_\ell(E) \otimes_{\mathbb{Q}_\ell} \bar{\mathbb{Q}}_\ell ,$$

where it is understood that Φ_r acts trivially on the second factor. We claim that there is a decomposition

$$V = V(\zeta) \oplus V(\zeta^{-1}), \ \dim V(\zeta) = \dim V(\zeta^{-1}) = 1 , \tag{1.9}$$

where ζ denotes a primitive d-th root of 1, and τ acts on $V(\zeta)$ (resp. $V(\zeta^{-1})$) via ζ (resp. ζ^{-1}). This is because $d > 2$, and the determinant of τ must be 1 since the Weil pairing identifies the second exterior power of V with $V_\ell(\mu)^{\otimes(-1)} \otimes \bar{\mathbb{Q}}_\ell$. Let u,v denote respective basis elements of $V(\zeta)$ and $V(\zeta^{-1})$. A straightforward exercise in linear algebra, again using the fact that $d > 2$, shows that

$$(\Sigma_\ell(E) \otimes \bar{\mathbb{Q}}_\ell)^{I_r} = \bar{\mathbb{Q}}_\ell(u \otimes v + v \otimes u) .$$

Pick any $\sigma \in G(F/\mathbb{Q}_r)$ which maps onto the inverse of the Frobenius element of the Galois group of the residue fields. It is proven in [15], p.499, that there exist complex numbers α_r, β_r with $\alpha_r\beta_r = r$ such that

$$\det(1 - \sigma X | V) = (1 - \alpha_r X)(1 - \beta_r X) .$$

Suppose first that $H/\mathbb{Q}_r$ is abelian, which, by Lemma 1.5, implies that $F/\mathbb{Q}_r$, is also abelian. Hence σ and τ commute, and thus σ respects the decomposition (1.9). Therefore, we must have

$$\sigma(u) = \alpha_r u , \ \sigma(v) = \beta_r v ,$$

and so

$$\det(1 - \sigma X | (\Sigma_\ell(E) \otimes \bar{\mathbb{Q}}_\ell)^{I_r}) = 1 - rX ,$$

as required. Suppose next that $H/\mathbb{Q}_r$ is not abelian. Thus σ and τ cannot commute, since $G(F/\mathbb{Q}_r)$ is topologically generated by τ and σ. But, as Φ_r is a normal subgroup of $G(F/\mathbb{Q}_r)$, $\sigma\tau\sigma^{-1}$ must be another generator of Φ_r which is different from τ. Since $d = 3,4,6$, we conclude that

$$\sigma\tau\sigma^{-1} = \tau^{-1} .$$

Hence σ interchanges the two eigenspaces in (1.9), and we can choose $v = \sigma(u)$. A simple argument of linear algebra, together with the fact that $\alpha_r\beta_r = r$, shows that $\sigma(u \otimes v) = -r\,(v \otimes u)$. Hence

$$\det(1 - \sigma X \mid (\Sigma_\ell(E) \otimes \bar{\mathbb{Q}}_\ell)^{I_r}) = 1 + rX .$$

This completes the proof of part (i).

Part (ii). As explained above, Φ_r has three possible structures, and, in each case, possesses a cyclic normal subgroup Δ of order d equal to 3 or 4. Fix a generator τ of this subgroup. Then we have the decomposition (1.9) for the action of Δ. Again writing u and v for generators of the two eigenspaces in (1.9), we find

$$(\Sigma_\ell(E) \otimes \bar{\mathbb{Q}}_\ell)^{\Delta} = \bar{\mathbb{Q}}_\ell\,(u \otimes v + v \otimes u) .$$

Suppose first that Φ_r is the semi-direct product of Δ with $\mathbb{Z}/4$. Then there exists λ in Φ_r such that λ and τ generate Φ_r and $\lambda\tau = \tau^2\lambda$. This relation shows that λ interchanges the two eigenspaces in (1.9), so that we can assume $v = \lambda(u)$. Since $\lambda^2 \neq 1$ on V, we must have $\lambda^2(u) = -u$, and therefore $\lambda\,(u \otimes v + v \otimes u) = -(u \otimes v + v \otimes u)$. Hence

$$(\Sigma_\ell(E) \otimes \bar{\mathbb{Q}}_\ell)^{\Phi_r} = 0 .$$

Suppose next that Φ_r contains the quaternion group Q_8 of order 8 (which is true for the two remaining cases). We claim that

$$(\Sigma_\ell(E) \otimes \bar{\mathbb{Q}}_\ell)^{Q_8} = 0 . \tag{1.10}$$

Indeed write generators τ and ρ as generators for Q_8 with the relations

$$\tau^4 = 1,\ \tau^2 = \rho^2,\ \rho\tau = \tau^3\rho\ .$$

The latter relation implies that ρ interchanges the eigenspaces in (1.9), and so we can assume again that $v = \rho(u)$. Arguing as in the previous case, we find that (1.10) is valid. This completes the proof of Lemma 1.4.

We end this section by defining a slightly different Euler product from $\mathcal{D}(E,s)$, which occurs more naturally when one applies Rankin's method. We shall call it the <u>imprimitive symmetric square</u> of E, and it is given by

$$D(E,s) = \prod_r D_r(r^{-s})^{-1}\ , \tag{1.11}$$

where

$$D_r(X) = \det(1 - \rho'_\ell(\mathrm{Frob}_r^{-1})X \mid W_\ell)\ \ (\ell \neq r)\ ;$$

here $\rho'_\ell : G \longrightarrow \mathrm{Aut}(W_\ell)$ is the representation given by

$$W_\ell = \mathrm{Sym}^2(H^1_\ell(E)^{I_r})\ ,$$

which is clearly unramified at r. Obviously, we have $D_r(X)$ divides $\mathcal{D}_r(X)$ for every prime r, and the calculations made earlier show that $D_r(X) = \mathcal{D}_r(X)$ unless E has additive reduction at r. Finally, we note that, unlike $\mathcal{D}(E,s)$, the imprimitive symmetric square $D(E,s)$ is not invariant under twisting E by quadratic characters of $\mathbb{Q}$.

§ 2. The symmetric square of a modular elliptic curve

Recall that an elliptic curve E over $\mathbb{Q}$ is said to be modular if there exists a primitive cusp form

$$f = \sum_{n=1}^{\infty} a_n q^n , \quad q = e^{2\pi i z} , \tag{2.1}$$

of weight 2 such that the Hasse-Weil L-series $L(E,s)$ of E over $\mathbb{Q}$ is given by

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s} ; \tag{2.2}$$

here a primitive cusp form means a normalized new form of some level. We assume throughout this section that E is modular. Our aim is to prove Conjecture 1.1, and also its analogue when $\mathcal{D}(E,s)$ is twisted by an arbitrary Dirichlet character χ of conductor prime to the geometric conductor of E (= the conductor of the ℓ-adic representation $V_\ell(E)$, by definition). Our method of proof will use the classical Rankin method as adapted by Li [12] and Shimura [20], and tedious case by case checking. In fact, the same results have been established by Jacquet and Gelbart [7] using representation theory (except they do not explicitly verify that their Euler factors at the bad primes coincide with the ones defined by ℓ-adic representations). While we fully admit that their approach is far more elegant and sophisticated, it seemed to us worthwhile to present for once the more classical approach. However, we do not completely avoid the use of some representation theory as we make use of the following deep theorem of Carayol [2], completing work of earlier authors. We first need some standard terminology. Let $g = \sum_{n=1}^{\infty} b_n q^n$ be a cusp form of weight 2 and character ε for $\Gamma_0(M)$, where M is any integer. If χ is a Dirichlet character, we define $g_\chi = \sum_{n=1}^{\infty} \chi(n) b_n q^n$. Then g_χ is a form of weight 2 and character $\varepsilon\chi^2$ of level the least common multiple of M and the square of the conductor of χ. If g is primitive, it is not necessarily true that g_χ is

primitive. However, assuming g primitive, there always exists a primitive form $h_\chi = \sum_{n=1}^{\infty} c_{n,\chi} q^n$ such that $c_{n,\chi} = \chi(n) b_n$ for all n which are prime to a certain finite set of primes S. We then say that h_χ is the primitive form equivalent to g_χ.

Theorem 2.1 (Carayol). Let

$$\rho_\ell : G \longrightarrow \mathrm{Aut}(T_\ell(E) \otimes_{\mathbf{Z}_\ell} \bar{\mathbf{Q}}_\ell)$$

be the ℓ-adic representation attached to a modular elliptic curve E, with associated primitive form f. For each Dirichlet charcater χ, let h_χ be the primitive form equivalent to the twist f_χ of f by χ, and let N_χ denote the exact level of h_χ. Then N_χ is equal to the conductor of the ℓ-adic representation obtained by twisting ρ_ℓ by χ. In particular, the level of f is the geometric conductor of E.

Let χ be a primitive Dirichlet character, and write c_χ for the conductor of χ. Let N be the geometric conductor of E. For the rest of this section, we impose the following hypothesis:-

Hypothesis. $(c_\chi, N) = 1$.

Write $\mathcal{D}(E,\chi,s)$ for the twist of the Dirichlet series $\mathcal{D}(E,s)$ by χ. Let C denote the conductor of the ℓ-adic representation (1.2) defining $\mathcal{D}(E,s)$, and put

$$C(\chi) = C \cdot c_\chi^3 \tag{2.3}$$

Put

$$\Gamma(\mathcal{D},\chi,s) = (2\pi)^{-s}\Gamma(s)\,\pi^{-\left(\frac{s-i_\chi}{2}\right)}\,\Gamma\left(\frac{s-i_\chi}{2}\right), \tag{2.4}$$

where $i_\chi = 0$ or 1 and $\chi(-1) = (-1)^{i_\chi}$. Finally, we put

$$G(\chi) = \sum_{a=1}^{c_\chi} \chi(a) \exp\left(\frac{2\pi i a}{c_\chi}\right), \tag{2.5}$$

$$W(\chi) = \chi(C)\sqrt{\chi(-1)c_\chi}\,\frac{G(\chi)}{G(\bar{\chi})^2}. \tag{2.6}$$

The principal result of this section is the following.

Theorem 2.2. Assume E is modular of conductor N, and that $(c_\chi, N) = 1$. Then

$$\Lambda(\mathcal{D},\chi,s) = C(\chi)^{s/2}\Gamma(\mathcal{D},\chi,s)\mathcal{D}(E,\chi,s)$$

has a holomorphic continuation over the whole complex plane, and satisfies the functional equation

$$\Lambda(\mathcal{D},\chi,s) = W(\chi)\ \Lambda(\mathcal{D},\bar{\chi},3-s) .$$

Following Li [12], the first step in the proof of Theorem 2.2 is to replace f by a primitive form g of possibly lower level. Indeed, we take g to be any form of weight 2 satisfying the following conditions:-

(2.7) g is primitive of level dividing the level N of f;

(2.8) there exists a Dirichlet character ε such that $g_\varepsilon = f$,

(2.9) the level of g is minimal amongst all forms satisfying the previous two conditions.

Clearly such a g always exists, but it need not be unique. We write M for the level of g (plainly M is unique), and call g a minimal form associated with f. Since f has trivial character, g must have character

$$\nu = \bar{\varepsilon}^2 . \tag{2.10}$$

We denote the Fourier expansion of g by

$$g = \sum_{n=1}^{\infty} b_n q^n . \tag{2.11}$$

For each prime r dividing M, we introduce the following strange Euler factor

$$\rho_r(X) = \begin{cases} 1 + rX & \text{if } b_r = 0 \text{ and } \mathrm{ord}_r(M) \text{ is even,} \\ 1 & \text{otherwise .} \end{cases}$$

We then define the Dirichlet series

$$(2.12) \qquad \mathcal{D}(g,s) = \prod_{r|M} \rho_r(r^{-s})^{-1} \frac{\zeta_M(2s-2)}{\zeta_M(s-1)} \sum_{n=1}^{\infty} \frac{|b_n|^2}{n^s} ,$$

where the subscript M indicates that the Euler factors at the primes dividing M have been omitted from the zeta functions. Let $\mathcal{D}(g,\chi,s)$ be the twist of this Dirichlet series by χ. Finally, for each prime r dividing M, we put

$$m(r) = \begin{cases} \left[\frac{\mathrm{ord}_r M}{2}\right] & \text{if } b_r = 0 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$B = \prod_{r|M} r^{\mathrm{ord}_r M - m(r)} .$$

We obtain Theorem 2.2 on combining the following two results, whose proof will take up the remainder of this section. Put

$$(2.13) \qquad A(\chi) = B^2 c_\chi^{\,3} , \quad W(g,\chi) = \chi(B^2)\sqrt{\chi(-1)c_\chi}\, G(\chi)/G(\bar{\chi})^2 .$$

Theorem 2.3. Assume $(c_\chi, N) = 1$, and put

$$\Lambda(g,\chi,s) = A(\chi)^{s/2}\Gamma(\mathcal{D},\chi,s)\mathcal{D}(g,\chi,s) .$$

Then $\Lambda(g,\chi,s)$ has a holomorphic continuation over the whole complex plane, and satisfies

$$\Lambda(g,\chi,s) = W(g,\chi)\ \Lambda(g,\bar{\chi},3-s) .$$

Theorem 2.4. We have $\mathcal{D}(g,s) = \mathcal{D}(E,s)$ and $C = B^2$.

The proof of Theorem 2.3, which will be given first, will be an application of results of Li [12] and Shimura [20]. Our proof of Theorem 2.4 will unfortunately consist of elaborate case by case checking at the bad primes.

We now begin the proof of Theorem 2.3. Put

$$M_\chi = Mc_\chi^2 .$$

We wish to apply Theorem 2.2 of [12] to the primitive forms $F_1 = g$ and $F_2 = g_\chi^-$. Our assumption that $(c_\chi, N) = 1$ implies that g_χ^- is primitive of level M_χ. We must first verify that conditions A), B), C) on p.141 of [12] are valid. As in [12], we decompose each integer R and each Dirichlet character ψ mod R as

$$R = \prod_{r|R} R_r \ , \ \psi = \prod_{r|R} \psi_r \quad (r \text{ prime}) \ ,$$

where $R_r = r^{\mathrm{ord}_r(R)}$ and ψ_r is a character modulo R_r. In the notation of [12], we have

$$M' = \prod_{r|c_{\chi^2}} c_{\chi_r^2}^2 / c_{\chi_r^2}$$

$$M'' = M \cdot \prod_{\substack{r|c_\chi \\ \chi_r^2 = 1}} c_{\chi_r}^2 .$$

(For any Dirichlet character ψ we write c_ψ for the conductor of ψ). Condition A) is valid, since for all $r|M''$ with $(r, c_\chi) = 1$, the forms F_1 and F_2 are certainly r-primitive in the sense of [12] by the minimality of g and the condition $(r, c_\chi) = 1$. As for condition B), it is true because for each prime $r|M'$ and each character ψ of r-power conductor, g_ψ and $g_{\chi\psi}^-$ are both primitive forms of respective levels

$$\tilde{N}_1 = M c_\psi^2 \ , \ \tilde{N}_2 = M c_{\chi\psi}^2 \ ,$$

and one sees easily that the least common multiple of $\tilde{N}_1$ and $\tilde{N}_2$ is at least M_χ . Finally, Condition C) is vacuously true since $(M,M') = 1$. For each prime $r|M''$, Li [12] elaborately defines on p.142 an Euler factor which she writes $\theta_r(s,F_1,F_2)$. Here is a simple description of this Euler factor in the case considered here.

Lemma 2.5. The Euler factor $\theta_r(s,F_1,F_2)$ on p.142 of [12] is given by

$$\theta_r(s,F_1,F_2) = \grave{a}_r(\chi(r)r^{-s}) \ ,$$

where $\grave{a}_r(X) = 1$ if $(r,M) = 1$ and

$$\grave{a}_r(X) = (1-X)\rho_r(r^{-1}X) \quad \text{if} \quad r|M \ .$$

Proof. This is an immediate consequence of the explicit description of $\theta_r(s,F_1,F_2)$ on p.142, and the known fact that $|b_r|^2$ is equal to r,1, or 0, according as we are in the three cases (i) $M_r = c_{\nu_r}$, (ii) $M_r = r$ and $\nu_r = 1$, and (iii) otherwise.

Our next step is to verify that our definition of the integer $m(r)$ coincides with that given in [12]. We begin with some notation. For any integer R and a prime r dividing R , let $W(r)$ denote the operator on forms of level R given by

$$W(r) = \begin{pmatrix} R_r x & y \\ Rz & R_r w \end{pmatrix} \ ,$$

where the integers x,y,z,w are chosen so that $x \equiv 1 \bmod R/R_r$, $y \equiv 1 \bmod R_r$, and $\det(W(r)) = R_r$. If F is a primitive form of level R , it is known that

$$F|W(r) = \lambda_r(F)F' \ ,$$

for some primitive form F' and a scalar $\lambda_r(F)$ of absolute value 1

- this equation then defines $\lambda_r(F)$. Now take r to be any prime dividing M such that $b_r = 0$. Following [12], we define $n(r)$ to be the largest integer n such that

$$\frac{\lambda_r(g_\psi)}{\lambda_r(g_{\bar{\chi}\psi})} = \frac{\lambda_r(g)}{\lambda_r(g_{\bar{\chi}})}$$

for all characters ψ with conductor dividing r^n .

Lemma 2.6. If $b_r = 0$, we have $n(r) \geq \left[\frac{\mathrm{ord}_r M}{2}\right]$, and thus our definition of $m(r)$ coincides with that of [12].

Proof. We consider the operator

$$R_\chi = \sum_{n=1}^{c_\chi} \bar{\chi}(u) \begin{pmatrix} c_\chi & 1 \\ 0 & c_\chi \end{pmatrix}^u ,$$

which has the properties (see [1])

$$g|R_\chi = G(\bar{\chi})g_\chi \ , \ g|R_\chi W(r) = \bar{\chi}(M_r)\cdot g|W(r)R_\chi \ .$$

This shows that

$$\frac{\lambda_r(g)}{\lambda_r(g_{\bar{\chi}})} = \bar{\chi}(M_r) \ .$$

On the other hand, by the minimal choice of g and the fact that $b_r = 0$, for each character ψ of r-power conductor, g_ψ will again be primitive of exact level say $M(\psi)$, where M divides $M(\psi)$. Hence we can apply the same argument with g replaced by g_ψ to conclude that

$$\frac{\lambda_r(g_\psi)}{\lambda_r(g_{\psi\bar{\chi}})} = \bar{\chi}(M(\psi)_r) \ .$$

To complete the proof of the lemma, we must show that $M(\psi)_r = M_r$ for all characters ψ of r-power conductor such that $c_\psi^2 | M_r$. By the minimality of g , it suffices to prove that $M(\psi)_r \leq M_r$ for all such

ψ , which follows from the fact that

$$g_\psi \text{ has level the LCM of } M, c_\psi^2, c_\psi c_\nu$$

and character $\nu\psi^2$, and Theorem 4.3 of [1] which shows that $(c_\nu)_r \leq \sqrt{M_r}$.

We now simplify the elaborate root number which occurs in [12]. For each prime $r|M'$, let $\Lambda_r(F_1,F_2)$ be as defined on p.143 of [12]. Note that, in our case, the set P of [12] is empty, and that only case IV of [12] occurs, since we have

$$M_r = 1 \ , \ c_{\chi_r} \neq 1 \ , \ b_r \neq 0 \ , \ \chi(r)b_r = 0 \ .$$

For brevity, let us put $c_r = c_{\chi_r}$. Define Q_r to be $M_r'^2$ or c_r^2 , according as $M_r' > c_r$ or not. Let ϕ_r be the primitive Dirichlet character attached to $(\chi/\chi_r)^2$. Then the definition of $\Lambda_r = \Lambda_r(F_1,F_2)$ is

$$\Lambda_r = (\bar{\nu}\phi_r)(c_r^2)\ \bar{\Phi}_r(M_r')\ \overline{G\ (\chi_r^2)\lambda_r(g_\chi^-)^2}\ Q_r c_r^{-2} \ .$$

Lemma 2.7. Assume that $r|M'$, and put $\delta_r = 1$ or 2 according as r is odd or even. Then

$$\Lambda_r = G(\bar{\chi}_r^2)\left(\frac{G(\chi_r)}{G(\bar{\chi}_r)}\right)^2 \delta_r^2\ \bar{\Phi}_r(\delta_r c_r) \ .$$

Proof. For $r|c_{\chi^2}$, we have $c_{\chi_r^2} = c_r/\delta_r$ and thus

$$M_r' = \delta_r c_r \ , \ Q_r = (\delta_r c_r)^2 \ .$$

It follows that

$$\Lambda_r = \bar{\nu}(c_r^2)\ \overline{G(\chi_r^2)}\ \overline{\lambda_r(g_\chi^-)^2}\ \delta_r^2\ \phi_r(c_r/\delta_r) \ .$$

By Theorem 4.1 of [1], we have

$$\lambda_r(g_{\chi_r}^-) = \bar{\nu}(c_r)\bar{\chi}_r(-1)G(\bar{\chi}_r)/G(\chi_r) \ .$$

Also by Proposition 3.4 of [1],

$$(g_{\chi_r}^- | R_{\chi\chi_r}^- W(r) = \phi_r(c_r) g_{\chi_r}^- | W(r) R_{\chi\chi_r}^- ,$$

and so, by comparison of the first Fourier coefficients,

$$G(\bar{\chi}\chi_r)\lambda_r(g_\chi^-) = \phi_r(c_r)\lambda_r(g_{\chi_r}^-)G(\bar{\chi}\chi_r) ,$$

whence

$$\lambda_r(g_\chi^-) = \phi_r(c_r)\bar{\nu}(c_r)\overline{G(\chi_r)}/G(\chi_r) .$$

Substituting this into the above expression for Λ_r , we obtain the assertion of the lemma.

We next derive a simpler expression for the elaborate function $A_\chi(s)$ defined on p.144 of [12], which regrettably in [12] mixes up the root number and the conductor. The definition of $A_\chi(s)$ is as follows

$$A_\chi(s) = A_{\chi,1}(s)A_{\chi,2}(s)A_{\chi,3}(s) ,$$

where

$$A_{\chi,1}(s) = \prod_{r|M} (\chi^2(r)r^{1-2s})^{\mathrm{ord}_r M - m(r)} ,$$

$$A_{\chi,2}(s) = \prod_{\substack{r|c_\chi \\ r\nmid c_{\chi^2}}} (\chi^2(r)r^{1-2s})^{2\mathrm{ord}_r c_\chi} ,$$

$$A_{\chi,3}(s) = \prod_{r|c_{\chi^2}} G(\chi_r^2)\Lambda_r\left(\frac{c_r^2}{M_r'}\right)^{1-2s} Q_r^{-s}\,\Phi_r\left(\frac{Q_r c_r^2}{M_r'}\right) .$$

Lemma 2.8.

$$A_\chi(s) = \frac{W(g,\chi)G(\chi)}{\sqrt{\chi(-1)c_\chi}}\left(Bc_\chi^2\right)^{1-2s} .$$

Proof. Clearly, we have $A_{\chi,1}(s) = \chi(B^2)B^{1-2s}$. For $r|c_\chi$, put

$$H_{r,\chi}(s) = \frac{G(\chi_r)^2}{G(\bar{\chi}_r)^2} (c_r^2)^{1-2s} \phi_r(c_r^2) .$$

By Lemma 2.7, we have

$$A_{\chi,3}(s) = \prod_{r|c_{\chi^2}} H_{r,\chi}(s) .$$

On the other hand, it is plain that

$$A_{\chi,2}(s) = \prod_{\substack{r|c_\chi \\ r\nmid c_{\chi^2}}} H_{r,\chi}(s) .$$

The assertion of the Lemma now follows from the well known decomposition formula

$$G(\chi) = \prod_{r|c_\chi} (\chi\bar{\chi}_r)(c_r) \cdot G(\chi_r) .$$

Put

$$\Gamma(\chi,s) = \pi^{-(\frac{s+i_\chi}{2})} \Gamma(\frac{s+i_\chi}{2}) .$$

Proposition 2.9. The function

$$\Omega(\chi,s) = \Lambda(g,\chi,s+1) c_\chi^{s/2} \Gamma(\chi,s) L(\chi,s)$$

has a holomorphic continuation over the whole complex plane, except for simple poles at $s = 0$ and $s = 1$ when χ is the trivial character, and satisfies the functional equation

$$\Omega(\chi,s) = \frac{W(g,\chi)G(\chi)}{\sqrt{\chi(-1)c_\chi}} \Omega(\bar{\chi},1-s) .$$

Proof. Recall that the function $L_{g,g_\chi^-}(s)$ is defined in [12] by

$$L_{g,g_\chi^-}(s) = L_{Mc_\chi}(\chi^2,2s) \sum_{n=1}^{\infty} \chi(n)|b_n|^2 \cdot n^{-(s+1)} .$$

In view of Lemma 2.5, we have

$$\prod_{r|M^n} a_r(\chi(r)r^{-s})^{-1} L_{g,g_{\bar{\chi}}}(s) = \mathcal{D}(g,\chi,s+1)L(\chi,s) .$$

The assertion of the proposition now follows from Lemma 2.8 and Theorem 2.2 of [12].

Corollary 2.10. $\Lambda(g,\chi,s)$ has a meromorphic continuation over the whole complex plane, and satisfies the functional equation given in Theorem 2.3.

This is immediate on combining Proposition 2.9 with the known functional equation for the Dirichlet L-series. Hence, to complete the proof of Theorem 2.3, we need only prove that $\Lambda(g,\chi,s)$ is entire. We do this by appealing to a basic result of Shimura [20]. To do this, we must slightly modify the above functions. Recall that the character ν of the form g is a character modulo M, and is not necessarily primitive. In the following, we write ν_0 for the primitive character associated with ν, and c_ν for its conductor. Recall that $\mathcal{D}(g,s)$ is defined by (2.12). Put

$$H(g,s) = \left(\sum_{n=1}^{\infty} \frac{b_n^{2-}\nu_0(n)}{n^s} \right) \cdot \frac{\zeta_M(2s-2)}{\zeta_M(s-1)} .$$

Let S be the set of primes r dividing M such that $\mathrm{ord}_r(M) = \mathrm{ord}_r(c_\nu)$.

Lemma 2.11. We have

$$\mathcal{D}(g,s) = U(g,s)H(g,s) , \tag{2.14}$$

where $U(g,s)$ is the finite Euler product

$$U(g,s) = \prod_{r|M} \rho_r(r^{-s})^{-1} \prod_{p\in S} (1-p^{1-s})^{-1} . \tag{2.15}$$

Proof. This boils down to showing that

$$\sum_{n=1}^{\infty} \frac{|b_n|^2}{n^s} = \left(\sum_{n=1}^{\infty} \frac{b_n^2 \overline{\nu_0}(n)}{n^s} \right) \times \prod_{p \in S} (1-p^{1-s})^{-1} .$$

This identity is an easy consequence of the standard lemma 1 on p.790 of [21], the knowledge of the absolute value of b_r for $r|M$ described in the proof of Lemma 2.5, and the fact that $\overline{b_n} = \overline{\nu_0}(n) b_n$ for $(n, c_\nu) = 1$ because g is primitive.

To complete the proof of Theorem 2.3, we shall apply Theorem 2 on p. 94 of [20], and the two remarks following it. Write $H(g,\chi,s)$ for the twist of the Dirichlet series $H(g,s)$ by χ, and put

$$\Theta(\chi,s) = \Gamma(\mathcal{D},\chi,s) H(g,\chi,s) .$$

Then [20] shows that $\Theta(\chi,s)$ is holomorphic, except possibly at $s = 1$ or $s = 2$. We claim that $\Theta(\chi,s)$ must in fact be holomorphic at $s = 2$. For the validity of condition (i) and (ii) of Theorem 2, together with Remark 2, would imply that $\chi^2 = 1$ and $\chi(-1) = -1$. But Remark 1 shows then that $\chi(n) = 1$ for all n prime to Mc_χ (since we know already that $\overline{b_n} = \overline{\nu_0}(n) b_n$ for all n prime to c_ν, because g is primitive), which is a contradiction. From (2.14), and the explici form (2.15) of the Euler factors $U(g,s)$, we conclude that (i) $\Lambda(g,\chi,s)$ is holomorphic on the line $R(s) = 2$, and (ii) the only possible poles of $\Lambda(g,\chi,s)$ are on the line $R(s) = 1$. But the functional equation of Theorem 2.3 (which, as remarked in Corollary 2.10, is already established) shows that a pole on the line $R(s) = 1$ for $\Lambda(g,\chi,s)$ implies the existence of a pole on the line $R(s) = 2$ for $\Lambda(g,\bar{\chi},s)$. This completes the proof of Theorem 2.3.

We now return to the proof of Theorem 2.4, postponing the case by case verification as long as possible. We begin by noting the following Euler product for $H(g,s)$, which is immediate from Lemma 1 on p.790 of [21]. For each prime r, let $\gamma_r, \delta_r \in \mathbb{C}$ be such that

$$\sum_{n=1}^{\infty} b_n n^{-s} = \prod_r (1-\gamma_r r^{-s})^{-1} (1-\delta_r r^{-s})^{-1} .$$

Lemma 2.12.

$$(2.16)\quad H(g,s) = \prod_r (1-\bar{\nu}_0(r)\gamma_r^2 r^{-s})^{-1} (1-\bar{\nu}_0(r)\delta_r^2 r^{-s})^{-1} (1-\bar{\nu}_0(r)\gamma_r\delta_r r^{-s})^{-1} .$$

We first verify Theorem 2.4 for all primes r such that $(r,M) = 1$. Let r be such a prime. By (2.14), the r-Euler factor of $\mathcal{D}(g,s)$ is the same as the r-Euler factor of $H(g,s)$. If $(r,N) = 1$, we know that $\gamma_r = \bar{\varepsilon}(r)\alpha_r$, $\delta_r = \bar{\varepsilon}(r)\beta_r$, where α_r,β_r are given by (1.6). As $\nu = \bar{\varepsilon}^{-2}$, we see from (1.7) that $\mathcal{D}(E,s)$ and $H(g,s)$ have the same Euler factor at r. Next we claim that the case $r|N$ and $(r,M) = 1$ can be reduced to the previous case. Indeed, if $r|N$, we have $(c_{\varepsilon^2},r) = 1$ because c_{ε^2} divides M. Hence, if ε_r denotes the r-part of ε, we see that $\varepsilon_r^2 = 1$. Now replace E by its twist E' by the quadratic character ε_r. Then E' must have good reduction at r, since $g_{\varepsilon\varepsilon_r}$ has its r-th Fourier coefficient non-zero ($g_{\varepsilon\varepsilon_r}$ is the primitive form corresponding to E' and has level prime to r). Since $\mathcal{D}(E,s) = \mathcal{D}(E',s)$, we have justified the above claim. It also follows that $\mathrm{ord}_r(B^2) = \mathrm{ord}_r(C) = 0$.

We next verify Theorem 2.4 at all primes r such that $\mathrm{ord}_r(j_E) < 0$. In fact, we can then suppose that E has split multiplicative reduction at r, since this will certainly be true for a twist of E by a quadratic character, and such a twist does not change $\mathcal{D}(E,s)$. Hence

$$\mathrm{ord}_r(N) = 1 , \quad \mathcal{D}_r(X) = 1 - X .$$

Thus necessarily $\mathrm{ord}_r(M) = 1$ and $\mathrm{ord}_r(c_\nu) = 0$. By the results of [11] applied to g, we must then have

$$\gamma_r = 0 , \quad \delta_r^2 = \nu(r) .$$

This proves that $H(g,s)$ has the r-Euler factor $1-r^{-s}$, and so the

same is true for $\mathcal{D}(g,s)$ since $U(g,s)$ has Euler factor 1 at r. Also $\mathrm{ord}_r(B) = 1$ because $b_r \neq 0$, and $\mathrm{ord}_r(C) = 2$, since, in the case of split multiplicative reduction, the extension $\mathbb{Q}_r(E_\ell)/\mathbb{Q}_r$ is tamely ramified for all $\ell \neq r$. Thus Theorem 2.4 is true for all such r.

We now turn to the remaining bad primes. These are characterized by the condition that E has potential good reduction at r and the group Φ_r defined in § 1 satisfies

(2.17) $\#(\Phi_r) > 2$.

Lemma 2.13. Let r be a prime of potential good reduction satisfying (2.17). Then the r-Euler factor of $\mathcal{D}(g,s)$ is given by $\mathcal{D}_r(g,r^{-s})$, where

$$\mathcal{D}_r(g,X) = 1-rX,\ 1+rX,\ 1,$$

according as (i) $\mathrm{ord}_r(M) = \mathrm{ord}_r(c_\nu)$, (ii) $\mathrm{ord}_r(c_\nu) < \mathrm{ord}_r(M)$ and $\mathrm{ord}_r(M)$ even, and (iii) $\mathrm{ord}_r(c_\nu) < \mathrm{ord}_r(M)$ and $\mathrm{ord}_r(M)$ odd and ≥ 3.

Proof. This is clear from Lemma 2.11, 2.12 and Theorem 3 of [11].

In view of Lemma 1.4, we must therefore show that the cases (i), (ii) and (iii) of Lemma 2.13 correspond exactly to the three possibilities (here m is any integer ≥ 3 with $(m,r) = 1$ and (2.17) is assumed to hold) (a) Φ_r cyclic and $\mathbb{Q}_r(E_m)/\mathbb{Q}_r$ abelian, (b) Φ_r cyclic and $\mathbb{Q}_r(E_m)/\mathbb{Q}_r$ non-abelian, and (c) Φ_r non-cyclic.

Lemma 2.14. Let r be a prime of potential good reduction satisfying (2.17). For each prime $\ell \neq 2,r$, the extension $\mathbb{Q}_r(E_\ell)/\mathbb{Q}_r$ is abelian if and only if $\mathrm{ord}_r(M) = \mathrm{ord}_r(c_\nu)$.

Proof. Let H denote the maximal unramified extension of $\mathbb{Q}_r$ in $\bar{\mathbb{Q}}_r$ and suppose that $\mathbb{Q}_r(E_\ell)/\mathbb{Q}_r$ is abelian. Then $H(E_\ell)/\mathbb{Q}_r$ is abelia

and we may identify the inertia group of this extension by restriction to $\mathbb{Q}_r(E_\ell)$ with Φ_r. We choose a representative $\sigma \in G(H(E_\ell)/\mathbb{Q}_r)$ for the Frobenius automorphism, and we denote by Γ the topological closure of the cyclic group generated by σ. Thus we clearly have the following decomposition as a direct product

$$G(H(E_\ell)/\mathbb{Q}_r) = \Phi_r \times \Gamma .$$

Note that $H(E_{\ell^\infty}) = H(E_\ell)$. Now let L denote the totally ramified extension of $\mathbb{Q}_r$ given by the Galois invariants under Γ. By local class field theory the cyclic extension $L/\mathbb{Q}_r$ corresponds to a character λ on $\mathbb{Z}_r^\times$ of finite order. The latter turns up in the ℓ-adic representation ρ_ℓ in Theorem 2.1 as well, since ρ_ℓ, when restricted to $G(\bar{\mathbb{Q}}_r/\mathbb{Q}_r)$, factors of course through $G(H(E_\ell)/\mathbb{Q}_r)$. Moreover ρ_ℓ is injective on Φ_r and diagonalizes. We may therefore assume that for $\tau \in \Phi_r$ we have

$$\rho_\ell(\tau) = \begin{pmatrix} \lambda(\tau) & 0 \\ 0 & \lambda(\tau)^{-1} \end{pmatrix} .$$

Thus after tensoring ρ_ℓ by λ we arrive at $(\rho_\ell \otimes \lambda)(\tau) = \begin{pmatrix} \lambda^2(\tau) & 0 \\ 0 & 1 \end{pmatrix}$,

which by a straightforward calculation turns out to be a twist of ρ_ℓ of minimal r-conductor among all twists by characters whose conductor is an r-power. So by Theorem 2.1 we get

$$M_r = N_{\varepsilon_r, r} \ , \ \nu_r = \bar{\varepsilon}_r^{\,2} \ ,$$

where now we have chosen a Dirichlet character ε_r of r-power conductor which locally at r is λ. In particular we see that $M_r = c_{\nu_r} = c_{\lambda^2}$.

Now we suppose $M_r = c_{\nu_r}$ and we shall prove that this implies that $\mathbb{Q}_r(E_\ell)/\mathbb{Q}_r$ is abelian. By the assumption $M_r = c_{\nu_r}$ the r-Euler

factor of the L-function attached to g is given by $1-b_r r^{-s}$ where $|b_r| = \sqrt{r}$. Hence the associated ℓ-adic representation $\rho_\ell \otimes \bar{\varepsilon}_r$ posesses non-trivial invariants in $V_\ell(E) \otimes \bar{\varepsilon}_r$ under the action of th inertia group. So we find $x \neq 0$ in $T_\ell(E) \otimes \bar{\mathbb{Q}}_\ell$ such that $\tau(x) = \varepsilon_r(\tau) \cdot x$ for $\tau \in \Phi_r$. By the same reasonning as in part (ii) of the proof of Lemma 1.4 this cannot happen if Φ_r is non-cyclic. Thus Φ_r is necessarily cyclic and therefore there is a second basis vector $y \in T_\ell(E) \otimes \bar{\mathbb{Q}}_\ell$ such that $\tau(y) = \bar{\varepsilon}_r(\tau) \cdot y$ for $\tau \in \Phi_r$, since by the Weil pairing Φ_r acts trivially on $x \otimes y - y \otimes x$. So the totally ramified cyclic extension $L/\mathbb{Q}_r$ which is defined by the character ε_r , is contained in $\mathbb{Q}_r(E_{\ell^\infty})$. Moreover $\mathbb{Q}_r(E_{\ell^\infty})/L$ is unramified, hence $\mathbb{Q}_r(E_{\ell^\infty})$ is abelian over $\mathbb{Q}_r$ thus completing the proof.

We can now verify Theorem 2.4 at all remaining bad primes $r \neq 2,3$ Since for these primes Φ_r is always cyclic and satisfies (2.17), the equality of r-Euler factors $\mathcal{D}_r(g,X) = \mathcal{D}_r(X)$ is obvious by Lemmas 2.13 and 2.14. In addition these primes have no wild ramification, so that $C_r = r^2$ since

$$\dim_{\mathbb{Q}_\ell}(\Sigma_\ell(E))^{I_r} = \text{degree } \mathcal{D}_r(X) = 1 .$$

On the other hand by definition of B we have $\text{ord}_r(B) = \text{ord}_r(M) - m(r)$ where $m(r) = [\text{ord}_r(M)/2]$ or 0 according as $M_r = r^2$ or not. Here we have used the fact from [11] that $b_r = 0$ if and only if r^2 divides M and c_ν divides M/r . So we get $B_r = r$ and therefore $C_r = B_r^2$.

The verification of Theorem 2.4 at the bad primus $r = 2,3$ will be achieved by the following tables whose proof will be given in the Appendix. These tables clearly imply that $\mathcal{D}_r(g,X) = \mathcal{D}_r(X)$ and $C_r = B_r^2$ for $r = 2,3$. We would like to point out that we do not claim that all considered cases occur in reality.

Φ_3	$G(\mathbb{Q}_3(E_4)/\mathbb{Q}_3)$	$ord_3(N)$	$ord_3(M)$	$ord_3(c_\varepsilon)$	$ord_3(c_\nu)$	$ord_3(B)$	$ord_3(C)$
$\mathbb{Z}/3$	abelian	4	2	2	2	2	4
	non-abelian	4	4	0	0	2	4
$\mathbb{Z}/4$	non-abelian	2	2	0	0	1	2
$\mathbb{Z}/6$	abelian	4	2	2	2	2	4
	non-abelian	4	4	0	0	2	4
$\mathbb{Z}/4\rtimes\mathbb{Z}/3$	non-abelian	3	3	0	0	2	4
		5	5	0	0	3	6

Φ_2	$G(\mathbb{Q}_2(E_3)/\mathbb{Q}_2)$	$ord_2(N)$	$ord_2(M)$	$ord_2(c_\varepsilon)$	$ord_2(c_\nu)$	$ord_2(B)$	$ord_2(C)$
$\mathbb{Z}/3$	non-abelian	2	2	0	0	1	2
$\mathbb{Z}/4$	non-abelian	8	6	4	3	3	6
$\mathbb{Z}/6$	non-abelian	4	2	2	0	1	2
		6	2	3	0	1	2
Q_8	non-abelian	5	5	0	0	3	6
		6	5	3	0	3	6
		9	9	0	0	5	10
$SL_2(\mathbb{F}_3)$	non-abelian	3	3	0	0	2	4
		4	3	2	0	2	4
		6	3	3	0	2	4
		7	7	0	0	4	8

§ 3. The p-adic analogue of the symmetric square

As before, E will denote a modular elliptic curve over $\mathbb{Q}$, and $D(E,s)$ the L-series attached to the symmetric square of the ℓ-adic representations $H^1_\ell(E)$. Our aim in this section is to construct a p-adic analogue of $D(E,s)$ for all odd prime numbers p at which E has good ordinary reduction. We begin by establishing a strengthened form of a result of Sturm [22] about the algebraicity of the special values of the twists of $D(E,s)$ by Dirichlet characters.

3.1. The algebraicity result. If f_1, f_2 are two forms of weight 2 for $\Gamma_0(N)$, one of which is a cusp form, we normalize the Petersson inner product via

$$\langle f_1, f_2 \rangle_N = \int_{B(N)} \overline{f_1(z)}\, f_2(z)\, dxdy ,$$

where $B(N)$ denotes a fundamental domain for the action of $\Gamma_0(N)$ on the upper half plane. If $D(E,s) = \sum_{n=1}^{\infty} \frac{d_n}{n^s}$ and χ is a Dirichlet character, we recall that $D(E,\chi,s) = \sum_{n=1}^{\infty} \frac{\chi(n) d_n}{n^s}$. Recall also that $G(\chi)$ denotes the Gauss sum of χ. Define

$$\rho(E,\chi) = \frac{G(\bar{\chi})\, D(E,\chi,1)}{\pi \langle f, f \rangle_N} , \tag{3.1}$$

where N is the conductor of E, and f is the primitive cusp form of weight 2 and level N corresponding to E.

Theorem 3.1. Assume that (i) the conductor c_χ of χ is prime to $2N$, and (ii) χ is not the non-trivial character of a real quadratic field. Then, for each automorphism σ of $\mathbb{C}$, we have $\rho(E,\chi)^\sigma = \rho(E,\chi^\sigma)$. In particular, $\rho(E,\chi)$ belongs to $\bar{\mathbb{Q}}$.

Remarks. (i) Results of this kind for the imprimitive symmetric square $D(E,\chi,s)$ were first proven by Sturm [22]. However, since the

Euler factors at the bad primes may vanish at $s=1$, we cannot apply Sturm's argument directly to the point $s=1$. Instead, we first apply Sturm's argument at the point $s=2$, where the Euler factors never vanish, and then apply the functional equation for $\mathcal{D}(E,\chi,s)$.

(ii). Theorem 3.1 is trivially true for all characters χ with $\chi(-1) = -1$, since the Γ-factors in the functional equation for the entire function $\Lambda(\mathcal{D},\chi,s)$ imply that $\mathcal{D}(E,\chi,s)$ must vanish at $s=1$ in this case.

(iii). The special case of Theorem 3.1 when χ is the trivial character χ_0 can be established more directly. If $f = \sum_{n=1}^{\infty} a_n q^n$, we have

$$D(E,s) = \frac{\zeta_N(2s-2)}{\zeta_N(s-1)} \sum_{n=1}^{\infty} \frac{a_n^2}{n^s},$$

where, as before, the subscript N means that the Euler factors at the primes dividing N have been omitted from the corresponding Euler products. Expressing the Dirichlet series on the right as a Rankin integral as in [ ], we conclude easily from (2.5) of [21] that

$$D(E,2) = \frac{288\ \pi^3}{N} \langle f,f\rangle_N .$$

Since

$$\mathcal{D}(E,s) = D(E,s) \prod_{p\in S_1} H_p(p^{-s})^{-1}, \tag{3.2}$$

where S_1 is a finite set of bad primes, and where $H_p(X)$ is a polynomial in $\mathbb{Q}[X]$ which does not vanish at $s=2$, it follows immediately that $\pi^{-3}\langle f,f\rangle_N^{-1}\ \mathcal{D}(E,2)$ belongs to $\mathbb{Q}$, whence the functional equation implies that $\pi^{-1}\langle f,f\rangle_N^{-1}\ \mathcal{D}(E,1)$ belongs to $\mathbb{Q}$, as required.

(iv). When χ is the non-trivial character of a real quadratic field, the conclusion of Theorem 3.1 almost certainly remains correct. However, we can do no better than Sturm [22] in this case, who showed that the

conclusion of Theorem 3.1 is valid if we replace $D(E,\chi,s)$ by the imprimitive function $D(E,\chi,s)$.

We now give the proof of Theorem 3.1, as we shall need the main ingredients of it for the p-adic constructions to follow. We refer the reader to the papers of Shimura [20] and Sturm [22] for the results on Fourier expansions of Eisenstein series of half integral weight which we quote without proof. In general, we use the notation of Shimura [19] when working with modular forms of half integral weight. In particular if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an element of $SL_2(\mathbb{Z})$ with $c \equiv 0 \bmod 4$, we recall that

$$j(\gamma,z) = \left(\frac{c}{d}\right)\varepsilon_d^{-1}(cz+d)^{1/2} ,$$

where $\varepsilon_d = 1$ or i , according as $d \equiv 1$ or $3 \bmod 4$, and the usual conventions of [19] are valid.

We first note that we can assume, without loss of generality, that the conductor N of E is divisible by 4. Indeed, if this is not true for E itself, it is easily seen to be true for the twist of E by the unique quadratic character of conductor 4, and, as was remarked earlier, the function $D(E,s)$ is invariant under the twists of E by quadratic characters.

The first main step in the proof is to give one of the classical expressions for the imprimitive function $D(E,\chi,s)$ as a Rankin integral. Let

$$\theta_\chi(z) = \frac{1}{2} \sum_{n=-\infty}^{\infty} \chi(n) q^{n^2} ,$$

which is of weight $\frac{1}{2}$ and level $4c_\chi^2$ (see [19]). Put

(3.3) $\qquad N_\chi = Nc_\chi^2$, where c_χ = conductor of χ .

Let W_χ denote a set of representatives of $\Gamma_\infty \backslash \Gamma_0(N_\chi)$, where Γ_∞ denotes the group of matrices $\pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ with $m \in \mathbb{Z}$. Following [20],

we define the Eisenstein series of weight $\frac{3}{2}$ via

$$E(z,\chi,s) = \sum_{\gamma \in W_\chi} y^{s/2} \chi(d_\gamma) j(\gamma,z)^{-3} |j(\gamma,z)|^{-2s} ,$$

where $z = x + iy$, and d_γ denotes the entry in the lower right hand corner of γ. Define

$$(3.4) \qquad \Phi(z,\chi,s) = L_{N_\chi}(\chi^2, 2s-2) E(z,\chi,s-2) ,$$

where, as before, the subscript N_χ means that the Euler factors at the primes dividing N_χ have been omitted from the Euler product defining the Dirichlet L-series. Recall that $f = \sum_{n=1}^{\infty} a_n q^n$ denotes the primitive cusp form of weight 2 for $\Gamma_0(N)$ which corresponds to E. We omit the proof of the following classical result (see [20], p.83), which is based on the elementary identity

$$D(E,\chi,s) = L_{N_\chi}(\chi^2, 2s-2) \sum_{n=1}^{\infty} \frac{\chi(n) a_{n^2}}{n^s} .$$

Proposition 3.2. We have

$$(3.5) \quad (4\pi)^{-s/2} \Gamma(\tfrac{s}{2}) D(E,\chi,s) = \int_{B(N_\chi)} \overline{f(z)}\, \theta_\chi(z) \Phi(z,\chi,s)\, dxdy ,$$

where $B(N_\chi)$ denotes a fundamental domain for $\Gamma_0(N_\chi)$.

We next give a rather complicated type of Fourier expansion for $\Phi(z,\chi,s)$ (see [22], p.236). The reader must bear with these elaborate formulae as they are the key to all subsequent arguments. Note also that we have slightly modified the result of [22] by applying the duplication formula for the Γ-function. For $n \in \mathbb{Z}$, we define

$$c_\chi(n,s) = \sum_{M \in \mathcal{M}} M^{1/2-s} \left\{ \sum_{j=1}^{M} \left(\frac{M}{j}\right) \chi(j) \varepsilon_j^3 \, e^{\frac{2\pi i n j}{M}} \right\} ,$$

where $\mathcal{M}$ denotes the set of all positive integers which are composed of products of powers of the primes dividing N_χ, and which are also divisible by N_χ itself. For each integer $n \neq 0$, let ρ_n denote

the unique primitive Dirichlet character satisfying

$$(3.6) \qquad \rho_n(d) = \left(\frac{-n}{d}\right)\chi(d) \quad \text{when} \quad (d, nc_\chi) = 1 .$$

Put

$$\beta_\chi(n,s) = \sum_{a,b} \mu(a)\rho_n(a)\chi^2(b)a^{1-s}b^{3-2s} ,$$

where the finite sum is over all positive integers a,b such that $(ab)^2$ divides n and $(ab, N_\chi) = 1$; also μ denotes the Möbius function. As in [22], for $w > 0$ and $\alpha, \beta \in \mathbb{C}$ with $R(\beta) > 0$, define

$$W(w,\alpha,\beta) = \Gamma(\beta)^{-1} \int_0^\infty (u+1)^{\alpha-1}u^{\beta-1}e^{-wu}du .$$

This function has holomorphic continuation over the whole β-plane (see [20]). Our desired expansion for $\Phi(z,\chi,s)$ is given by

$$(3.7) \qquad \Phi(z,\chi,s) = A_0(y,\chi,s) + \sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} A_n(y,\chi,s)e^{2\pi inx} ,$$

where

$$(3.8) \qquad A_0(y,\chi,s) = y^{s/2-1}L_{N_\chi}(\chi^2, 2s-2) + y^{\frac{1-s}{2}}(1+i)\sqrt{\pi}(s-2)\frac{\Gamma(s-\frac{3}{2})}{\Gamma(s)} \times$$

$$\times c_\chi(0,s)L_{N_\chi}(\chi^2, 2s-3) .$$

When $n > 0$, the coefficient $A_n(y,\chi,s)$ is given by

$$(3.9) \qquad A_n(y,\chi,s) = y^{s/2-1}\frac{1+i}{\sqrt{n}}\cdot(4\pi n)^{s-1}e^{-2\pi ny}\frac{\Gamma(\frac{s}{2})}{\Gamma(s)} \times$$

$$\times \beta_\chi(n,s)c_\chi(n,s)L_{N_\chi}(\rho_n, s-1)W(4\pi ny, \frac{s+1}{2}, \frac{s}{2}-1) .$$

When $n < 0$, we have

$$(3.10) \qquad A_n(y,\chi,s) = y^{s/2-1}\frac{1+i}{\sqrt{|n|}}(4\pi|n|)^{s-1}e^{-2\pi|n|y}\frac{\Gamma(\frac{s-1}{2})}{\Gamma(s-2)} \times$$

$$\times \beta_\chi(n,s)c_\chi(n,s)L_{N_\chi}(\rho_n,s-1)W(4\pi|n|y,\tfrac{s}{2}-1,\tfrac{s+1}{2}) \ .$$

We now study two specialisations of these formulae, treating the exceptional case first.

Case 1. Suppose χ is the non-trivial character of a real quadratic field. The specialisation of (3.7) to $s = 2$ in this case is unpleasant, since we will have $A_n(y,\chi,2) \neq 0$ for those $n < 0$ such that ρ_n is the trivial character. On the other hand, the specialisation to $s = 1$ is good, since for $n < 0$, we always have $L_{N_\chi}(\rho_n,0) = 0$ because $\rho_n(-1) = 1$ and $N_\chi > 1$, whence $A_n(y,\chi,1)=0$. As $W(w,1,-\frac{1}{2}) = w^{1/2}$, we obtain that $\Phi(z,\chi,1) = \sum_{n=0}^{\infty} d_n(\chi)q^n$, where

$$d_0(\chi) = 2\pi(1+i)\zeta_{N_\chi}(-1)c(0,1)$$

$$d_n(\chi) = 2\pi(1+i)L_{N_\chi}(\rho_n,0)\beta_\chi(n,1)c_\chi(n,1) \ .$$

Using Lemma 4 of [22], a simple calculation shows that $v_n(\chi)^\sigma = v_n(\chi^\sigma)$ for every automorphism σ of $\mathbb{C}$, where $v_n(\chi) = G(\bar{\chi})\pi^{-1}d_n(\chi)$. On the other hand, (3.5) implies that

$$G(\bar{\chi})\pi^{-1}D(E,\chi,s) = 2\,\langle f(z),\theta_\chi(z)\pi^{-1}G(\bar{\chi})\Phi(z,\chi,1)\rangle_{N_\chi} \ .$$

Hence Lemma 4 of Shimura [21] implies that the conclusion of Theorem 3.1 remains valid in this case, provided we replace the primitive function $\mathcal{D}(E,s)$ by the imprimitive function $D(E,s)$.

Case 2. Suppose now that $\chi^2 \neq \chi_0$, where χ_0 is the trivial character. Thus $\rho_n \neq \chi_0$ for all integers $n \neq 0$. Putting $s = 2$ in the formula (3.10), it follows that $A_n(y,\chi,2) = 0$ for all $n < 0$, because $\Gamma(s-2)$ has a pole and $L_{N_\chi}(\rho_n,s-1)$ is holomorphic at $s = 2$. Since $W(w,\frac{3}{2},0) = 1$, we conclude that $\Phi(z,\chi,2) = \sum_{n=0}^{\infty} e_n(\chi)q^n$, where

$$e_0(\chi) = L_{N_\chi}(\chi^2,2)$$

$$e_n(\chi) = 4\pi\sqrt{n}(1+i)\beta_\chi(n,2)c_\chi(n,2)L_{N_\chi}(\rho_n,1) .$$

Proposition 3.3. For each integer $n \geq 0$, put

$$\gamma_n(\chi) = \pi^{-2}G(\bar{\chi}^2)e_n(\chi) .$$

Then, for every automorphism σ of $\mathbb{C}$, we have $\gamma_n(\chi)^\sigma = \gamma_n(\chi^\sigma)$.

Proof. The assertion for $n = 0$ follows immediately from the functional equation for $L(\chi^2,s)$ and the fact that $L(\bar{\chi}^2,-1)^\sigma = L(\overline{\chi^\sigma}^2,-1)$. Now fix an integer $n > 0$, and let η be a positive integer prime to nN_χ such that $\sigma(\zeta) = \zeta^\eta$ for all nN_χ-th roots of unity ζ. By the Lemma 4 of [22], we have

$$c_\chi(n,2)^\sigma = \varepsilon_\eta^{-3}\,\overline{\chi^\sigma(\eta)}\; c_{\chi^\sigma}(n,2) .$$

Since $\chi_n(-1) = -1$, the functional equation for $L(\rho_n,s)$ implies that

$$L_{N_\chi}(\rho_n,1) = -\frac{i\,G(\rho_n)}{c_{\rho_n}} L(\bar{\rho}_n,0) \prod_{p\mid N_\chi}\left(1-\frac{\rho_n(p)}{p}\right) ,$$

where c_{ρ_n} denotes the conductor of ρ_n. As $L(\bar{\rho}_n,0)^\sigma = L(\overline{\rho_n^\sigma},0)$, a rather tricky calculation shows that

$$\gamma_n(\chi)^\sigma/\gamma_n(\chi) = (\sqrt{n})^{\sigma-1}\left(\frac{n}{\eta}\right) = 1 ,$$

completing the proof of the proposition.

Proposition 3.4. Under the same hypothesis as in Theorem 3.1, we have $\xi(E,\chi)^\sigma = \xi(E,\chi^\sigma)$ for every automorphism σ of $\mathbb{C}$, where

$$\xi(E,\chi) = \frac{G(\bar{\chi}^2)D(E,\chi,2)}{\pi^3\langle f,f\rangle_N} .$$

Proof. Putting $s = 2$ in (3.5), and $\tilde{\xi}(E,\chi) = \dfrac{G(\bar{\chi}^2)D(E,\chi,2)}{\pi^3\langle f,f\rangle_N}$, we find

$$\tilde{\xi}(E,\chi) = \frac{4\langle f,\Omega_\chi(z)\rangle_{N_\chi}}{\langle f,f\rangle_N} ,$$

where $\Omega_\chi(z) = \pi^{-2}G(\bar{\chi}^{-2})\theta_\chi(z)\Phi(z,\chi,2)$. Now $\Omega_\chi(z)$ is a holomorphic modular form of weight 2 and level N_χ , which, by Proposition 3.3, satisfies $\Omega_\chi(z)^\sigma = \Omega_{\chi^\sigma}(z)$. Hence Lemma 4 of Shimura [21] implies that the conclusion of Proposition 3.4 is valid with the value of the imprimitive function $D(E,\chi,2)$ instead of $\mathcal{D}(E,\chi,2)$. But, by (3.2), we have

$$\mathcal{D}(E,\chi,s) = D(E,\chi,s) \prod_{p\in S_1} H_p(\chi(p)p^{-s}) ,$$

where $H_p(X)$ is a polynomial in $\mathbb{Q}[X]$, which, by its explicit form given earlier, clearly does not vanish at $X = \chi(p)p^{-2}$, for any Dirichlet character χ . Hence the conclusion of Proposition 3.4 follows.

We can now complete the proof of Theorem 3.1. Applying the functional equation for $\mathcal{D}(E,\chi,s)$ (Theorem 2.2), and recalling that $\chi(-1)=1$, we obtain

$$\pi^{-1}G(\bar{\chi})\mathcal{D}(E,\chi,1) = \delta(\chi)\pi^{-3}G(\chi^2)\mathcal{D}(E,\bar{\chi},2) ,$$

where

$$\delta(\chi) = 2^{-1}.C^{1/2}c_\chi^3\,\chi(C)(G(\chi^2)G(\bar{\chi})^2)^{-1} .$$

Since it was shown in § 2 that C is the square of an integer, we see that $\delta(\chi)^\sigma = \delta(\chi^\sigma)$ for every automorphism σ of $\mathbb{C}$. Thus Theorem 3.1 follows from Proposition 3.4.

3.2. <u>p-adic interpolation</u>. For each prime p , let $\mathbb{C}_p$ denote the completion of the algebraic closure of the field of p-adic numbers $\mathbb{Q}_p$. Recall that $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. We fix, once and for all, an embedding of $\bar{\mathbb{Q}}$ in $\mathbb{C}_p$ - but, for simplicity, we do not indicate this embedding explicity in our subsequent notation. Our aim in this section is to study the p-adic interpolation of the numbers $\rho(E,\chi)$ when χ varies over all Dirichlet characters of p-power

conductor. Throughout, we impose the following:-

Hypothesis. $p \neq 2$ and E has good ordinary reduction at p.

An equivalent form of this hypothesis is that $p \neq 2$ and the trace of Frobenius a_p of E at p is prime to p. Hence precisely one of the inverse roots of the polynomial

$$(3.11) \quad 1 - a_p X + pX^2 = (1 - \alpha_p X)(1 - \beta_p X)$$

will be a unit at p. From now on, we suppose that α_p is this inverse root which is a unit at p. Recall that a measure μ on $\mathbf{Z}_p^\times$ with values in $\mathbb{C}_p$ is a finitely additive function on the set of open and closed subsets of $\mathbf{Z}_p^\times$ which is bounded (we do not assume that a measure is necessarily integral valued). The following is the main technical result of this section. It does, however, suffer from the defect that it involves the naive symmetric square $D(E,s)$ rather than $\mathcal{D}(E,s)$, and that we are forced to impose the condition that 4 divides the conductor N of E.

Theorem 3.5. Assume $4 \mid N$. Then there exists a unique measure μ_E on $\mathbf{Z}_p^\times$ satisfying (i) $\int_{\mathbf{Z}_p^\times} d\mu_E = 0$, and (ii) for every Dirichlet character χ of p-power conductor $c_\chi = p^{m_\chi}$ with $m_\chi > 0$, we have

$$(3.12) \quad \int_{\mathbf{Z}_p^\times} \chi d\mu_E = \alpha_p^{-2m_\chi} \frac{G(\bar{\chi}) D(E,\chi,1)}{\pi \langle f, f \rangle_N}.$$

Remarks. (i) Recall that a distribution on $\mathbf{Z}_p^\times$ is simply a finitely additive function on the set of open and closed subsets of $\mathbf{Z}_p^\times$. The existence of a distribution on $\mathbf{Z}_p^\times$ satisfying the conditions of Theorem 3.5 is, of course, obvious. The difficulty of the proof lies in showing that this distribution is a measure, i.e. it is bounded. (ii) Theorem 3.5, in a more general form, has been proven independently by Hida (unpublished) by a similar method.

We now begin the proof of Theorem 3.5. Following Hida [10], the first step is to replace the initial form f of level N by a form f_0 of level $N_0=Np$; here f_0 is given explicitely by

$$(3.13)\quad f_0(z) = f(z)-\beta_p f(pz) .$$

The following lemma, whose detailed proof we omit, is an immediate consequence of (3.13) and the fact that $f = \sum_{n=1}^{\infty} a_n q^n$, being primitive of level N , is automatically an eigenform for all Hecke operators of level N . For each prime number λ , let $T(\lambda)$ denote the λ-th Hecke operator of level N_0 .

Lemma 3.6. The form $f_0(z)$ is an eigenform for all Hecke operators of level $N_0 = Np$, which satisfies

$$(3.14)\quad f_0|T(\lambda) = a_\lambda f_0 (\lambda\neq p),\ f_0|T(p) = \alpha_p f_0 .$$

In the following, we denote the Fourier expansion of f_0 by

$$(3.15)\quad f_0 = \sum_{n=1}^{\infty} \alpha_n q^n .$$

By Lemma 3.6, for each prime λ , there exist (possibly 0) complex numbers u_λ, v_λ such that

$$(3.16)\quad \sum_{n=1}^{\infty} \frac{\alpha_n}{n^s} = \prod_{\lambda} (1-u_\lambda \lambda^{-s})^{-1} (1-v_\lambda \lambda^{-s})^{-1} .$$

We define $G(s)$ to be the naive symmetric square of the form f_0 , i.e.

$$(3.17)\quad G(s) = \prod_{\lambda}(1-u_\lambda^2\lambda^{-s})^{-1} (1-v_\lambda^2\lambda^{-s})^{-1} (1-u_\lambda v_\lambda \lambda^{-s})^{-1} .$$

Lemma 3.7. $G(s) = (1-\beta_p^2 p^{-s})(1-p^{1-s})D(E,s)$.

Proof. By definition, $D(E,s)$ is the naive symmetric square of the Euler product of $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$. The assertion of the lemma is then plain, since (3.14) shows that

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = (1-\beta_p p^{-s})^{-1} \sum_{n=1}^{\infty} \frac{\alpha_n}{n^s} .$$

Remarks. Let $G(\chi,s)$ denote the twist of the Dirichlet series $G(s)$ by a Dirichlet character χ. Assume now that χ has p-power conductor. It is plain from Lemma 7 that

$$G(1) = 0,\ G(\chi,1) = D(E,\chi,1) \quad \text{for all} \quad \chi \neq \chi_0 .$$

Thus the integrals in Theorem 3.5 can be expressed more simply in terms of the $G(\chi,1)$.

We next express $G(\chi,s)$ as a Rankin integral similar to (3.5). We suppose from now on that χ ranges only over Dirichlet characters of p-power conductor; also we assume that $\chi(-1) = 1$ since otherwise $G(\chi,1) = 0$. In addition, until further notice, we assume that $\chi \neq \chi_0$. Let h_0 be the form of weight 2 and level N_0 given by

$$(3.18) \quad h_0 = \sum_{n=1}^{\infty} \bar{\alpha}_n q^n .$$

Using the elementary identity

$$G(\chi,s) = L_{N_\chi}(\chi^2,2s-2) \sum_{n=1}^{\infty} \frac{\chi(n)\alpha_{n^2}}{n^s} ,$$

an entirely similar argument to that used in the proof of Proposition 3.2 implies the following expression. Recall that $4|N$.

Proposition 3.8. Assume $\chi \neq \chi_0$. Then

$$(3.19) \quad (4\pi)^{-s/2}\Gamma(\tfrac{s}{2})G(\chi,s) = \int_{B(N_\chi)} \overline{h_0(z)}\ \theta_\chi(z)\Phi(z,\chi,s)\,dxdy .$$

Putting $s = 1$ in this formula, we obtain

$$(3.20) \quad G(\chi,1) = 2\langle h_0, \theta_\chi(z)\Phi(z,\chi,1)\rangle_{N_\chi} .$$

The following crucial result exploits the fact that we work with the form h_0 of level N_0, rather than the original form f. For each integer $M \geq 1$, let $W(M) = \begin{pmatrix} 0 & -1 \\ M & 0 \end{pmatrix}$. Also, we write $T(p)$ for the p-th Hecke operator of level N_χ.

Proposition 3.9. Assume $\chi \neq \chi_0$, and recall that $c_\chi = p^{m_\chi}$. For each integer $m \geq m_\chi$, we have

$$(3.21)\quad G(\chi,1) = 2\alpha_p^{2(m_\chi - m)} \langle h_0 | W(N_0), H_\chi | T(p)^{2m-1} \rangle_{N_0},$$

where $H_\chi = (\theta_\chi(z)\Phi(z,\chi,1))|W(N_\chi)$.

To establish this result, let S_χ denote the trace map from $\Gamma_0(N_\chi)$ to $\Gamma_0(N_0)$ (For forms of weight 2). We always write operators for modular forms on the right, so that $g|A \circ B) = (g|A)|B$.

Lemma 3.10. (i) The adjoint of the p-th Hecke operator $T(p)$ of level N_0 is $W(N_0) \circ T(p) \circ W(N_0)$; (ii). We have

$$S_\chi \circ W(N_0) = W(N_\chi) \circ T(p)^{2m_\chi - 1}.$$

Proof. We omit the proof of (i), which is standard. To prove (ii), if g is a form of weight 2 for $\Gamma_0(N_\chi)$, one verifies immediately that

$$g|S_\chi = \sum_{e \in \mathbf{Z}/p^{2m_\chi - 1}\mathbf{Z}} g|\begin{pmatrix} 1 & 0 \\ N_0 e & 1 \end{pmatrix}.$$

Suppose now that $g|W(N_\chi) = \sum_{n=0}^{\infty} c_n q^n$. In view of the equation

$$\begin{pmatrix} 1 & 0 \\ N_0 e & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ N_0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ N_\chi & 0 \end{pmatrix}\begin{pmatrix} p^{1-2m_\chi} & -ep^{1-2m_\chi} \\ 0 & 1 \end{pmatrix},$$

we conclude that

$$g|S_\chi \circ W(N_0)) = \sum_{e \in \mathbf{Z}/p^{2m_\chi - 1}\mathbf{Z}} (g|W(N_\chi))|\begin{pmatrix} 1 & -e \\ 0 & p^{2m_\chi - 1} \end{pmatrix} = \sum_{n=0}^{\infty} c_{np^{2m_\chi - 1}} q^n,$$

and the expression on the right is plainly the Fourier development of the image under $T(p)^{2m_\chi - 1}$ of $g|W(N_\chi)$, thereby completing the proof of part (ii) of the lemma.

Returning to the proof of Proposition 3.9, we conclude from (3.20) and the fact that h_0 is of level N_0 that

$$G(\chi,1)=2\langle h_0,(\theta_\chi(z)\Phi(z,\chi,1))\,|\,S_\chi\rangle_{N_0}=2\langle h_0\,|\,W(N_0),(\theta_\chi(z)\Phi(z,\chi,1))\,|\,S_\chi\circ W(N_0)\rangle_{N_0}$$

Applying (ii) of Lemma 3.10, it follows that

$$G(\chi,1)=2\,\langle h_0\,|\,W(N_0),H_\chi\,|\,T(p)^{2m_\chi-1}\rangle_{N_0}\ .$$

As h_0 is an eigenvector for $T(p)$ with eigenvalue β_p, this last formula can be rewritten as

$$G(\chi,1)=2\alpha_p^{-2(m-m_\chi)}\langle h_0\,|\,T(p)^{2(m-m_\chi)}\circ W(N_0)),H_\chi\,|\,T(p)^{2m_\chi-1}\rangle_{N_0}\ .$$

Since $W(N_0)^2=1$, we conclude from (ii) of Lemma 3.10 that

$$G(\chi,1)=2\alpha_p^{2(m_\chi-m)}\langle h_0\,|\,W(N_0),H_\chi\,|\,T(p)^{2m-1}\rangle_{N_0}\ .$$

This completes the proof of Proposition 3.9.

For each integer $m\geq 1$, let Δ_m denote the set consisting of all Dirichlet characters of conductor dividing p^m, which are distinct from the trivial character χ_0. Let e be any integer prime to p. Writing μ_E for the unique distribution on $\mathbf{Z}_p^\times$ satisfying (i) and (ii) of Theorem 3.5, it is plain that

$$\mu_E(e+p^m\mathbf{Z}_p)=\frac{1}{\varphi(p^m)}\sum_{\chi\in\Delta_m}\chi^{-1}(e)\alpha_p^{-2m_\chi}\frac{G(\chi^{-1})G(\chi,1)}{\pi\langle f,f\rangle_N}\ ,$$

where φ denotes Euler's function. To prove Theorem 3.5, we must show that $\mu_E(e+p^m\mathbf{Z}_p)$ remains p-adically bounded as e ranges over all integers prime to p and $m\longrightarrow\infty$. The key fact, underlying the proof of Theorem 3.5, is that (3.21) enables us to simplify the term $\alpha_p^{-2m_\chi}$ in the above expression for $\mu_E(e+p^m\mathbf{Z}_p)$. Explicitly, (3.21) gives

$$(3.22)\qquad \mu_E(e+p^m\mathbf{Z}_p)=2\alpha_p^{-2m}\langle h_0\,|\,W(N_0),R_m\,|\,T(p)^{2m-1}\rangle_{N_0}/\langle f,f\rangle_N\ .$$

where

$$(3.23)\qquad R_m=\frac{1}{\varphi(p^m)}\sum_{\chi\in\Delta_m}\chi^{-1}(e)\frac{G(\chi^{-1})}{\pi}H_\chi\ ,$$

and, as in Proposition 3.9, $H_\chi = (\theta_\chi(z)\Phi(z,\chi,1))\,|\,W(N_\chi)$. Note the remarkable fact that R_m is independent of the elliptic curve E .

As will be explained later, the following result on the Fourier development of the form R_m yields almost immediately Theorem 3.5.

Theorem 3.11. Let $R_m = \sum_{n=1}^{\infty} r_n(m) q^n$. Then the Fourier coefficients $r_n(m)$ belong to $\mathbb{Q}$ for all integers $n \geq 1$. Moreover, $r_n(m)$ is p-integral whenever p^{2m-1} divides n .

We immediately give the proof of Theorem 3.11. Assuming that $\chi \neq \chi_0$, we define as in [20]

$$E^*(z,\chi,s) = E(-\frac{1}{N_\chi z},\chi,s)(-izc_\chi N^{1/2})^{-3/2} .$$

Now it is well known (see [19], p.457) that

$$\theta_\chi(-\frac{1}{N_\chi z}) = p^{-m_\chi/2} G(\chi)(-p^{m_\chi}\frac{iNz}{2})^{1/2}\theta_{\bar{\chi}}(N'z) ,$$

where $N' = N/4$. It follows that the form H_χ is given by

$$(3.24)\quad H_\chi(z) = -J(z,\chi,1)p^{-m_\chi}G(\chi)\theta_{\bar{\chi}}(N'z) ,$$

where

$$J(z,\chi,s) = \frac{N_\chi^{1/4}}{\sqrt{2}} L_{N_\chi}(\chi^2,2s-2)E^*(z,\chi,s-2) .$$

Using the expansion of $E^*(z,\chi,s)$ given in [20], we deduce immediately the following analogue of (3.7)

$$(3.25)\quad J(z,\chi,s) = B_0(y,\chi,s) + \sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} B_n(y,\chi,s)e^{2\pi i n x} ,$$

where

$$B_0(y,\chi,s) = L_{N_\chi}(\chi^2,2s-3)N_\chi^{-(\frac{s-1}{2})} y^{-(\frac{s-1}{2})} \pi^{1/2}\frac{\Gamma(s-\frac{3}{2})}{(s-1)\Gamma(s-2)} .$$

To give the explicit expression for $B_n(y,\chi,s)$ when $n \neq 0$, we need

some slightly different notation from that used in § 3.1. Firstly, the function $W(\omega,\alpha,\beta)$ will be the same as defined in § 3.1. However, we now write χ_n for the primitive Dirichlet character satisfying

$$\chi_n(x) = \left(\frac{-nN}{x}\right)\chi(x) \quad \text{when} \quad (x,nNp) = 1 .$$

Moreover, we put

$$\alpha_\chi(n,s) = \Big(\sum_{a,b} \mu(a)\chi_n(a)\chi^2(b)a^{1-s}b^{3-2s}\Big) L_{N_\chi}(\chi_n,s-1) ,$$

where the sum is taken over all positive integers a,b such that $(ab)^2$ divides n, and $(ab,Np)=1$. If $n > 0$, we then have

$$B_n(y,\chi,s) = y^{s/2-1} N_\chi^{-(\frac{s-1}{2})} 2^{s-1} n^{s-3/2} \pi^{s-\frac{1}{2}} \Gamma\left(\tfrac{s+1}{2}\right)^{-1} \alpha_\chi(n,s) W\left(4\pi ny, \tfrac{s+1}{2}, \tfrac{s}{2}-1\right) e^{-2\pi ny} ,$$

and, for $n < 0$, we have

$$B_n(y,\chi,s) = y^{s/2-1} N_\chi^{-(\frac{s-1}{2})} 2^{s-1} |n|^{s-\frac{3}{2}} \pi^{s-\frac{1}{2}} \Gamma\left(\tfrac{s}{2}-1\right)^{-1} \alpha_\chi(n,s) W\left(4\pi|n|y, \tfrac{s}{2}-1, \tfrac{s+1}{2}\right) e^{-2\pi|n|y} .$$

We must put $s=1$ in these formulae to obtain the Fourier development of $J(z,\chi,1)$. As $\chi(-1)=1$, we have $\chi_n(-1)=1$ when $n < 0$, whence $L_{N_\chi}(\chi_n,0)=0$, and this in turn implies that $B_n(y,\chi,1)=0$ when $n < 0$. Since $W(w,1,-\frac{1}{2}) = \sqrt{w}$ for $w > 0$, a simple direct calculation shows that

$$(3.26) \quad J(z,\chi,1) = 2\pi \left\{ L_{N_\chi}(\chi^2,-1) + \sum_{n=1}^{\infty} q^n t_n(\chi) \right\} ,$$

where

$$(3.27) \quad t_n(\chi) = L_{N_\chi}(\chi_n,0) \sum_{a,b} \mu(a)\chi_n(a)\chi^2(b)b .$$

In view of the explicit expressions (3.23), (3.24), (3.26) and (3.27), it is plain that the $r_n(m)$ belong to $\mathbb{Q}$ for all $n \geq 1$.

We suppose from now until the end of the proof of Theorem 3.11 that n denotes an integer ≥ 1 satisfying

$$(3.28) \quad p^{2m-1} \text{ divides } n .$$

The delicate part of the proof is to show that the Fourier coefficient $r_n(m)$ is p-integral. Put

$$\lambda_m = -2/\varphi(p^m) .$$

Now (3.23), (3.24) and (3.26) show that $r_n(m)$ is given explicitly by

$$r_n(m) = \lambda_m \sum_{(n_1,n_2)\in W_n} \sum_{(a,b)\in V_{n_2}} \sum_{\chi\in\Delta_m} \mu(a) b \chi^2(b) \chi^{-1}(n_1 e) \chi_{n_2}(a) L_{N_\chi}(\chi_{n_2},0) ;$$

here W_n denotes the set of pairs (n_1,n_2) of positive integers, which are relatively prime to p, and which satisfy

(3.29) $\quad n_1^2 N' + n_2 = n$, where $N' = N/4$;

also V_{n_2} denotes the set of pairs (a,b) of positive integers, which are relatively prime to Np, and which satisfy $(ab)^2$ divides n_2. By definition, we have

$$\chi_{n_2} = \chi \cdot \varepsilon_{n_2} ,$$

where ε_{n_2} is the character of the imaginary quadratic field $\mathbb{Q}(\sqrt{-n_2 N})$. Note that ε_{n_2} has conductor prime to p, because $(p,n_2 N) = 1$ and $p \neq 2$. Hence the above expression can be rewritten as

$$r_n(m) = \lambda_m \sum_{\chi\in\Delta_m} \sum_{(n_1,n_2)\in W_n} \sum_{(a,b)\in V_{n_2}} \mu(a) b \varepsilon_{n_2}(a) \chi(b^2 a) \chi^{-1}(n_1 e) L_N(\chi\varepsilon_{n_2},0) .$$

We now make use of p-adic L-functions to study the integrality at p of this last expression. If ρ is a Dirichlet character with $\rho(-1) = 1$, we write $L_p(\rho,s)$ for the Leopoldt-Kubota p-adic L-function of ρ. If $\rho(-1) = -1$, put $L_p(\rho,s) \equiv 0$. Let ω denote the unique character modulo p satisfying $\omega(x) \equiv x \bmod p$. It is well known that

$$L_p(\rho,0) = (1-\rho\omega^{-1}(p)) L(\rho\omega^{-1},0) .$$

First take $\rho = \chi\varepsilon_{n_2}\omega$, with $\chi \in \Delta_m$. Then p necessarily divides the

conductor of $\rho\omega^{-1} = \chi\varepsilon_{n_2}$ since $\chi \neq \chi_0$, and so

$$L_p(\chi\varepsilon_{n_2}\omega,0) = L(\chi\varepsilon_{n_2},0) \quad \text{for} \quad \chi \in \Delta_m .$$

Now suppose that $\rho = \chi_0\varepsilon_{n_2}\omega$, with the trivial character χ_0. Here the conductor of $\rho\omega^{-1} = \varepsilon_{n_2}$ is prime to p. Moreover, multiplying both sides of (3.29) by N, and recalling that $m \geq 1$ and p^{2m-1} divides n, we see immediately that

$$\varepsilon_{n_2}(p) = \left(\frac{-n_2N}{p}\right) = 1 ,$$

whence $L_p(\chi_0\varepsilon_{n_2}\omega,0) = 0$. Now let C_m denote the set of all character of conductor dividing p^m, i.e. $C_m = \Delta_m \cup \{\chi_0\}$. Note that, for all $\chi \in C_m$, we have

$$\prod_{r|N}(1-\chi\varepsilon_{n_2}(r)) = \sum_{d|N}\mu(d)\chi\varepsilon_{n_2}(d) ,$$

where r runs over the primes dividing N, and d runs over the positive divisors of N. Finally, let n_1^* denote the multiplicative inverse of n_1e modulo p^m. Putting all these facts together, we see that the expression for $r_n(m)$ given at the end of the previous paragraph can be rewritten as

$$r_n(m) = \lambda_m \sum_{(n_1,n_2)\in W_n} \sum_{(a,b)\in V_{n_2}} \sum_{d|N} \mu(ad)\varepsilon_{n_2}(ad)bM_m(ab^2dn_1^*) ,$$

where, for any integer x prime to p, we have

$$(3.30) \quad M_m(x) = \sum_{\chi\in C_m} \chi(x)L_p(\chi\varepsilon_{n_2}\omega,0) .$$

Recalling that $\lambda_m = -2/\varphi(p^m)$, we see that the proof of Theorem 3.11 will be complete once the following lemma is established.

Lemma 3.12. *For each integer* x *prime to* p, *we have* $M_m(x) \equiv 0 \bmod p^{m-1}$.

In fact, Lemma 3.12 is a well known integrality and holomorphy state-

ment about the Kubota-Leopoldt p-adic L-functions, whose proof we do not give here, but simply recall two more familiar formulations of it. The first is the assertion that there exists a measure ρ on $\mathbf{Z}_p^\times$, with values in $\mathbf{Z}_p$, satisfying

$$\int_{\mathbf{Z}_p^\times} \chi d\rho = L_p(\chi\varepsilon_{n_2}\omega,0)$$

for all characters χ of p-power conductor (such a measure exists because $\chi\varepsilon_{n_2}\omega$ can never be a character of the cyclotomic $\mathbf{Z}_p$-extension of $\mathbb{Q}$, since ε_{n_2} is non-trivial, and has conductor prime to p). The second formulation is that, for each integer i modulo $p-1$, there exists a formal power series $B_i(T)$ in $\mathbf{Z}_p[[T]]$ such that

$$B_i(\chi(\gamma)-1) = L_p(\chi\varepsilon_{n_2}\omega,0) ,$$

for all characters χ of p-power conductor such that $\chi|\mu_{p-1}=\omega^i$, here γ denotes a topological generator of $1 + p\mathbf{Z}_p$, and μ_{p-1} denotes the group of $(p-1)$-st roots of unity in $\mathbf{Z}_p^\times$.

We can now complete the proof of Theorem 3.5. Let $F = \mathbb{Q}(\alpha_p)$, and let $M(N_0)$ denote the vector space over F of all holomorphic modular forms of weight 2 for $\Gamma_0(N_0)$, whose Fourier coefficients belong to the field F. As in § 4 of [10], we can define an F-linear form

$$\ell_f : M(N_0) \longrightarrow F$$

by the formula

$$\ell_f(g) = \frac{\langle h_0|W(N_0),g\rangle_{N_0}}{\langle h_0|W(N_0),f_0\rangle_{N_0}} .$$

Let $\varepsilon(f) = \pm 1$ be defined by $f|W(N) = \varepsilon(f)f$. A simple direct calculation shows that

$$\langle h_0|W(N_0),f_0\rangle_{N_0} = \varepsilon(f)\alpha_p(1-\alpha_p^{-2})(1-p\alpha_p^{-2})\langle f,f\rangle_N .$$

Hence it follows from (3.22) that

$$\mu_E(e+p^m\mathbf{Z}_p) = 2\alpha_p^{1-2m}\varepsilon(f)(1-\alpha_p^{-2})(1-p\alpha_p^{-2})\ell_f(R_m|T(p)^{2m-1}) .$$

Since α_p is a p-adic unit, the proof of Theorem 3.5 is completed by the following argument. Let $J(N_0)$ denote the $\mathbf{Z}$-module of all modular forms of weight 2 for $\Gamma_0(N_0)$, whose Fourier coefficients belong to $\mathbb{Q}$ and are p-integral. By Theorem 3.11, the modular form $R_m|T(p)^{2m-1}$ belongs to $J(N_0)$. We claim that ℓ_f is p-adically bounded on $J(N_0)$ This is because $J(N_0) \otimes \mathbf{Z}_p$ is well known to be a finitely generated $\mathbf{Z}_p$-module, and we can clearly extend ℓ_f by F-linarity to an F-valued linear form on $M(N_0) \otimes_F F$; here F denotes the completion of F with respect to the p-adic valuation. This finishes the proof of Theorem 3.5

Even though we have been unable to prove it, we conjecture that the following stronger form of Theorem 3.5 holds. As always, we assume that $p \neq 2$ and that E has good ordinary reduction at p.

Conjecture 3.13. For each modular elliptic curve E defined over $\mathbb{Q}$, there exists a unique measure τ_E on $\mathbf{Z}_p^\times$ satisfying:-

(i) $\int_{\mathbf{Z}_p^\times} d\tau_E = 0$;

(ii) for every Dirichlet character χ of p-power conductor $c_\chi = p^{m_\chi}$, with $m_\chi > 0$, we have

$$\int_{\mathbf{Z}_p^\times} \chi d\tau_E = \alpha_p^{-2m_\chi} \frac{G(\bar{\chi})D(E,\chi,1)}{\pi\langle f,f\rangle_N} .$$

Here we are tacitly assuming the truth of the algebraicity statement of Theorem 3.1 when χ is a non-trivial real quadratic character.

We now reformulate Theorem 3.5 so as to give a weak form of Conjecture 3.13. Suppose for the rest of this section that E is an arbitrary modular elliptic curve (in particular, we now drop the assumption that 4 divides the conductor N of E). We define J to

be the following finite set of primes consisting of 2 and all primes r such that E has potential good reduction at r and the group Φ_r of § 1 is cyclic of order > 2. Define

$$\mathcal{D}_J(E,s) = \prod_{r \notin J} \mathcal{D}_r(r^{-s})^{-1} ,$$

so that $\mathcal{D}_J(E,s)$ is simply obtained from $\mathcal{D}(E,s)$ by suppressing the Euler factors at the primes in J.

Theorem 3.14. *There exists a unique measure* ϕ_E *on* $\mathbf{Z}_p^\times$ *satisfying:-*

(i) $\int_{\mathbf{Z}_p^\times} d\phi_E = 0$;

(ii) *for every Dirichlet character* χ *of p-power conductor* $c_\chi = p^{m_\chi}$, *with* $m_\chi > 0$, *we have*

$$\int_{\mathbf{Z}_p^\times} \chi d\phi_E = \alpha_p^{-2m_\chi} \frac{G(\bar{\chi}) \mathcal{D}_J(E,\chi,1)}{\pi \langle f,f \rangle_N} .$$

Proof. Let E_1 be a twist of E by a quadratic character such that (i) E_1 has split multiplicative reduction at all primes r such that $\mathrm{ord}_r(j_E) < 0$, and (ii) E_1 has the group Φ_r of § 1 of order > 2 at all primes r of potential good reduction. Such a quadratic twist E_1 is easily seen to exist. We cannot apply Theorem 3.5 directly to E_1, as we do not know a priori that 4 divides the conductor N_1 of E_1. Let E_2 be E_1 if $4 | N_1$, and otherwise let E_2 be the twist of E_1 by the quadratic character of conductor 4. We claim that

$$D(E_2,s) = \mathcal{D}_J(E,s) . \tag{3.31}$$

This is plain from the following two observations. Firstly, we have

$$D(E_2,s) = D(E_1,s)\ U(s) ,$$

where

$$U(s)=1,\ 1-2^{-s}\ ,\ \text{or}\ (1-2^{1-s})(1-\alpha_2^2 2^{-s})(1-\beta_2^2 2^{-s})\ ,$$

according as $4|N_1$, 2 divides N_1 exactly, or $(2,N_1) = 1$. Secondly, we have

$$\mathcal{D}(E,s)=\mathcal{D}(E_1,s)=D(E_1,s) \times \prod_{r\in J_1} \mathcal{D}_r(r^{-s})^{-1}\ ,$$

where J_1 consists of all primes r in J (including possibly $r = 2$ such that E has potential good reduction at r and the group Φ_r o § 1 is cyclic of order > 2 . Noting that

$$\alpha_p(E)^2 = \alpha_p(E_2)^2\ ,$$

Theorem 3.14 follows from applying Theorem 3.5 to the curve E_2.

To finish this section, we give the reformulation of these result in terms of the Iwasawa algebra of $\Gamma = G(\mathbb{Q}_\infty/\mathbb{Q})$, where $\mathbb{Q}_\infty$ denotes the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We follow the notation at the beginning of the paper. Thus

$$\Delta = G(\mathbb{Q}(\mu_p)/\mathbb{Q})\ ,\ \Theta = \Gamma \times \Delta = G(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})\ ,$$

and we identify Θ with $\mathbb{Z}_p^\times$ via the action of Θ on μ_{p^∞} . Fix a topological generator γ of Γ . As usual, we then identify the $\mathbb{Z}_p$-Iwasawa algebra Λ of Γ with

$$\Lambda = \mathbb{Z}_p[[T]]\ ,$$

the ring of formal power series in T with coefficients in $\mathbb{Z}_p$. Here is an equivalent form of Conjecture 3.13 in terms of the Iwasawa algeb

Conjecture 3.13. (second form). For each character ψ of Δ , there exists $\delta_\psi \neq 0$ in $\mathbb{Z}_p$ and $G_\psi(T) \in \Lambda$ satisfying:-

(i) $G_{\psi_0}(0) = 0$ when ψ_0 is the trivial character of Δ ;

(ii) for every character χ of finite order of Θ , with $c_\chi = p^{m_\chi}$ and $m_\chi > 0$, such that $\chi|\Delta = \psi$, we have

$$(3.32)\quad G_\psi(\chi(\gamma)-1) = \delta_\psi \alpha_p^{-2m_\chi} \frac{G(\bar{\chi})\mathcal{D}(E,\chi,1)}{\pi\langle f,f\rangle_N} .$$

Remarks.

(i) If $\psi(-1) = -1$, Remark (ii) after Theorem 3.1 shows that $G_\psi(T) \equiv 0$.

(ii) We will show in § 5 that Conjecture 3.13 is true when E admits complex multiplication.

(iii) Conjecture 3.13 is also true when N is even and square free, since this hypothesis implies that $\mathcal{D}(E,s) = D(E,s)$, and that the Euler factor at 2 of these functions is $1-2^{-s}$, which is a p-adic unit at $s = 1$.

(iv) The zero of $G_{\psi_0}(T)$ at $T = 0$ should be seen as arising because the p-Euler factor of $\mathcal{D}(E,s)$, namely

$$(1-p^{1-s})(1-\alpha_p^2 p^{-s})(1-\beta_p^2 p^{-s}) ,$$

vanishes at $s = 1$.

Finally, we point out that Theorem 3.14 yields a weak form in general of the above conjecture. Put

$$V(s) = \prod_{r\in J} \mathcal{D}_r(r^{-s}) .$$

It is clear from the explicit form of the Euler factors at the primes in J that, for each character ψ of Δ , there exists $H_\psi(T) \in \Lambda$ as follows. For every character χ of finite order of Θ with $\chi|\Delta = \psi$, we have

$$H_\psi(\chi(\gamma)-1) = V(\chi,1) .$$

Then Theorem 3.14 shows that there exists $G_\psi(T)$ in the quotient field of Λ such that $H_\psi(T)G_\psi(T) \in \Lambda$ and

$$G_{\psi}(\chi(\gamma)-1) = \alpha_p^{-2m_\chi} \frac{G(\bar{\chi})\mathcal{D}(E,\chi,1)}{\pi\langle f,f\rangle_N}$$

for all characters χ of finite order of Θ with $\chi|\Delta=\psi$, except for the finitely many characters χ satisfying either $V(\chi,1)=0$ or χ is real quadratic.

§ 4. The Main Conjecture

Our aim in this section is to define a natural Iwasawa module for the Galois group $\Theta = G(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ attached to the ℓ-adic representation $\Sigma_\ell(E)$ given by (1.1), where p is an odd prime such that E has good ordinary reduction at p. The definition of this Iwasawa module has been motivated by an analogous description of the classical Selmer group of E over $\mathbb{Q}(\mu_{p^\infty})$ (see [6] for a detailed discussion of these questions for the Selmer group). We formulate a Main Conjecture for the even eigenspaces of this module under the action of $\Delta = G(\mathbb{Q}(\mu_p)/\mathbb{Q})$, as well as a conjecture for the Λ-rank of the odd eigenspaces.

4.1. Definition of the Iwasawa module. The ℓ-adic representation $\mathrm{Sym}^2(V_\ell(E))$ is endowed with a natural lattice $\mathrm{Sym}^2(T_\ell(E))$, and we define

$$W_\ell = \mathrm{Sym}^2(V_\ell(E))/\mathrm{Sym}^2(T_\ell(E)) .$$

An alternative description of W_ℓ is given by

$$W_\ell = \varinjlim_n \mathrm{Sym}^2(E_{\ell^n}) ,$$

where the inductive limit is taken relative to the homomorphisms induced by the inclusions $E_{\ell^n} \hookrightarrow E_{\ell^{n+1}}$.

Let v denote a place of $\bar{\mathbb{Q}}$ above p, and write $\tilde{E}_v$ for the reduction of E modulo v. Put

$$\tilde{W}_v = \varinjlim_n \mathrm{Sym}^2(\tilde{E}_{v,p^n}) .$$

The homomorphism of reduction modulo v on points clearly induces a surjection $r_v : W_p \longrightarrow \tilde{W}_v$. The kernel of this homomorphism will play a basic role in the following, and we denote it by $W^0_{p,v}$. Thus we have the exact sequence

$$(4.1)\quad 0 \longrightarrow W_{p,v}^{0} \longrightarrow W_p \xrightarrow{r_v} \tilde{W}_v \longrightarrow 0 \ .$$

Our hypothesis that E has ordinary reduction at p implies that $W_{p,v}^{0}$ is isomorphic as an abelian group to $(\mathbb{Q}_p/\mathbb{Z}_p)^2$.

Let $Q_\infty = \mathbb{Q}(\mu_{p^\infty})$, and write p for the unique place of Q_∞ above p . Write $Q_{\infty,p}$ for the union of the completions at p of all finite extensions of $\mathbb{Q}$ contained in Q_∞ . Similarly, picking a place v of $\bar{\mathbb{Q}}$ above p , we denote by $\bar{\mathbb{Q}}_v$ the union of the completions at v of all finite extensions of $\mathbb{Q}$ contained in $\bar{\mathbb{Q}}$. We identify $Q_{\infty,p}$ with a subfield of $\bar{\mathbb{Q}}_v$. Let $J_{\infty,v}$ denote the inertia subgroup of $G(\bar{\mathbb{Q}}_v/Q_{\infty,p})$. We now define

$$H(Q_{\infty,p},\ W_p)$$

to be the subgroup of $H^1(Q_{\infty,p},\ W_p)$ consisting of all cohomology classes which admit a representative cocycle δ satisfying

$$(4.2)\quad \delta(\sigma) \in W_{p,v}^{0} \quad \text{for all} \quad \sigma \in J_{\infty,v} \ .$$

One verifies easily that this subgroup $H(Q_{\infty,p},\ W_p)$ depends only on p (or p) , and not on the choice of the particular place v of $\bar{\mathbb{Q}}$ above p .

We can now define the Iwasawa module $S(\Sigma)$ which seems to us to be the natural one attached to Θ and the ℓ-adic representation (1.1) For each finite place w of Q_∞ , write $Q_{\infty,w}$ for the union of the completions at w of all finite extensions of $\mathbb{Q}$ contained in Q_∞ . Write j_w for the restriction map

$$j_w : H^1(Q_\infty, W_p) \longrightarrow H^1(Q_{\infty,w}, W_p) \ .$$

Key Definition. $S(\Sigma)$ is the subgroup of $H^1(Q_\infty, W_p)$ consisting of all cohomology classes α such that $j_w\alpha = 0$ for all finite places w not dividing p , and $j_p\alpha \in H(Q_{\infty,p}, W_p)$.

Remarks. (i). We originally had in mind a somewhat different

definition of the Iwasawa module attached to Σ_ℓ, and it was only after much prodding from Greenberg that we realized that the above definition seems to be the natural one. (ii). One motivation for the above definition is that, if one replaces W_p by E_{p^∞} in it, one obtains precisely the classical Selmer group of E over Q_∞ (see [6]).

We now turn to the study of the Iwasawa module $S(\Sigma)$. In fact, it is more convenient to work with its compact dual

$$(4.3)\quad Z(\Sigma) = \mathrm{Hom}(S(\Sigma), \mathbb{Q}_p/\mathbb{Z}_p) .$$

Although it does not seem worth going into details here, it is not difficult to prove that $Z(\Sigma)$ is a finitely generated module over the Iwasawa algebra Λ. The first deep question about $Z(\Sigma)$ is to predict conjecturally the Λ-rank of the various eigenspaces of $Z(\Sigma)$ under the action of $\Delta = G(\mathbb{Q}(\mu_p)/\mathbb{Q})$. For each character ψ of Δ, write

$$Z_\psi(\Sigma) = \text{eigenspace of } Z(\Sigma) \text{ on which } \Delta \text{ acts via } \psi .$$

Miraculously, the Λ-rank of $Z_\psi(\Sigma)$ appears to be predicted by the Γ-factor in the functional equation for the complex L-series $\mathcal{D}(E,\psi,s)$. By (2.4) and Theorem 2.2, this Γ-factor is given explicitly by

$$\Gamma(\mathcal{D},\psi,s) = (2\pi)^{-s}\Gamma(s)\pi^{-(\frac{s-i_\psi}{2})}\Gamma(\tfrac{s-i_\psi}{2}) ,$$

where $i_\psi = 0$ or 1 according as $\psi(-1) = 1$ or $\psi(-1) = -1$.

Conjecture 4.1. For each character ψ of Δ, the Λ-rank of $Z_\psi(\Sigma)$ is equal to the order of the pole of $\Gamma(\mathcal{D},\psi,s)$ at $s = 1$. In other words, the Λ-rank of $Z_\psi(\Sigma)$ should be 0 or 1, according as $\psi(-1) = 1$ or $\psi(-1) = -1$.

In § 5, we shall show that, when $\psi(-1) = -1$, the Λ-rank of $Z_\psi(\Sigma)$ is at least 1 if E admits complex multiplication. We shall also verify

that, in the complex multiplication case, the two variable Main Conjecture (see [5]) implies Conjecture 4.1.

Recall that, if A is a finitely generated torsion Λ-module, it is pseudo-isomorphic to a Λ-module of the form

$$\Lambda/(f_1) \oplus \ldots\ldots \oplus \Lambda/(f_r) ,$$

where $f_1,\ldots,f_r$ are non-zero elements of Λ. We call $f = f_1 \ldots f_r$ the characteristic power series of A. It is uniquely determined up to multiplication by a unit of Λ. A key question is that of predicting the characteristic power series of $Z_\psi(\Sigma)$ when ψ is a character of Δ with $\psi(-1) = 1$.

Main Conjecture 4.2. Let ψ be a character of Δ with $\psi(-1)=1$. Assume that Conjecture 3.13 and 4.1 are valid for ψ. Then there exists $v_\psi \neq 0$ in $\mathbb{Q}_p$ such that the p-adic L-function $v_\psi G_\psi(T)$ is a characteristic power series of $Z_\psi(\Sigma)$.

Remark. Presumably there is a natural choice of the constant δ_ψ of Conjecture 3.13, which would allow us to take the constant u_ψ of Conjecture 4.2 equal to 1. However, we must leave this question open at present.

Needless to say, Conjecture 4.2 is deep, and its proof is probably a long way off. In the case when E has complex multiplication, we shall show in § 5 that Conjecture 4.2 is a consequence of the two variable Main Conjecture.

Perhaps the most striking immediate consequence of Conjecture 4.2 occurs when ψ is the trivial character ψ_0 of Δ. Then, assuming the p-adic L-function $G_{\psi_0}(T)$ exists, it vanishes at $T = 0$ by (i) of Conjecture 3.13. Combining this with Conjecture 4.2, we obtain the following assertion.

Corollary of Conjecture 4.2. The group

$S(\Sigma)^{\theta}$, where $\theta = G(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$

always contains a copy of $\mathbb{Q}_p/\mathbb{Z}_p$.

We recall that, as is assumed throughout this section, p here is any odd prime such that E has good ordinary reduction at p . It would be very interesting to find a proof of this corollary in general. In the case when E has complex multiplication, we shall give a proof of the corollary in § 5.

§ 5. The CM case

The Iwasawa theory of elliptic curves E over $\mathbb{Q}$ with complex multiplication is, at least conjecturally, well understood (see [5]). The aim of this section is to verify that, in the complex multiplicatio case, the conjectures given in § 4 are indeed consequences of the two variable Main Conjecture of [5] and classical cyclotomic Iwasawa theory.

We assume throughout this section that the elliptic curve $E/\mathbb{Q}$ has complex multiplication by the maximal order $\mathcal{O}$ of an imaginary quadratic field K. Our hypothesis that E has good ordinary reductio at p is well-known to be equivalent to the assertion that E has good reduction at p and p splits in K. We suppose always that this is the case and that $p > 2$. Write $p = pp^*$ for the factorization of p in K. Let ε denote the Dirichlet character of the quadratic extension $K/\mathbb{Q}$. Finally, we write ϕ for the Größencharakter of the elliptic curve E/K in the sense of Deuring. Thus the Hasse-Weil L-series of E over $\mathbb{Q}$ coincides with the Hecke L-function $L(\phi,s)$. Let ϕ^2 denote the primitive Größencharakter attached to the square of ϕ.

Proposition 5.1. The L-function of the primitive symmetric square $\mathcal{D}(E,s)$ decomposes into the product of the two L-functions attached to ϕ^2 and ε in the form

$$\mathcal{D}(E,s) = L(\phi^2,s) \cdot L(\varepsilon,s-1) .$$

Proof. We give a proof by comparing Euler factors. For the primes where E has good reduction this can easily be done using the fact that $\phi(\bar{a}) = \overline{\phi(a)}$ for any ideal a in $\mathcal{O}$ where ϕ is defined. The comparison at primes of bad reduction being rather elaborate, we shall shorten the argument by using the fact that E is in particular a

modular elliptic curve. Thus we do know that $\mathcal{D}(E,s)$ satisfies a functional equation for $s \longrightarrow 3-s$, as well as the product of L-series on the right hand side of the decomposition formula above. By Lemma 1.4 for any prime r of bad reduction we have

$$\mathcal{D}_r(X) = 1-u_r rX,\ u_r = 0,1,-1,$$

since in the CM-case E has potential good reduction everywhere. So we find

$$\mathcal{D}(E,s)\cdot L(\phi^2,s)^{-1}\cdot L(\varepsilon,s-1)^{-1} = \prod_{r|N} (1-v_r r^{1-s})/(1-u_r r^{1-s})$$

where u_r, v_r are $0,1$ or -1. If the right hand side in this equation is not equal to 1, then it has a zero or a pole on the line $\mathrm{Re}(s)=1$. By the functional equation satisfied by all occuring L-functions, the finite Euler product under consideration would also have a zero or a pole on the line $\mathrm{Re}(s)=2$, which is obviously impossible. This proves the proposition.

As an easy consequence of Proposition 5.1 we get the decomposition formula of the twisted L-functions for any Dirichlet character χ of conductor c_χ prime to the conductor N of E. Recall that in the CM case $N = c_\varepsilon \cdot N_{K/\mathbb{Q}}(c_\phi)$, where c_ϕ denotes the conductor of the Größencharakter ϕ. Let $\chi_K = \chi \circ N_{K/\mathbb{Q}}$ denote the composition of the norm map of $K/\mathbb{Q}$ with the Dirichlet character χ.

Remark 5.2. If $(c_\chi, N)=1$ then we have

$$\mathcal{D}(E,\chi,s) = L(\phi^2\chi_K, s) \cdot L(\varepsilon\chi, s-1).$$

We now turn to the p-adic theory. As in § 4 let $Q_\infty = \mathbb{Q}(\mu_{p^\infty})$ and write $F_\infty = \mathbb{Q}(E_{p^\infty})$ and $K_\infty = K(\mu_{p^\infty})$.

Lemma 5.3. The field of complex multiplication K is a subfield of the field of p-division points $\mathbb{Q}(E_p)$.

Proof. If the lemma were not true, we had $K \cap F_\infty = \mathbb{Q}$. Since $K(E_{p^\infty})/K$ is an abelian extension this would imply that $F_\infty/\mathbb{Q}$ is abelian. But this extension is known to be always non-abelian, hence the lemma follows.

Let $G_\infty = G(F_\infty/K)$. It is well-known that the torsion subgroup Δ_2 of G_∞ is isomorphic to $G(\mathbb{Q}(E_p)/K)$ under the restriction map and that there is a canonical splitting $G_\infty = \Delta_2 \times \Gamma_2$ where $\Gamma_2 = G(F_\infty/\mathbb{Q}(E_p))$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. We recall here the basic facts about the p-adic interpolation of the special values of Hecke L-series. Let $\mathbb{C}_p$ denote the completion of an algebraic closure of $\mathbb{Q}_p$ and let A denote the ring of integers of the completion of the maximal unramified extension of $\mathbb{Q}_p$. As Weil has remarked, the composition of an embedding $i_p : K \longrightarrow \mathbb{Q}_p$ with the Größencharakter $C = \phi^a \bar{\phi}^{-b}$ of K defines a continuous Galois character $C_p : G_\infty \longrightarrow \mathbb{C}_p^\times$. C is called viable if $a > -b \geq 0$. It is essentially a result of Eisenstein that for a viable Größencharakter we have

$$\Omega_\infty(C) \cdot L(C,1) \in K ,$$

where $\Omega_\infty(C)$ is an explicitely given non-zero complex number (see [23] and [5]). We summarize the p-adic interpolation properties of these numbers: Fix two topological generators σ, τ of Γ_2 . Write $\hat{G}_\infty = \mathrm{Hom}(G_\infty, \mathbb{C}_p^\times)$ and $\hat{\Delta}_2 = \mathrm{Hom}(\Delta_2, \mathbb{Z}_p^\times)$.

Proposition 5.4. There is a unique function $L_p : \hat{G}_\infty \longrightarrow \mathbb{C}_p$ satisfying the following two conditions:-

a) For each $\psi \in \hat{\Delta}_2$ there is a power series $g_\psi(S,T) \in A[[S,T]]$ such that for all $\lambda \in \hat{G}_\infty$ with $\lambda|\Delta_2 = \psi$ we have

$$L_p(\lambda) = g_\psi(\lambda(\sigma)-1,\ \lambda(\tau)-1)\ .$$

b) <u>For each viable Größencharakter</u> $C = \phi^{a}\bar{\phi}^{b}$ <u>we have</u>

$$\Omega_p^{-(a-b)} L_p(C_p) = \Omega_\infty(C) L(C,1) (1-\frac{C(p)}{Np}) (1-\bar{C}(p)^{-1})$$

<u>with a certain p-adic period</u> $\Omega_p \in A^\times$.

Now let M_∞ resp. M_∞^* denote the maximal abelian pro-p-extension over F_∞ which is unramified outside the primes of F_∞ lying above p resp. p^* , and put $X_\infty = G(M_\infty/F_\infty)$ resp. $X_\infty^* = G(M_\infty^*/F_\infty)$. By the usual action of G_∞ on X_∞ or X_∞^* the later groups become modules over the completed group ring $\Lambda_{\Gamma_2} = \mathbb{Z}_p[[\Gamma_2]]$. This Iwasawa algebra is non-canonically isomorphic, depending on the choice of σ and τ , to the ring of formal power series in two variables $\mathbb{Z}_p[[S,T]]$ by sending σ and τ to $1+S$ and $1+T$ respectively. We normalize our choice of σ and τ such that σ resp. τ is a topological generator of Γ_+ resp. Γ_- , where these are the respective subgroups of Γ_2 such that complex conjugation $\rho \in G_\infty$ acts trivially on Γ_+ , i.e. $\rho\sigma\rho=\sigma$, and the action on Γ_- is given by $\rho\tau\rho=\tau^{-1}$. It is not hard to see that X_∞ is a finitely generated Λ_{Γ_2}-torsion module. Under the action of $\Delta_2 \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$ the module X_∞ splits into its eigenspaces

$$X_\infty = \sum_{\psi\in\hat{\Delta}_2}^{\oplus} X_{\infty,\psi}\ ,$$

where the eigenspace $X_{\infty,\psi}$ consists of all $x\in X_\infty$ such that any $\delta\in\Delta_2$ acts by $\delta(x) = \psi(\delta)\cdot x$. By the classification theory of finitely generated Λ_{Γ_2}-modules for any such module A there is a pseudo-isomorphism from A to a direct sum of modules of the form $\Lambda_{\Gamma_2}/(f_\kappa)$, $\kappa=1,\ldots,k$, where the f_κ are non-zero elements of Λ_{Γ_2} . The power series $f(S,T)$, which corresponds to the product $f_1\ldots f_k$, is called a <u>characteristic power series</u> of A . There is much evidence in favour of (see [23], [5]):

The two variable Main Conjecture. For each character $\Psi \in \hat{\Delta}_2$ a characteristic power series of the Ψ-component $X_{\infty,\Psi}$ is given by the p-adic L-function $g_\Psi(S,T)$.

Let ψ denote any character of $\Delta = G(\mathbb{Q}(\mu_p)/\mathbb{Q})$ and $\psi_K \in \hat{\Delta}_2$ the corresponding character defined by $\psi_K = \psi \circ N_{K/\mathbb{Q}}$. Also for the Größencharakter ϕ attached to the elliptic curve E let $\phi_{\Delta_2} = \phi_p | \Delta_2$, the restriction of the Galois character ϕ_p to Δ_2 .

Theorem 5.5. If the two variable Main Conjecture is valid for a character of the form $\Psi = \phi^2_{\Delta_2} \cdot \psi_K$, then the Rank Conjecture 4.1 is true for ψ . If in addition $\psi(-1)=1$, then Main Conjecture 4.2 holds for ψ .

We shall at first verify that Conjecture 3.13 is valid in the CM case. Let τ_E denote the distribution on $\mathbb{Z}_p^\times$ uniquely defined by the integrals (i) and (ii) in conjecture 3.13.

Lemma 5.6. For every Dirichlet character χ of p-power conducto the integral $\int_{\mathbb{Z}_p^\times} \chi \, d\tau_E$ is algebraic, i.e. in $\bar{\mathbb{Q}}$.

Proof. If χ is not the non-trivial character of a real quadrat field, this follows by Theorem 3.1. Now suppose that χ is the exceptional character corresponding to a real quadratic field. Since for instance by (3.2) we know that $L(\phi^2,1) \neq 0$, we can apply Theorem 1 of [21]. Thus we obtain that

$$L(\phi^2 \chi_K, 1) \in L(\phi^2, 1) \cdot \bar{\mathbb{Q}} ,$$

hence the algebraicity statement of the lemma follows also for the exceptional character by Remark 5.2.

We need an extended and more precise version of Proposition 5.4 to the extend that we want the explicit interpolation formula for the special

values of the L-functions of the Größencharakters $C = \phi^2\chi_K$, where χ runs over all Dirichlet characters of p-power conductor. The following formula is well-known and essentially contained in [18]. Let χ be a character of conductor $c_\chi = p^n$ such that $\chi|\Delta = \psi$ and $\psi(-1)=1$. Define the constants

$$C_0 = d_K \cdot Nc_{\phi^2},\quad C_1 = 24 \cdot W(\bar{\phi}^2) \cdot C_0^{-1/2},$$

where d_K denotes the absolute value of the discriminant of K and $W(\bar{\phi}^2)$ is the root number in Hecke's functional equation

$$\left(\frac{2\pi}{\sqrt{C_0}}\right)^{-s} \Gamma(s) L(\bar{\phi}^2, s) = W(\bar{\phi}^2) \left(\frac{2\pi}{\sqrt{C_0}}\right)^{3-s} \Gamma(3-s) L(\phi^2, 3-s).$$

Then we have for $\Psi = \phi^2_{\Delta_2} \cdot \psi_K$

$$(5.1)\quad \Omega_p^{-2} \cdot g_\Psi(\chi(\kappa(\sigma)) \cdot \phi_p^2(\sigma) - 1,\ \phi_p^2(\tau) - 1)$$
$$= \pi \Omega^{-2} C_1 \bar{\chi}(C_0) \phi(p^*)^{-2n} G(\bar{\chi}) L(C,1) \left(1 - \frac{C(p)}{p}\right)\left(1 - C^{-1}(p^*)\right),$$

where the lattice Λ of E in $\mathbb{C}$ is of the form $\Lambda = \mathcal{O} \cdot \Omega$. Note that for χ non-trivial we always have that $C(p) = C^{-1}(p^*) = 0$.

On the other hand by classical cyclotomic Iwasawa theory there is a power series $G_p(\varepsilon\omega\psi, S) \in \mathbb{Z}_p[[S]]$ which interpolates the special values of the Dirichlet L-series $L(\varepsilon\chi, 0)$ for non-trivial χ by

$$(5.2)\quad G_p(\varepsilon\omega\psi, \chi(\kappa(\sigma))^{-1} - 1) = L(\varepsilon\chi, 0).$$

Here ω denotes the Teichmüller character. Note, that $G_p(\varepsilon\omega, 0) = 0$.

Proposition 5.7. Conjecture 3.13 is valid in the CM case. In particular for each character ψ of Δ with $\psi(-1)=1$ we have

$$G_\psi(S) = I_\psi \cdot u_\psi(S) \Omega_p^{-2} g_\psi(\phi_p^2(\sigma)(S+1) - 1, \phi_p^2(\tau) - 1) \cdot G_p(\varepsilon\omega\psi, (1+S)^{-1} - 1),$$

where $u_\psi(S)$ is the invertible power series in $\mathbb{Z}_p[[S]]$ such that $u_\psi(\chi(\kappa(\sigma)) - 1) = \chi(C_0)$ for every character χ of p-power conductor with

$\chi|\Delta=\psi$, and I_ψ is an algebraic number $\neq 0$.

Proof. In view of Remark 5.2 the proof is complete by putting together the formulas (5.1) and (5.2) above.

Remark 5.8. The previous arguments in fact yield much more precise information about possible denominators of the measure τ_E . Let

$$\varphi : (\Gamma_0(N)\backslash H)^* \longrightarrow E$$

denote a Weil parametrization of E . A little exercise shows that the distribution $\deg(\varphi).\tau_E$ has p-integral values for $p > 3$ and not only that the values of τ_E have bounded p-adic absolute value.

Next we shall consider the Iwasawa module $S(\Sigma)$ of § 4 under the substantially simplifying assumption that E has complex multiplication. The factorization $p = pp^*$ in K gives rise to the splitting of various Galois modules attached to E and p . For each integer n, let E_{p^n} resp. $E_{p^{*n}}$ denote the group of p^n-division points resp. p^{*n}-division points on E . For the corresponding Tate module write

$$T_p = \varprojlim E_{p^n} , \quad V_p = T_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

and analoguously define T_{p^*} and V_{p^*} . The canonical splitting $E_{p^n} = E_{p^n} \oplus E_{p^{*n}}$ induces the splitting of the Tate module

$$T_p(E) = T_p \oplus T_{p^*} , \quad V_p(E) = V_p \oplus V_{p^*} .$$

Moreover the p-divisible group W_p attached to the ℓ-adic representation $\mathrm{Sym}^2(V_\ell(E))$ has the following decomposition

$$(5.3) \qquad W_p = W_p \oplus W_{p^*} \oplus \mu_{p^\infty}(\varepsilon) ,$$

where we have defined $W_p = \mathrm{Sym}^2(V_p)/\mathrm{Sym}^2(T_p)$ and W_{p^*} similarly and where $\mu_{p^\infty}(\varepsilon)$ is equal to μ_{p^∞} as a group but with the Galois action twisted by the imaginary-quadratic character ε associated with

$K/\mathbb{Q}$. Note that the action of $G(F_\infty/K)$ respects the decomposition (5.3), whereas an automorphism, which is non-trivial on K , permutes W_p and W_{p^*} but still acts on $\mu_{p^\infty}(\varepsilon)$. Let M_∞ denote the maximal abelian p-extension of F_∞ which is unramified outside the primes above p , and put

$$X_\infty = G(M_\infty/F_\infty) \ .$$

Let $U_\infty = G(F_\infty/Q_\infty)$ and write $\mathrm{Hom}_{(p)}(X_\infty,W_p)$ for the group of homomorphisms which for any prime v above p of F_∞ send the inertia group I_v to $W_{p,v}^0$, the kernel of reduction mod v in W_p .

Proposition 5.9. The restriction map

$$\mathrm{res} : H^1(Q_\infty,W_p) \longrightarrow H^1(F_\infty,W_p)^{U_\infty}$$

induces a quasi-isomorphism of Θ-modules

$$S(\Sigma) \xrightarrow{\sim} \mathrm{Hom}_{(p)}(X_\infty,W_p)^{U_\infty} \ .$$

Proof. We first want to show that the initial restriction map has finite kernel and cokernel. Let $K_\infty = KQ_\infty$ and let c denote the generator of the cyclic group $G(K_\infty/Q_\infty)$ of order 2. Put $H_\infty=G(F_\infty/K_\infty)$ and consider W_p as H_∞-module. By the usual inflation-restriction sequence from Galois cohomology we have

$$0 \to H^1(H_\infty,W_p) \to H^1(K_\infty,W_p) \to H^1(F_\infty,W_p)^{H_\infty} \to H^2(H_\infty,W_p) \ .$$

Lemma 5.10. We have

$$H^i(H_\infty,W_p) = \mu_{p^\infty}(\varepsilon) \oplus T_i \quad (i=1,2) \ ,$$

where T_i is a finite p-group.

Let us assume for the moment that the lemma is valid. Another application of the inflation-restriction sequence yields

$$H^1(Q_\infty,W_p) = H^1(K_\infty,W_p)^{<c>} \ .$$

So by Lemma 5.10 and the fact that for $p > 2$ the sequence above remains exact, when we pass to <c>-invariants, we immediately see that the initial restriction map res has finite kernel and cokernel. In particular the induced map on $S(\Sigma)$ has finite kernel. Since res also has finite cokernel, there is a constant p-power q such that for any given homomorphism $f \in \mathrm{Hom}_{(p)}(X_\infty, W_p)^U$ there is a 1-cocycle $\delta : G(\bar{\mathbb{Q}}/Q_\infty) \longrightarrow W_p$ with $q.f=\mathrm{res}(\delta)$. We claim that in fact the 1-cohomology class $[\delta]$ of δ belongs to $S(\Sigma)$. So we must look at the behaviour of $[\delta]$ under the various local restriction maps j_w from § 4. First let w be a prime of $\bar{\mathbb{Q}}$ which does not lie above p . Then $F_{\infty,w}=(F_1Q_\infty)_w$ is a bicyclic extension of $Q_{\infty,w}$ of degree dividing $2(p-1)$ and therefore we have an injection

$$H^1(Q_{\infty,w}, W_p) \hookrightarrow H^1(F_{\infty,w}, W_p) .$$

The properties of f imply that $\delta(\sigma)=0$ for all σ in the inertia group of $\bar{\mathbb{Q}}_w/F_{\infty,w}$. So δ must vanish on $G(\bar{\mathbb{Q}}_w/F_{\infty,w})$ since there is no proper unramified abelian p-extension over $F_{\infty,w}$ and by the injection above we obtain that $j_w[\delta]=0$. Now let v be a prime of $\bar{\mathbb{Q}}$ above p . Write δ_v for the 1-cocycle δ restricted to $G(\bar{\mathbb{Q}}_v/Q_{\infty,p})$ assuming that v lies above the prime p of K . It is well-known that $F_{\infty,v}/Q_{\infty,p}$ is unramified, and therefore the inertia subgroup $J_{\infty,v}$ of $G(\bar{\mathbb{Q}}_v/Q_{\infty,p})$ coincides with the inertia subgroup I_v of $G(\bar{\mathbb{Q}}_v/F_{\infty,v})$. Thus again by the required properties of f our δ_v sends $J_{\infty,v}$ to $W_{p,v}^0$, hence $[\delta_v]$ belongs to $H(Q_{\infty,p}, W_p)$, which completes the proof of Proposition 5.9.

Proof of Lemma 5.10. We write $H^i(H_\infty, W_p)$ as the inductive limit of the finite cohomology groups $H^i(G(F_n/K_n), \mathrm{Sym}^2 E_{p^n})$, where $F_n=\mathbb{Q}(E_{p^n})$ and $K_n=K(\mu_{p^n})$. Since $G(F_n/K_n)$ is cyclic we are led to compute H^0 and H^{-1} . On the other hand the decomposition (5.3) allows us to treat each term of W_p separately. If we fix a topolo-

gical generator $\tilde{\tau}$ of $G(F_\infty/K_\infty)$, the action of $\tilde{\tau}$ on $\mathrm{Sym}^2 E_{p^n}$ is just multiplication by $\phi_p(\tilde{\tau})^2$. Thus the $G(F_n/K_n)$-invariants of $\mathrm{Sym}^2 E_{p^n}$ have order bounded independently of n and therefore $H^0(H_\infty, W_p)$ as well as $H^0(H_\infty, W_{p^*})$ is finite. Obviously we have $H^0(H_\infty, \mu_{p^\infty}(\varepsilon)) = \mu_{p^\infty}(\varepsilon)$ which proves the lemma for $i=2$. The norm map of F_n/K_n on $\mathrm{Sym}^2 E_{p^n}$ being multiplication by

$$\sum_{i=0}^{\varphi(p^n)-1} \phi_p(\tilde{\tau})^{2i} = (\phi_p(\tilde{\tau})^{2\varphi(p^n)}-1)/(\phi_p(\tilde{\tau})-1) ,$$

we immediately find that the kernel of this map has an index in $\mathrm{Sym}^2 E_{p^n}$ bounded independently of n. Since the same is true for the index of $(\tilde{\tau}-1)\mathrm{Sym}^2 E_{p^n}$ in $\mathrm{Sym}^2 E_{p^n}$ we see that $H^1(H_\infty, W_p)$ as well as $H^1(H_\infty, W_{p^*})$ is finite. The lemma is clear now also for $i=1$ since plainly we have $H^1(G(F_n, K_n), \mu_{p^n}(\varepsilon)) = \mu_{p^{n-1}}(\varepsilon)$.

Proposition 5.11. We have

$$\mathrm{Hom}_{(p)}(X_\infty, W_p) = \mathrm{Hom}(X_\infty, W_p) \oplus \mathrm{Hom}(X_\infty^*, W_{p^*}) \oplus \mathrm{Hom}(X_\infty, \mu_{p^\infty}(\varepsilon)) ,$$

and therefore a quasi-isomorphism of Θ-modules

$$S(\Sigma) \xrightarrow{\sim} \mathrm{Hom}(X_\infty, W_p)^{H_\infty} \oplus \mathrm{Hom}((X_\infty)_{H_\infty, \varepsilon}, \mu_{p^\infty}(\varepsilon)) ,$$

where $H_\infty = G(F_\infty/KQ_\infty)$ and Θ acts on the right hand side through $G(KQ_\infty/K)$. The subscript ε denotes the ε-eigenspace for the $G(KQ_\infty/Q_\infty)$-action.

Proof. Write any homomorphism $f : X_\infty \longrightarrow W_p$ as a sum $f = f_1+f_2+f_3$ according to the decomposition (5.3). Then obviously f belongs to $\mathrm{Hom}_{(p)}(X_\infty, W_p)$ if and only if f_1 vanishes on I_v for all v above p^* and f_2 vanishes on I_v for all v above p. This being equivalent to the condition that f_1 factors through X_∞ and f_2 factors through X_∞^*, we obtain the required decomposition of $\mathrm{Hom}_{(p)}(X_\infty, W_p)$. We observe that the action of complex conjugation

$\rho \in G(F_\infty/\mathbb{Q})$ sends X_∞ to X_∞^* and W_p to W_{p^*}. Hence ρ permutes the first two terms in the decomposition of $\mathrm{Hom}_{(p)}(X_\infty, W_p)$. We arrive at U_∞-invariants by first taking H_∞-invariants followed by taking $G(KQ_\infty/Q_\infty)$-invariants. Since conjugation by ρ sends an element of H_∞ to its inverse, ρ permutes the H_∞-invariants of the first two terms, i.e.

$$\rho(\mathrm{Hom}(X_\infty, W_p)^{H_\infty}) = \mathrm{Hom}(X^*, W_{p^*})^{H_\infty}.$$

Since for the generator c of $G(KQ_\infty/Q_\infty)$ the involution $\kappa = \rho|_{KQ_\infty} \cdot c \in G(KQ_\infty/K)$ acts as an automorphism on the H_∞-invariants of each term, we obtain that c also permutes the H_∞-invariants of the first two terms. Thus we get

$$\mathrm{Hom}_{(p)}(X_\infty, W_p)^{U_\infty} = (1+c)\mathrm{Hom}(X_\infty, W_p)^{H_\infty} \oplus \mathrm{Hom}((X_\infty)_{H_\infty, \varepsilon}, \mu_{p^\infty}(\varepsilon))$$

which by Proposition 5.9 completes the proof of Proposition 5.11.

Corollary 5.12. For each character ψ of Δ there is a quasi-isomorphism of Λ-modules

$$Z_\psi(\Sigma) \xrightarrow{\sim} (X_\infty, \phi_{\Delta_2}^2 \cdot \psi_K \otimes T_p^{\otimes(-2)})_{\Gamma_-} \oplus (X_\infty)_{H_\infty, \varepsilon\omega\psi} \otimes T_p(\mu)^{\otimes(-1)}(\varepsilon)$$

Proof. This is a straightforward exercise in Pontrjagin duality.

Now we are going to treat the two Λ-modules on the right hand side in Corollary 5.12 separately.

Proposition 5.13. If the two variable Main Conjecture is valid for a character of the form $\Psi = \phi_{\Delta_2}^2 \cdot \psi_K \in \hat{\Delta}_2$, then $(X_{\infty,\Psi} \otimes T_p^{\otimes(-2)})_{\Gamma_-}$ is a Λ-torsion module with a characteristic power series generating the same ideal in $A[[S]]$ as $g_\psi(\phi_p^2(\sigma)(S+1)-1, \phi_p^2(\tau)-1)$.

Proof. Let $f_\Psi(S,T)$ denote a characteristic power series of $X_{\infty,\Psi}$. Therefore the $\mathbb{Z}_p[[S,T]]$-torsion module $V = X_{\infty,\Psi} \otimes T_p^{\otimes(-2)}$

has the characteristic power series

$$f_V(S,T) = f_\Psi(\phi_p^2(\sigma)(S+1)-1,\ \phi_p^2(\tau)(T+1)-1) \ .$$

The $\mathbb{Z}_p[[S]]$-module given by the Γ_--coinvariants $V_{\Gamma_-} = V/T\cdot V$ plainly is a $\mathbb{Z}_p[[S]]$-torsion module if and only if $f_V(S,0)$ is non-zero, i.e. if T does not divide $f_V(S,T)$. By our assumption this condition is equivalent to the non-vanishing of $g_\Psi(\phi_p^2(\sigma)(S+1)-1,\ \phi_p^2(\tau)-1) \in A[[S]]$. By (5.1) this can be achieved by the non-vanishing of the special values $L(\phi^2\chi_K,1)$ or, which comes to the same, by the non-vanishing of $L(\phi^2\chi_K,2)$. But this follows easily via Hadamard's reasonning. Now V_{Γ_-} is a $\mathbb{Z}_p[[S]]$-torsion module and we obtain a characteristic power series from the equality of Λ-modules

$$\Lambda \cdot f_{V_{\Gamma_-}}(S) = \Lambda \cdot f_V(S,0) \cdot f_{V^{\Gamma_-}}(S) \ ,$$

where in addition V^{Γ_-} is pseudo-null as a $\mathbb{Z}_p[[S,T]]$-module (cf. [14] p.10). We are done if we can show that V has no proper pseudo-null submodule. By Théorème 23 of [14] and a result of Greenberg (cf. [14] p.45) one knows that X_∞ has no proper pseudo-null $\mathbb{Z}_p[[S,T]]$-submodules, hence $X_\infty \otimes T_p^{\otimes(-2)}$ has no such submodules. This finishes the proof of Proposition 5.13.

We now concentrate on the second term of $Z_\psi(\Sigma)$ in the decomposition of Corollary 5.12. Let M'_∞ denote the maximal abelian extension of $K_\infty = KQ_\infty$ inside M_∞ and let Δ_- denote the torsion subgroup of H_∞ , which has the natural decomposition $H_\infty = \Delta_- \times \Gamma_-$. Further let N_∞ denote the maximal abelian pro-p-extension of K_∞ , which is unramified outside the primes above p .

Lemma 5.14. a) There is an isomorphism of $G(K_\infty/\mathbb{Q})$-modules

$$(X_\infty)_{H_\infty} \xrightarrow{\sim} G(M'_\infty/F_\infty) \ .$$

b) Furthermore the restriction map induces an isomorphism

$$G(M'_\infty/F_\infty) \xrightarrow{\sim} G(N_\infty/F_\infty^{\Delta_-}) \ .$$

Proof. By a standard result in Iwasawa theory the commutator group of $G(M_\infty/K_\infty(E_p))$ is given by

$$G(M_\infty/K_\infty(E_p))^{com} = (X_\infty)^{\tau-1} \ ,$$

where, as defined earlier, τ generates Γ_-. Note that $K_\infty(E_p) = F_\infty^{\Gamma_-}$. Hence the maximal abelian extension $\tilde{M}_\infty$ of $K_\infty(E_p)$ inside M_∞ has Galois group over F_∞ given by

$$G(\tilde{M}_\infty/F_\infty) = (X_\infty)_{\Gamma_-} \ .$$

The Galois group $G = G(\tilde{M}_\infty/K_\infty(E_p))$ is an abelian pro-p-group and the group extension

$$1 \longrightarrow G \longrightarrow G(\tilde{M}_\infty/K_\infty) \longrightarrow \Delta_- \longrightarrow 1$$

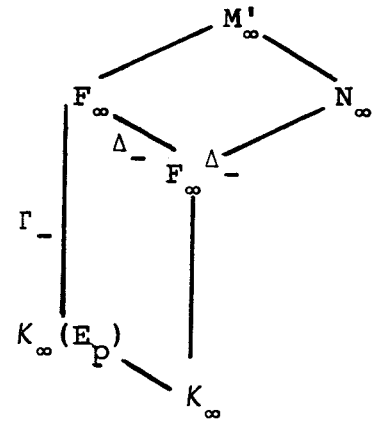
must split. Therefore it follows easily that $G(\tilde{M}_\infty/K_\infty)^{com} = I_{\Delta_-} G$ with the augmentation ideal $I_{\Delta_-} = (\delta-1)\mathbb{Z}_p[\Delta_-]$ for some arbitrary generator δ of the cyclic group Δ_-. Thus we get

$$G(M'_\infty/F_\infty) \cong G(\tilde{M}_\infty/F_\infty)/I_{\Delta_-} G \ ,$$

where in fact $I_{\Delta_-} G = I_{\Delta_-} G(\tilde{M}_\infty/F_\infty)$, hence we find the required isomorphism in a) from

$$G(M'_\infty/F_\infty) \cong G(\tilde{M}_\infty/F_\infty)_{\Delta_-} = (X_\infty)_{H_\infty} \ .$$

Decomposing $G(M'_\infty/K_\infty)$ in its non-p-part, which is Δ_- via restriction to F_∞, and its pro-p-part, we arrive at once at the desired isomorphism in b), which proves the lemma. We add the following diagram in order to illustrate the situation.



We have now everything at hand to finish the proof of Theorem 5.5. We begin with the proof of the Rank Conjecture 4.1. By Corollary 5.12, Proposition 5.13 and Lemma 5.14 the Λ-rank of $Z_\psi(\Sigma)$ is given as

$$\operatorname{rank}_\Lambda Z_\psi(\Sigma) = \operatorname{rank}_\Lambda G(N_\infty/K_\infty)_{\varepsilon\omega\psi} \otimes T_p(\mu)^{\otimes(-1)}(\varepsilon) \ .$$

On the other hand by Theorem 1.8 in [4] for any character λ of $G(K(\mu_p)/\mathbb{Q})$ the Λ-rank of $G(N_\infty/K_\infty)_\lambda$ is 0 or 1 according as λ is an even or odd character. Since the Teichmüller character ω as well as ε both are odd characters we find that $Z_\psi(\Sigma)$ has Λ-rank equal 0 or 1 according as ψ is even or odd, hence Conjecture 4.1 is valid.

Remark 5.15. Even without assuming the validity of the two variable Main Conjecture the previous arguments show that in the CM-case we always have

$$\operatorname{rank}_\Lambda Z_\psi(\Sigma) \geq 1 \quad \text{for odd} \quad \psi \ .$$

For the proof of Main Conjecture 4.2 assume that ψ is an even character. By Proposition 5.7 we know that Conjecture 3.13 is valid in the CM-case. From the exact sequence of $G(K_\infty/\mathbb{Q})$-modules

$$0 \longrightarrow (X_\infty)_{H_\infty} \longrightarrow G(N_\infty/K_\infty) \longrightarrow \mathbb{Z}_p(\varepsilon) \longrightarrow 0$$

we get by Lemma 5.14 for any even character ψ an isomorphism

the $\varepsilon\omega\psi$-eigenspaces of $(X_\infty)_{H_\infty}$ and $G(N_\infty/K_\infty)$. In terms of the characteristic polynomial

$$f_p(\varepsilon\omega\psi,t) = \det(t-(\sigma-1);\ (X_\infty)_{H_\infty,\varepsilon\omega\psi})$$

we obtain that the characteristic polynomial of the twisted module generates the same ideal in $\mathbb{Z}_p[[t]]$ as $f_p(\varepsilon\omega\psi,\kappa(\sigma)\cdot(1+t)-1)$, hence by the Theorem of Mazur-Wiles in [13] they generate the same ideal as the power series $G_p(\varepsilon\omega\psi,(1+t)^{-1}-1)$ from (5.2). This fact together with Propositions 5.7, 5.13 and Corollary 5.12 tells us that up to a factor $v_\psi \neq 0$ in $\mathbb{Q}_p$ a characteristeric power series of $Z_\psi(\Sigma)$ is given by $G_\psi(S)$, thus completing the proof of Theorem 5.5.

We finish this section by the following remark.

Remark 5.16. In the CM-case the corollary of Main Conjecture 4.2 always is valid.

Proof. By Pontrjagin duality one has to show that $Z_{\psi_0}(\Sigma)_\Gamma$ contains a copy of $\mathbb{Z}_p$, where ψ_0 denotes the trivial character. By the previous arguments this is an immediate consequence of the fact that $G_p(\varepsilon\omega,S)$ vanishes at $S=0$.

6. Appendix

In this appendix we shall verify the two tables given at the end of § 2 , which for the primes $r=2$ and 3 list all possibly arising cases under the assumption that E has potential good reduction at r and $\# \Phi_r \geq 3$.

Case r=3. In order to compute the conductor of E and of the symmetric square at the prime $r=3$ we use the following lemma.

Lemma A.1. Let Φ_3 denote the inertia group in $G(\mathbb{Q}_3(E_4)/\mathbb{Q}_3)$ and let $G_0 \supseteq G_1 = \ldots = G_\nu \neq G_{\nu+1} = \{id\}$ denote the series of higher ramification groups. Then we have $\nu = 0,1,2$ according as Φ_3 is cyclic of order 4,3,6 and we have $\nu = 2$ or 6 if Φ_3 is non-cyclic.

Proof. Let q denote the maximal ideal in the ring of integers $\mathcal{O}_F$ of $F=\mathbb{Q}_3(E_4)$. Consider the different

$$\mathfrak{d}_{F/\mathbb{Q}_3} = q^{\#\Phi_3 - 1 + 2\nu}$$

and the discriminant $\mathfrak{d}_{F/T}$ of F over the inertia field $T=F^{\Phi_3}$. The case $\Phi_3 = \mathbb{Z}/4$ being obvious we may assume that G_1 is cyclic of order 3. Now for cyclic Φ_3 of order 3 and 6 the extension F/T is by class field theory given by a finite character λ on $\mathcal{O}_T^\times$. So by the "Führerdiskriminantenformel" and from the fact that the map from $1+3\mathcal{O}_T$ to $1+9\mathcal{O}_T$ which sends x to x^3 , is surjective, we get $c_\lambda = c_{\lambda^2} = 9$ and $c_{\lambda^3} = 3$ if λ^3 is not the trivial character, hence $\mathfrak{d}_{F/T} = 3^4\mathcal{O}_T$ or $3^9\mathcal{O}_T$ according as Φ_3 is cyclic of order 3 or 6. Now by comparison with the different we find the predicted values of ν . Finally let Φ_3 be non-cyclic, i.e. Φ_3 is the non-abelian semi-direct product of $\mathbb{Z}/4$ with its normal subgroup $\mathbb{Z}/3$. Let H denote the cyclic subgroup of order 6. The Galois invariants $L=F^H$ define a ramified quadratic extension of T where $L/\mathbb{Q}_3$ is abelian. Now ν does not change if we replace T by an unramified extension T' and

F resp. L by $F'=FT'$ resp. $L'=LT'$. This is clear by the properties of the function $\phi_{F/T'}$ giving the upper numeration of ramification groups in terms of the lower one (cf. [3] p.37). So we may assume that L' contains the ramified quadratic extensions of $\mathbb{Q}_3$ and in particula that $\mathbb{Q}_3(\mu_3) \subseteq L'$. Hence we have $L'=T'(\mu_3)$ and $F'=L'(\sqrt[6]{u})$ for some $u \in L'$. We denote by L_1' the quadratic extension of L' in F' give by the Galois invariants under G_1 . Further let $v \in L_1'$ denote an element such that $F'=L_1'(\sqrt[3]{v})$ and where either v is a unit or $v=\pi_1$ is a uniformizing element of L_1' . Therefore the discriminant of the Kummer extension F'/L_1' , which is $\mathfrak{d}_{F'/L_1'} = \pi_1^{2(\nu+1)}$ in general, becomes π_1^{14} in the case $v=\pi_1$. If v is a unit we still find that $\mathfrak{d}_{F'/L_1'}$ divides π_1^{12} , i.e. $\nu \leq 5$. In order to achieve $\nu=2$ we consider the character χ of order 6 on $O^\times = O_L^\times$, which by class field theory corresponds to F'/L' . Again we write the discriminant $\mathfrak{d}_{F'/L'} = \pi^{5+2\nu}$ (here $\pi=1-\zeta$ and ζ is a primitive third root of 1) by the "Führerdiskriminantenformel" as $\mathfrak{d}_{F'/L'} = (c_{\chi_2} c_{\chi})^2 \cdot c_{\chi^3}$, which by the fact that $1+\pi^i O=(1+\pi^i O)^2$ yields $c_\chi=\pi^{1+\nu/2}$. In particular we find that ν is even, hence $\nu=2$ or 4 . Finally an easy calculation, where one exploits how $G(L_1'/T')$ acts on $G(F'/L')$ by conjugation, shows that χ is trivial on $(1+\pi^2 O)^2$, hence c_χ divides π^2 and $\nu=2$, which completes the proof of the lemma.

The columns for $\mathrm{ord}_3 N$ and $\mathrm{ord}_3 C$ in the table now follow by

Lemma A.2. The 3-part of the conductor N of E is given by

$$\mathrm{ord}_3 N = 2,\ 2+6\nu/d \text{ and } 2+\nu/2$$

according as (i) Φ_3 is cyclic of order 4, (ii) Φ_3 is cyclic of order $d=3$ or 6 and (iii) Φ_3 is non-abelian. The 3-part of the conductor C of the symmetric square is given by

$$\mathrm{ord}_3 C = 2,\ 2+6\nu/d \text{ and } 3+\nu/2$$

according as the cases (i), (ii), (iii) turn up.

Proof. By definition $ord_3 N$ (resp. $ord_3 C$) $= \varepsilon+\delta$ where $\varepsilon =$ $\dim V - \dim V^{\Phi_3}$ and

$$\delta = \sum_{i=1}^{\infty} \frac{\#G_i}{\#G_0} \dim_{\mathbb{F}_\ell} M/M^{G_i}$$

for $V = H^1_\ell(E)$ resp. $Sym^2 H^1_\ell(E)$ and $M = E_\ell$ resp. $Sym^2 E_\ell$ with any $\ell \geq 5$. As we saw in the proof of Lemma 1.4, we have $\varepsilon = 2$ for $V = H^1_\ell(E)$ in all cases and for the symmetric square we have $\varepsilon = 2$ and 3 where $\varepsilon = 2$ if and only if Φ_3 is cyclic, i.e. in the cases (i) and (ii). Since $\delta = 0$ in the tame case (i) we may assume for the remainder of the proof that G_1 is cyclic of order 3. Choose $\ell \equiv 1(3)$ and decompose $M = E_\ell$ as in the proof of Lemma 1.4 into 1-dimensional G_1-eigenspaces

$$M = M(\zeta) \oplus M(\zeta^{-1}) .$$

Thus in particular $M^{G_1} = 0$, hence $\delta = 6v/\#\Phi_3$, which shows the formula for $ord_3 N$. On the other hand this decomposition of E_ℓ also shows for $M = Sym^2 E_\ell$, that M^{G_1} is trivial, hence also $\delta = 6v/\#\Phi_3$ here, thus proving the formula for $ord_3 C$. The proof of the lemma is therefore complete.

We continue the verification of our table. We first dispose of the harmless case where Φ_3 is non-abelian. By Lemmas A.1, A.2 we know that $ord_3 N$ is odd and therefore f must be 3-minimal, i.e. $ord_3 N = ord_3 M$ by Theorem 4.4 in [1]. So we find the last two rows of the table. Now we can assume that Φ_3 is cyclic. If the order of Φ_3 is 4 , then the full Galois group must be non-abelian, since there is no totally ramified cyclic extension over $\mathbb{Q}_3$ of degree 4. So by Lemma 2.14 either f is 3-minimal or $ord_3 M = 1$ since $ord_3 N = 2$ now. But in the latter case a quadratic twist of E would have multiplicative reduction at 3, which is impossible for Φ_3 cyclic of order 4. This

proves the third row of the table. For the remaining cyclic Φ_3 of order 3 and 6 we remark that by Lemma 2.14 the remainder of the proof can be reduced to show, that for f not 3-minimal only the abelian case $\mathrm{ord}_3 M = \mathrm{ord}_3 c_\nu = 2$ can occur. Let f be not 3-minimal. Since we know $\mathrm{ord}_3(N) = 4$, $\mathrm{ord}_3(M)$ must be ≤ 3. This implies already that ε_3^2 is non-trivial, since otherwise ε_3 had conductor equal 3 and therefore the 3-primary part of the level of $g_\varepsilon (=f)$ were a divisor of 27 in contradiction to $\mathrm{ord}_3(N) = 4$. So the order of ν_3 is divisible by 3 and therefore

$$2 \leq \mathrm{ord}_3(c_\nu) \leq \mathrm{ord}_3(M) \leq 3 .$$

By Theorem 4.3 in [1] the combination $\mathrm{ord}_3(c_\nu)=2$, $\mathrm{ord}_3(M)=3$ is impossible, since g is minimal. Hence $\mathrm{ord}_3(c_\nu) = \mathrm{ord}_3(M)$ and we are in the abelian case by Lemma 2.14. As we saw in the proof of that Lemma, the I_3-action on $V_\ell(E) \otimes \bar{\mathbb{Q}}_\ell$ diagonalizes in the form

$$\rho_\ell(\tau) = \begin{pmatrix} \varepsilon_3(\tau) & 0 \\ 0 & \varepsilon_3^{-1}(\tau) \end{pmatrix} .$$

In particular we have $4 = \mathrm{ord}_3 N = \mathrm{ord}_3(c_\varepsilon{}^2)$ and therefore $\mathrm{ord}_3(c_\nu)=2$. This completes the verification of the table for $r = 3$.

Case r = 2 . It is clear by local class field theory that the Galois group $G = G(\mathbb{Q}_2(E_3)/\mathbb{Q}_2)$ cannot be abelian for cyclic Φ_2 of order 3 and 6, since there is no ramified cyclic cubic extension over $\mathbb{Q}_2$. But also for cyclic Φ_2 of order 4, G is non-abelian, since otherwise $\mathrm{ord}_2(M) = \mathrm{ord}_2(c_\nu)$ by Lemma 2.14 which contradicts the 2-minimality of g by Theorem 4.4 in [1]. So G is always non-abelia which yields the first column of the table. We start by completing the first, third and forth row. Assuming that Φ_2 is cyclic of order 3, the ramification is tame, hence $\mathrm{ord}_2(N) = 2$ and moreover $\mathrm{ord}_2(M) =$

by Theorem 4.4 in [1]. By Lemma 1.4 and by the tame ramification we have $ord_2 C = 2$, thus completing the first row. For cyclic Φ_2 of order 6 let L_1 denote the subfield of the compositum $H(E_3)$ of the maximal unramified extension $H/\mathbb{Q}_2$ with $\mathbb{Q}_2(E_3)$, which is given by the invariants under τ^2 , where τ is the generator of Φ_2 . Here Φ_2 is considered as the inertia group of $H(E_3)/\mathbb{Q}_2$. The abelian extension $L_1/\mathbb{Q}_2$ is the compositum of a ramified quadratic extension $L_1'/\mathbb{Q}_2$ with H . Hence there is a quadratic character ε_2 such that for the twist E' of E by that character the action of the inertia group I_2 factors through Φ_2' , which is cyclic of order 3. Applying Theorem 4.1 in [1] this proves $ord_2(M) = 2$ and $ord_2(N) = ord_2(c_\varepsilon{}^2)$ by the results in the previous case. The quadratic character ε_2 has conductor 4 or 8, which immediately yields the missing entries in the third and the forth row. Now we suppose that Φ_2 is cyclic of order 4. Let again τ denote a generator of Φ_2 and let $\sigma \in G$ represent $Frob_2 \in G/\Phi_2$. Since G is known to be non-abelian we have $\sigma\tau = \tau^{-1}\sigma$ and $\tau^4 = 1$. Now the inertia field T certainly contains $\mathbb{Q}_2(\mu_3)$ and moreover the Galois group $G(F/\mathbb{Q}_2(\mu_3))$ is generated by τ and σ^2 . This Galois group is obviously abelian and also a subgroup of $SL_2(\mathbb{F}_3)$. Since there is no abelian subgroup in $SL_2(\mathbb{F}_3)$ having a proper subgroup isomorphic to a cyclic group of order 4, we find that $T = \mathbb{Q}_2(\mu_3)$ and therefore G is either dihedral of order 8 or $G = Q_8$. We continue the computation of the possible conductors. The totally ramified cyclic extension F/T corresponds to a character κ on $\mathbb{Z}_2[\mu_3]^\times$ of order 4 , whose conductor is necessarily $c_\kappa = 2^3 \mathfrak{o}_T$ or $2^4 \mathfrak{o}_T$. By the "Führerdiskriminantenformel" for F/T we find the discriminants $\mathfrak{d}_{F/T} = 2^8 \mathfrak{o}_T$ or $2^{11}\mathfrak{o}_T$, hence $\mathfrak{d}_{F/\mathbb{Q}_2} = 2^{16}$ or 2^{22} . The series of higher ramification groups of F/T is of the form

$$\Phi_2 = G_0 = G_1 = \ldots = G_\nu \supsetneq G_{\nu+1} = \ldots = G_{\nu+\mu} \supsetneq G_{\nu+\mu+1} = \{id\} .$$

The largest integer $a = \nu + \mu$ such that G_a is non-trivial, can be

expressed by the conductor $c_{F/T}$ of F/T using the function $\phi_{F/T}$ from [3] as

$$c_{F/T} = \phi_{F/T}(a) + 1$$

(see Proposition 1 on p.157 in [3]), where it is immediate from the definition of $\phi_{F/T}$ that $\phi_{F/T}(a) = \nu+\mu/2$. Thus we obtain $(\nu,\mu) = (1,2)$ or $(2,2)$ as the only possible solutions of the system of diophantine equations

$$\nu + \mu/2 = \mathrm{ord}_2(c_\kappa)-1 \ , \ 3(\nu+1) + \mu = \mathrm{ord}_2(\mathfrak{d}_{F/T}) \ .$$

Since there are only trivial $G_{\nu+\mu}$-invariants in E_3 we therefore find that the 2-part of the level N is given by $\mathrm{ord}_2(N) = 6$ or 8 . We will show that 6 is impossible. By Theorem 4.4 in [1] f is not 2-minimal in both cases. Let $h \in S_2(N',\chi^{-2})$ be a 2-minimal form such that $h_\chi = f$ and c_χ is a 2-power. Again by Theorem 4.4 in [1] h is 2-minimal if and only if one of the following conditions holds: a) $\mathrm{ord}_2(N') = 0$ or 2, b) $\mathrm{ord}_2(N')$ is even, ≥ 4 and $2\,\mathrm{ord}_2(c_{\chi^2}) = \mathrm{ord}_2(N')$, c) $\mathrm{ord}_2(N')$ is odd and $2\,\mathrm{ord}_2(c_{\chi^2}) < \mathrm{ord}_2(N')$. Now we assume that $\mathrm{ord}_2(N) = 6$, hence $\mathrm{ord}_2(N') \leq 5$. Then b) is impossible since $c_{\chi^2} \neq 4$ for any χ . For the same reason we find that χ^2 is the trivial character in the cases a) and c). Hence in these cases h necessarily belongs to the quadratic twist E' of E by χ , where I_2 now acts on E_3' through a finite quotient Φ_2' , whose possible structures are: the trivial group, a cyclic group of order 3, Q_8 or $SL_2(\mathbb{F}_3)$. Here we have used that a) and c) cannot occur for cyclic Φ_2 of order 4 or 6, since we have already verified that $\mathrm{ord}_2(N') = 4,6$ or 8 in these cases. On the other hand the inertia group over the quadratic extension field $K_\chi/\mathbb{Q}_2$ defined by χ , must act in the same way on E_3 as on E_3' , which is impossible for our cyclic Φ_2 of order 4 and the possible group structures of Φ_2' listed above. Thus

we showed that $\mathrm{ord}_2(N) = 8$, $(\nu,\mu) = (2,2)$, $\mathfrak{d}_{F/T} = 2^{11}\mathcal{O}_T$, $c_\kappa = 2^4\mathcal{O}_T$, $c_{\kappa^2} = 2^3\mathcal{O}_T$. By the before mentioned criterion for 2-minimality we find that $\mathrm{ord}_2(M) = 6$ or 7 and $\mathrm{ord}_2(c_\varepsilon) = 4$. In order to show that only $\mathrm{ord}_2(M) = 6$ can possibly occur, we choose again a character χ of $\mathbb{Z}_2^\times$, but now of order 4, such that $c_\chi = 2^4$ and such that the quadratic extension $K_\chi/\mathbb{Q}_2$, defined by χ^2 , and the quadratic extension T_κ/T , defined by κ^2 , are related by $T_{\kappa^2} = TK_\chi$. We claim that the 3-adic representation given by the twist $(T_3(E) \otimes \bar{\mathbb{Q}}_3) \otimes \chi$ has in fact 2-conductor equal to 2^6 , i.e. $\mathrm{ord}_2(M) = 6$. The verification is left as an exercise to the reader. To finish the second row of the table we still must show that $\mathrm{ord}_2 C = 6$. By Lemma 1.4 we have $\varepsilon_2 = 2$. Take any prime $\ell \equiv 1 \bmod 4$, so that E_ℓ decomposes into two eigenspaces where τ acts like multiplication by a primitive fourth root of unity ζ resp. ζ^{-1} , say $E_\ell = \mathbb{F}_\ell \cdot x \oplus \mathbb{F}_\ell \cdot y$. Hence we immediately get that the Galois invariants of the symmetric square under the action of the higher ramification groups are given by

$$(\mathrm{Sym}^2 E_\ell)^{G_i} = \mathrm{Sym}^2 E_\ell \quad \text{or} \quad \mathbb{F}_\ell \cdot (x\otimes y + y\otimes x)$$

according as G_i is cyclic of order 2 or 4. Thus we find $\delta_2 = 2\nu$ and therefore $\mathrm{ord}_2(C) = 2+4$.

Now we suppose $\Phi_2 = Q_8$. For $F = \mathbb{Q}_2(E_3)$ we observe again that the inertia field is given by $T = \mathbb{Q}_2(\mu_3)$, since otherwise we had $G(F/\mathbb{Q}_2) = GL_2(\mathbb{F}_3)$ and $(T : \mathbb{Q}_2) = 6$, i.e. $GL_2(\mathbb{F}_3)$ would have a cyclic quotient of order 6, which is not true. So $G = G(F/\mathbb{Q}_2)$ is obviously a 2-Sylow group of $GL_2(\mathbb{F}_3)$, hence dihedral of order 16. Moreover there is a ramified quadratic extension $K_1/\mathbb{Q}_2$ in F such that $G(F/K_1)$ is cyclic of order 8. Again we have to determine the series of higher ramification groups

$$\Phi_2 = G_0 = G_1 = \ldots = G_\nu \supsetneq G_{\nu+1} = \ldots = G_{\nu+\mu} \supsetneq G_{\nu+\mu+1} = \ldots = G_{\nu+\mu+\lambda} \supsetneq G_{\nu+\mu+\lambda+1} = \{\mathrm{id}\} ,$$

where possibly $\mu = 0$. The 2-conductor of E is of the form

$ord_2(N) = 2+2\nu+\mu+\lambda/2$. Next we compute a set of triples (ν,μ,λ) which contains all possibly occuring triples in our situation. We firstly write the discriminant of $F/\mathbb{Q}_2$ as $ord_2(\mathfrak{d}_{F/\mathbb{Q}_2}) = 14(\nu+1) + 6\mu + 2\lambda$ and secondly via the "Führerdiskriminantenformel" of F/K_1 for all possible fields K_1 and all possible characters ψ on the 1-units of K_1 with $\psi^4 = 1$ as

$$\mathfrak{d}_{F/\mathbb{Q}_2} = N_{K_1/\mathbb{Q}_2}(c_\psi^4 \cdot c_\psi^{2^2}) \cdot \mathfrak{d}_{K_1/\mathbb{Q}_2}^8 .$$

Here we take into account that TK_1/K_1 is unramified. Now let π denote a prime of K_1 and write U_n for the group of units of K_1 which are congruent 1 modulo π^n . Since $U_7 = U_3^4$ we have that c_ψ divides π^7 . Since $G(F/\mathbb{Q}_2)$ is dihedral, a generator ρ of $G(K_1/\mathbb{Q}_2)$ acts on $G(F/K_1)$ such that $\psi(1+\pi\alpha)^{-1} = \psi(1+\pi^\rho\alpha^\rho)$, hence $U_1^{1+\rho}$ is in the kernel of ψ . In particular ψ is trivial on $(1+4)^{1+\rho} = 1+3\cdot 2$ which is congruent to $1+\pi^6$ modulo π^7 , hence c_ψ divides π^6 . One easily checks that $c_{\psi^2}=\pi^2$ or π^4 according as $c_\psi=\pi^3,\pi^4,\pi^5$ or $c_\psi=\pi^6$. Furthermore the case $c_\psi = \pi^5$ cannot occur for $K_1 = \mathbb{Q}_2(\sqrt{-1})$ and $K_1 = \mathbb{Q}_2(\sqrt{3})$, where with $\pi = 1-\sqrt{-1}$ resp. $\pi = \sqrt{3} - 1$, ψ is trivial on $(1+\pi^3)^{1+\rho} \equiv 1+\pi^4 \bmod \pi^5$. We now list the various cases for c_ψ and the simultanious solutions (ν,μ,λ) with integral $\nu \geq 1$ and $\mu,\lambda \geq 0$ of the diophantine equations

$$(*)\quad ord_\pi(c_\psi)=\nu+\mu+\lambda/2+1,\ ord_2(\mathfrak{d}_{F/\mathbb{Q}_2})=14(\nu+1)+6\mu+2\lambda)$$

where as previously we use the function ϕ_{F/K_1} and that we have $\phi_{F/K_1}(\nu+\mu+\lambda) = \nu+\mu+\lambda/2$. There are exactly 6 ramified quadratic extensions $K_1/\mathbb{Q}_2$. For the fields $K_1=\mathbb{Q}_2(\sqrt{-1}),\ \mathbb{Q}_2(\sqrt{3})$ where $\mathfrak{d}_{K_1/\mathbb{Q}_2}=4$, we find

$\mathrm{ord}_\pi(c_\psi)$	$\mathrm{ord}_\pi(c_{\psi^2})$	$\mathrm{ord}_2 \mathfrak{d}_{F/\mathbb{Q}_2}$	(ν,μ,λ)	$\mathrm{ord}_2(N)$
3	2	32	(1,0,2)	5
4	2	36	(1,0,4)	6
6	4	48	(1,2,4)	8

For the other fields $K_1 = \mathbb{Q}_2(\sqrt{\pm 2}), \mathbb{Q}_2(\sqrt{\pm 6})$ where $\mathfrak{d}_{K_1/\mathbb{Q}_2} = 8$, we only find a solution of (*) for $\mathrm{ord}_\pi(c_\psi)=6$. So we get $\mathrm{ord}_\pi(c_{\psi^2})=4$, $\mathrm{ord}_2(\mathfrak{d}_{F/\mathbb{Q}_2})=56$, $(\nu,\mu,\lambda) = (2,1,4)$ and $\mathrm{ord}_2(N)=9$ in this case. We want to exclude the case $\mathrm{ord}_2(N)=8$. Let L denote the intermediate field $K_1 \subset L \subset F$ such that $(L : K_1) = 4$. Since $c_{\psi^2} = \pi^4$ we have $4 = \phi_{L/K_1}(a)+1$, where $a \geq 0$ is the largest integer such that the a-th higher ramification group $G(L/K_1)_a$ of L/K_1 is non-trivial. Thus we know $a = \phi_{L/K_1}(a) = 3$ and by the well-known properties of the function ϕ we have

$$G(L/K_1)_3 = G(L/K_1)^3 = G(F/K_1)^3 G(F/L) \big/ G(F/L) ,$$

and this is a cyclic group of order 2. On the other hand $\phi_{F/K_1}(7)=3$ and $G(F/K_1)_7 = G(F/L)$ implies $G(F/K_1)^3 = G(F/L)$, which contradicts the isomorphy above. Hence $\mathrm{ord}_2(N) = 8$ is impossible. For $\mathrm{ord}_2(N)=5,9$ the entries of our table are now clear up to the value of $\mathrm{ord}_2 C$ by the 2-minimality criterion from Theorem 4.4 in [1]. By Lemma 1.4 we have $\varepsilon_2 = 3$. We claim that $\delta_2 = 3\nu+\mu$. This follows easily by the same procedure as in the previous case by decomposing E_ℓ into its eigenspaces for the action of $G_{\nu+1}$. Thus we find that $\mathrm{ord}_2(C) = 6$ or 10 according as $\mathrm{ord}_2(N) = 5,6$ or $\mathrm{ord}_2(N) = 9$. For $\mathrm{ord}_2(N) = 6$ the form f is not 2-minimal and by the before mentioned 2-minimality criterion f is the twist h_χ of a 2-minimal form h of level N' with $\mathrm{ord}_2(N') = 3$ or 5 by a quadratic character χ of conductor $c_\chi = 2^3$. The case $\mathrm{ord}_2(N') = 3$ cannot occur since otherwise E would be the quadratic twist of an elliptic curve E' where the inertia group I_2 acted on E'_3 through $\phi'_2 \cong SL_2(\mathbb{F}_3)$, since the 2-conductor 2^3 has

never occured for the other possible group structures of ϕ_2 according to the so far verified part of our table. But replacing E by E' does not change $ord_2 C = 6$ and, as will be shown in the following, for $\phi_2 \cong SL_2(\mathbb{F}_3)$ always $ord_2 C \neq 6$.

From now on we assume that $\phi_2 \cong SL_2(\mathbb{F}_3)$. Therefore the inertia field T of $F = \mathbb{Q}_2(E_3)$ must be equal to $\mathbb{Q}_2(\mu_3)$, and we have necessarily that $G = G(F/\mathbb{Q}_2)$ is isomorphic to $GL_2(\mathbb{F}_3)$. The series of higher ramification groups is of the form

$$\phi_2 = G_0 \supsetneq G_1 = \ldots = G_\nu \supsetneq G_{\nu+1} = \ldots = G_{\nu+\lambda} \supsetneq G_{\nu+\lambda+1} = \{id\} ,$$

where G_1 is the quaternion group Q_8 of order 8 and $G_{\nu+\lambda}$ is cyclic of order 2. Note that a higher ramification group of order 4 is impossible, since there is no normal cyclic subgroup of order 4 in $GL_2(\mathbb{F}_3)$. Now let $K \subset F$ denote the subfield such that $K/\mathbb{Q}_2$ is norma and $G(K/\mathbb{Q}_2)$ is isomorphic to $PGL_2(\mathbb{F}_3) = S_4$. There are exactly 3 normal extensions $K'/\mathbb{Q}_2$ with Galois group isomorphic to S_4(see [9]) These are given with $(i,j) = (1,0)$, $(0,1)$ or $(1,1)$ by

$$K_{ij} = \mathbb{Q}_2(\mu_3, \sqrt[3]{2}, \sqrt{x_{ij}}, \sqrt{x_{ij}^{\rho}}) , \quad x_{ij} = (1+\sqrt[3]{2})^i (1+\sqrt[3]{4})^j 3^i$$

where the automorphism ρ acts trivially on μ_3 and sends $\sqrt[3]{2}$ to $\zeta \sqrt[3]{2}$ for a fixed generator ζ of μ_3 . The higher ramification groups G_t' in $G(K_{ij}/\mathbb{Q}_2)$ are as follows: for $(i,j) = (0,1)$ G_1' is the direct product of two cyclic groups of order 2 and G_2' is trivial, for $(i,j) = (1,0)$ or $(1,1)$ $G_1' = G_5'$ is the direct product of two cyclic groups of order 2 and G_6' is trivial. This tells us that $\nu = 1$ for $(i,j) = (0,1)$ and $\nu = 5$ in the other two cases by the properties of the function $\phi_{F/\mathbb{Q}_2}$, which completes the last column of our table by the obvious formula $ord_2(C) = 3+\nu$. Since the 2-conductor of E is given by $ord_2(N) = 2+2\nu/3+\lambda/6$, we find that λ is congruent 2 or 4 modulo 6 according as $\nu = 1$ or $\nu = 5$. Let L denote the subfield of $K = K_{ij}$ given by $L = \mathbb{Q}_2(\mu_3, \sqrt[3]{2}, \sqrt{x_{ij}})$, and consider the character

ψ on the 1-units of L, which by class field theory corresponds to the cyclic extension F/L of degree 4. Then ψ^2 corresponds to K/L and from the discriminant $\mathfrak{d}_{K/L}$ we can read off that $c_{\psi^2} = \pi_L^2$ or π_L^6 according as $\nu = 1$ or $\nu = 5$. Here π_L denotes a prime element of L. Similarly we obtain

$$\mathfrak{d}_{F/L} = \pi_L^{3(\nu+1)+\lambda} = c_\psi^2 \cdot c_{\psi^2},$$

hence $c_\psi = \pi_L^{2+\lambda/2}$ or $\pi_L^{6+\lambda/2}$ according as $\nu = 1$ or $\nu = 5$. Let U_n denote the group of units which are congruent 1 modulo π_L^n in L. Since taking squares sends U_7 to U_{13}, we see that ψ is trivial on U_{13}. On the other hand we know that $\lambda/2$ is congruent 1 or 2 modulo 3 according as $\nu = 1$ or $\nu = 5$, hence $c_\psi = 13$ is impossible and c_ψ must therefore divide π_L^{12}. This leaves the possibilities that $\mathrm{ord}_{\pi_L}(c_\psi) = 3,6,9,12$ for $\nu = 1$ and $\mathrm{ord}_{\pi_L}(c_\psi) = 8$ or 11 for $\nu = 5$. Once we have excluded the cases $c_\psi = \pi_L^8, \pi_L^9$ we can finish our table as follows. The values for $\mathrm{ord}_2(N)$ are immediate once we insert the remaining possible (ν,λ) in the previous formula. The minimal level M cannot have $\mathrm{ord}_2(M) = 0$ or 2 by the same argument as in the case where Φ_2 was a quaternion group of order 8. Also $\mathrm{ord}_2(M) = 5$ is impossible since this can only occur if $\mathrm{ord}_2(N) = 6$ and if the character ε with $f = g_\varepsilon$ has $\mathrm{ord}_2 c_\varepsilon = 3$ i.e. its 2-part c_2 is quadratic. But then a quadratic twist E' of E would have level N' with $\mathrm{ord}_2 N' = 5$ and $\mathrm{ord}_2(C') = \mathrm{ord}_2(C) = 4$, which is impossible by the first and the last column of our table. Note that these have already been verified completely. The remaining open entries are obvious now. We finish the proof be excluding $c_\psi = \pi_L^8$ and π_L^9. The first case is impossible since then $c_{\psi^2} = \pi_L^6$ would imply that ψ^2 is non-trivial on U_5 whereas the fact that $U_5^2 \subseteq U_8$ implies that ψ^2 is trivial on U_5. The case $c_\psi = \pi_L^9$, where $c_{\psi^2} = \pi_L^2$, is impossible since then ψ is trivial on $U_4^2 = U_8$. This completes the proof of the table for $r = 2$.

References

1. *Atkin, A.; Li, W.:* Twists of newforms and pseudo-eigenvalues of W-operators. Invent.Math.48, 221-243 (1978).

2. *Carayol, H.:* Courbes de Shimura, formes automorphes et représentations galoisiennes. Thèse, Université Paris VII, 1984.

3. *Cassels, J.W.S.; Fröhlich, A.:* Algebraic Number Theory. London-New York, Academic Press 1967.

4. *Coates, J.:* P-adic L-functions and Iwasawa's theory. In: Algebra Number Fields, Fröhlich, A.(ed.), London-New York, Academic Press 1977.

5. *Coates, J.:* Elliptic curves and Iwasawa theory. In: Modular Forms. R.A.Rankin (Editor) 1984.

6. *Coates, J.; Greenberg, R.:* Iwasawa theory for abelian varieties. (in preparation).

7. *Gelbart, S.; Jacquet, H.:* A relation between automorphic representations of GL(2) and GL(3). Ann.Sci.École Norm. Sup.11, 471-542 (1978).

8. *Greenberg, R.:* On the Birch and Swinnerton-Dyer Conjecture. Invent. Math.72, 241-265 (1983).

9. *Henniart, G.:* Représentations du groupe de Weil d'un corps local Thèse de 3^e cycle, Publ.Math.Univ. Paris-Sud, Orsay 1978

10. *Hida, H.:* A p-adic measure attached to the zeta functions associated with two elliptic modular forms. I. Invent.Math. 79, 159-195 (1985).

11. *Li, W.:* Newforms and functional equations. Math.Ann.212, 285-315 (1975).

12. *Li, W.:* L-series of Rankin type and their functional equations. Math.Ann.244, 135-166 (1979).

13. *Mazur, B.; Wiles, A.:* Class fields of abelian extensions of $\mathbb{Q}$. Invent.Math.76, 179-330 (1984).

14. *Perrin-Riou, B.:* Arithmétique des courbes elliptiques et théorie d'Iwasawa. Mém.Soc.Math. France, Suppl.112, 1984, fasc.4.

15. *Serre, J.-P.; Tate, J.:* Good reduction of abelian varieties. Ann. of Math. 88, 492-517 (1968).

16. *Serre, J.-P.:* Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). Séminaire Delange-Pisot-Poitou 1969/70, exp. 19.

17. *Serre, J.-P.:* Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent.Math.15, 259-331 (1972).

18. *Shalit, E.de:* On p-adic L-functions associated with CM elliptic curves, and arithmetical applications. Thesis, Princeton University, 1984.

19. *Shimura, G.:* On modular forms of half integral weight. Ann. of Math.97, 440-481 (1973).

20. *Shimura, G.:* On the holomorphy of certain Dirichlet series. Proc. London Math.Soc.31, 79-98 (1975).

21. *Shimura, G.:* The special values of the zeta functions associated with cusp forms. Com.Pure Appl.Math.29, 783-804 (1976).

22. *Sturm, J.:* Special values of zeta functions and Eisenstein series of half integral weight. Amer.J.Math.102, 219-240 (1980).

23. *Yager, R.I.:* On two variable p-adic L-functions. Ann.of Math.115, 411-449 (1982).