Pure and Applied Mathematics Quarterly
Volume 5, Number 4
(*Special Issue: In honor of
John Tate, Part 1 of 2*)
1311—1341, 2009

Euler Factors and Local Root Numbers for Symmetric Powers of Elliptic Curves

Neil Dummigan, Phil Martin, Mark Watkins

Dedicated to Prof. John Tate on the occasion of his 80th birthday

Abstract: For any elliptic curve E over a number field, there is, for each $n \geq 1$, a symmetric n^{th}-power L-function, defined by an Euler product, and conjecturally having a meromorphic continuation and satisfying a precise functional equation. The sign in the functional equation is conjecturally a product of local signs. Given an elliptic curve over a finite extension of some $\mathbb{Q}_p$, we calculate the associated Euler factor and local sign, for any $n \geq 1$.
Keywords: elliptic curve, root number, symmetric power L-function.

1. Introduction

Let E be an elliptic curve defined over a number field K. Let S be a finite set of places containing all the archimedean places and all places of bad reduction. For any $v \notin S$ there exists a complex number α_v of absolute value $q_v^{1/2}$ such that $\#E(\mathbb{F}_v) = 1 + q_v - \alpha_v - \overline{\alpha}_v$. For any integer $n \geq 1$ one may define the (incomplete) n^{th} symmetric power L-function $L_S(\text{Sym}^n E, s)$ to be $\prod_{v \notin S} \left(\prod_{j=0}^{n} (1 - \alpha_v^j \overline{\alpha}_v^{n-j} q_v^{-s}) \right)^{-1}$, for $\Re s > (n/2) + 1$. For $n = 1$ this is the usual L-function, the subject of the conjecture of Birch and Swinnerton-Dyer.

For curves with complex multiplication, the work of Hecke [He] establishes a functional equation and meromorphic continuation for $L_S(\text{Sym}^n E, s)$, with a pole

Received September 19, 2006.
MSC2000: 11G40.

at $s = n/2 + 1$ precisely when $4|n$. Furthermore, the distribution of $\arg \alpha_v$ for v that split is given by the measure $d\theta/\pi$ for $0 \leq \theta \leq \pi$.

It has been known for 40 years that, if, for every $n \geq 1$, $L_S(\mathrm{Sym}^n E, s - (n/2))$ has a holomorphic continuation to $\Re s \geq 1$, with no zeros on the line $\Re s = 1$, then the Sato-Tate conjecture [T2, §4], on the distribution of the arguments of the α_v, is true for E. See [Sh] for details, or [Se2, pp. I-26]. R. Taylor and his collaborators have recently proved the hypothesis in the case that K is totally real and E has at least one prime of multiplicative reduction [CHT, HSBT, Tay], and so $\arg \alpha_v$ is equi-distributed with respect to $(2/\pi)(\sin^2 \theta)\, d\theta$ for such curves. More generally, if f is a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_K)$ then there is an associated sequence of L-functions $L_S(\mathrm{Sym}^n f, s)$. The Ramanujan-Petersson conjecture (that $|\alpha_v| = q_v^{1/2}$) would follow if one knew that $L_S(\mathrm{Sym}^n f, s)$ converges absolutely for $\Re s > (n/2) + 1$. Again, see [Sh].

In this paper we are concerned with the L-functions $L(\mathrm{Sym}^n E, s)$, defined by Euler products $\prod_v L_v(\mathrm{Sym}^n E, s)$ over all finite places v of K. There is a simple formula for the Euler factor at any finite place, but at a place of bad reduction it is usually not so easy to make it explicit. As special cases of the L-functions attached to motives, there are precise conjectures about their orders of vanishing and leading terms at integer points. If one puts $\Lambda(s) = N_n^{s/2} \gamma(s) L(\mathrm{Sym}^n E, s)$, where N_n is a certain conductor and $\gamma(s)$ is a certain product of "gamma factors", to be thought of as Euler factors at archimedean places, then, again as a special case of a very general conjecture, there is supposed to be a meromorphic continuation and functional equation

$$\Lambda(s) = \pm \Lambda(n + 1 - s).$$

The sign appearing in this conjecture is specified precisely as a product, over all places v, of local signs. Again in the case that K is totally real and E has at least one prime of multiplicative reduction, this meromorphic continuation and precise functional equation have been proved by Taylor et. al. [Tay].

The Euler factors and local signs depend only on E/K_v. Those at the archimedean places are summarised in the table in 5.3 of [D3]. Here we consider only those at finite places. We start with K a finite extension of $\mathbb{Q}_p$, and an elliptic curve E/K. Attached to E is a 2-dimensional complex representation σ' of the Weil-Deligne group $\mathcal{W}'(\overline{K}/K)$, which gives rise to all the ℓ-adic representations of $\mathrm{Gal}(\overline{K}/K)$ coming from the ℓ-adic Tate modules of E, for all primes $\ell \neq p$. For

each $n \geq 1$ we have the $(n+1)$-dimensional symmetric n^{th}-power representation σ'_n of $\mathcal{W}'(\overline{K}/K)$, to which is attached an Euler factor $L(\sigma'_n, s)$ and a local sign $W(\sigma'_n)$.

The elliptic curve E/K may have good reduction, (multiplicative or) potentially multiplicative reduction, or (bad but) potentially good reduction. The latter case is subdivided according to a finite set of possibilities for the image under σ' of the inertia subgroup of the Weil group $\mathcal{W}(\overline{K}/K)$. In each case we calculate $L(\sigma'_n, s)$. This calculation is trivial for primes of good reduction, and fairly easy for primes of potentially multiplicative reduction. The case $n = 2$ was already done by Coates and Schmidt [CS], but for $n > 2$ the cases of potentially good reduction become more complicated. When n is odd and reduction is bad, we find that $L(\sigma'_n, s) = 1$ for all but a couple of cases.

We find that $W(\sigma'_n) = 1$ always for even n. For odd n, $W(\sigma'_n) = \pm 1$, by (iv) in the Proposition of §12 of [R1]. In each case we determine the possibilities for the sequence $(W(\sigma'_n))$. By comparing the answer for general n with that for $n = 1$, we find typically that all the $W(\sigma'_n)$ can be expressed in terms of $W(\sigma')$. Sometimes conductor exponents also appear in the formulas. Explicit determination of $W(\sigma')$ (starting from a Weierstrass equation for E) is easy in the cases of good and potentially multiplicative reduction ($W(\sigma') = 1$ for the former). For potentially good reduction and $p \geq 5$, it has been dealt with by Rohrlich [R3, Theorem 2]. It has been dealt with by Halberstadt [Hal] for $K = \mathbb{Q}_2$ or $\mathbb{Q}_3$, and for general K by Kobayashi [Ko] ($p = 3$) and Whitehouse [Wh] ($p = 2$).

The motivation for our calculations was extensive numerical experimentation by the last named author (for elliptic curves over $\mathbb{Q}$), testing the precise functional equation of $L(\mathrm{Sym}^n E, s)$ [MW], and his computations of critical values of these L-functions, which can be compared with the predictions of the Bloch-Kato conjecture [DW]. For both purposes, it is important to have all the Euler factors, including those attached to primes of bad reduction. When $K = \mathbb{Q}_p$, the $W(\sigma'_n)$ were found experimentally long before we were able to calculate them.

We begin in §§2 and 3 with generalities on representations of the Weil-Deligne group, and the associated L-factors, conductors and local root numbers. In §4 we turn to the representations attached to elliptic curves, and dispatch the cases of good reduction and potentially multiplicative reduction. The remaining sections deal with the case of potentially good reduction, subdivided according to the

image $\mathcal{I}$ of the inertia subgroup. In all cases we proceed by decomposing the symmetric n^{th}-power representation σ_n of the Weil group into smaller pieces, then taking a product of L-factors or root numbers for the pieces. The simplest case is where $\mathcal{I}$ is cyclic and commutes with Frobenius. Here σ_n is just a direct sum of characters. The next simplest case, treated in §6, is when $\mathcal{I}$ is cyclic but does not commute with Frobenius. Here we follow Rohrlich in applying a theorem of Fröhlich and Queyrut. In §7 we prove that $W(\sigma_n) = 1$ in all cases when n is even (in §§5-6 we give a direct proof for $\mathcal{I}$ cyclic). This uses Deligne's formula for the local signs for orthogonal representations in terms of their second Stiefel-Whitney classes. §§8–12 deal with the "exotic" cases for $p = 2$ or 3, with $\mathcal{I}$ non-cyclic (and n odd). The deepest case is when $\mathcal{I} \simeq \mathrm{SL}_2(\mathbb{F}_3)$ and K does not contain the cube roots of unity, given in §10. In this case, σ_n does not decompose as a sum from inducing characters of a quadratic extension of K, but we are able to reduce to the case that $\mathcal{I} \simeq Q_8$ by passing to a non-Galois cubic extension of K, similar to an argument of Kutzko [K].

2. Representations of the Weil-Deligne group

A convenient reference for representations of the Weil-Deligne group is [R1], which is based on [D1] and [T1]. For simplicity, we take K to be a finite extension of $\mathbb{Q}_p$, with finite residue field k of characteristic p and order q. Let $\overline{K}$ be a separable closure of K, and let the inertia group I be the kernel of the natural reduction map from $\mathrm{Gal}(\overline{K}/K)$ to $\mathrm{Gal}(\overline{k}/k)$. Let $\phi \in \mathrm{Gal}(\overline{k}/k)$ be the inverse of the Frobenius automorphism $x \mapsto x^q$. This is a topological generator for $\mathrm{Gal}(\overline{k}/k)$. Let the Weil group $\mathcal{W}(\overline{K}/K)$ be the inverse image in $\mathrm{Gal}(\overline{K}/K)$ of the subgroup of integer powers of ϕ. Let Φ be any element of $\mathcal{W}(\overline{K}/K)$ mapping to ϕ. See §§1 and 2 of [R1] for more on the Weil group, its natural topology and its representations. Using the normalisation of the Artin map $K^\times \simeq \mathcal{W}(\overline{K}/K)^{\mathrm{ab}}$ which sends a uniformiser to the image of an inverse Frobenius element (mapping to ϕ), we identify characters (not necessarily unitary) of $\mathcal{W}(\overline{K}/K)$ with characters of $K^\times$. Let ω be the unramified (i.e. trivial on I) character of $\mathcal{W}(\overline{K}/K)$ taking the value q^{-1} on any inverse Frobenius element Φ.

The Weil-Deligne group $\mathcal{W}'(\overline{K}/K)$ is a certain semi-direct product of $\mathcal{W}(\overline{K}/K)$ and $\mathbb{C}$, with the product topology. Following §3 of [R1], by a representation of $\mathcal{W}'(\overline{K}/K)$ on a finite-dimensional complex vector space V we mean a continuous

homomorphism

$$\sigma' : \mathcal{W}'(\overline{K}/K) \to \mathrm{GL}(V)$$

whose restriction to the subgroup $\mathbb{C}$ is complex analytic. This is equivalent to a pair (σ, N), where σ is a continuous representation of $\mathcal{W}(\overline{K}/K)$ on V and N is a nilpotent endomorphism of V such that

$$\sigma(g)N\sigma(g)^{-1} = \omega(g)N \quad \forall g \in \mathcal{W}(\overline{K}/K).$$

The relation between σ' and (σ, N) is such that

$$\sigma'(gz) = \sigma(g)\exp(zN) \quad \forall g \in \mathcal{W}(\overline{K}/K), z \in \mathbb{C}.$$

Let ℓ be a prime different from p. Fix a non-trivial continuous homomorphism $t_\ell : I \to \mathbb{Q}_\ell$ (which necessarily factors through the ℓ-part of the tame quotient). Also fix a choice of inverse Frobenius element $\Phi \in \mathcal{W}(\overline{K}/K)$. Consider an ℓ-adic representation of $\mathrm{Gal}(\overline{K}/K)$, i.e. a continuous homomorphism

$$\sigma'_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V_\ell),$$

where V_ℓ is a finite-dimensional vector space over $\mathbb{Q}_\ell$. By a theorem of Grothendieck (proved in the appendix to [ST]), there exists a nilpotent endomorphism N_ℓ of V_ℓ such that

$$\sigma'_\ell(i) = \exp(t_\ell(i)N_\ell)$$

for all i in some open subgroup of I. We have $N_\ell = 0$ if and only if σ'_ℓ is trivial on some open subgroup of I. Defining $\sigma_\ell : \mathcal{W}(\overline{K}/K) \to \mathrm{GL}(V_\ell)$ by

$$\sigma_\ell(g) = \sigma'_\ell(g)\exp(-t_\ell(i)N_\ell),$$

where $g = \Phi^m i$ for some $m \in \mathbb{Z}$ and $i \in I$, it may be shown that σ_ℓ is a homomorphism, trivial on some open subgroup of I. Furthermore,

$$\sigma_\ell(g)N_\ell\sigma_\ell(g)^{-1} = \omega(g)N_\ell \quad \forall g \in \mathcal{W}(\overline{K}/K).$$

Using a field embedding $\iota : \mathbb{Q}_\ell \to \mathbb{C}$, one obtains a representation $\sigma'_{\ell,\iota} = (\sigma_{\ell,\iota}, N_{\ell,\iota})$ of $\mathcal{W}'(\overline{K}/K)$. By Lemma 8.4.3 of [D1], its isomorphism class does not depend on the choices of t_ℓ and Φ, only on σ'_ℓ (and possibly ι).

3. Local Euler factors, conductors and root numbers

3.1. **Euler factors.** Let $\sigma' = (\sigma, N)$ be a representation of $\mathcal{W}'(\overline{K}/K)$ on V. Let $V^I := \{v \in V : \ \sigma(g)v = v \quad \forall g \in I\}$, $V_N := \ker N$ and $V_N^I := V^I \cap V_N$. Define

$$L(\sigma', s) = \det(1 - q^{-s}\sigma(\Phi)|V_N^I)^{-1}.$$

This is independent of the choice of inverse Frobenius element Φ.

$$(L1) \quad L(\sigma' \oplus \tau', s) = L(\sigma', s)L(\tau', s).$$

$$(L2) \quad L(\mathrm{ind}_K^L \rho', s) = L(\rho', s).$$

Here σ' and τ' are representations of $\mathcal{W}(\overline{K}/K)$ while ρ' is a representation of $\mathcal{W}(\overline{K}/L)$, with L a finite extension of K. The notation ind_K^L denotes the induction of a representation of $\mathcal{W}(\overline{K}/L)$ to one of $\mathcal{W}(\overline{K}/K)$. We also write $\rho|_L$ for the restriction of a representation ρ to a subgroup $\mathcal{W}(\overline{K}/L)$ of $\mathcal{W}(\overline{K}/K)$. The property (L1) is obvious, but (L2) is due to Artin. It is proved in Prop. 3.8 of [D1], repeated in §8 of [R1].

If $\sigma' = \sigma_{\ell,\iota}$ coming from an ℓ-adic representation σ'_ℓ of $\mathrm{Gal}(\overline{K}/K)$ as in the previous section, it is easy to show that $L(\sigma', s)$ is the "image under ι" of

$$\det(1 - q^{-s}\sigma'_\ell(\Phi)|V_\ell^I)^{-1}.$$

See §9 of [R1].

3.2. **Conductors.** Let σ' be as above. The conductor is the ideal $\mathfrak{N}(\sigma') = \pi_K^{a(\sigma')}O_K$, where π_K is a uniformising element and the integer $a(\sigma') = a(\sigma)+b(\sigma')$, where below we define both $a(\sigma)$, which depends only on the representation σ of $\mathcal{W}(\overline{K}/K)$, and $b(\sigma')$, which is zero if $N = 0$.

In fact, we have $b(\sigma') = \dim(V^I/V_N^I)$. In most cases we consider we have $N = 0$, so we shall be concerned primarily with $a(\sigma)$. This is defined by the finite sum

$$a(\sigma) = \sum_{j=0}^{\infty} \frac{|G_j|}{|G|} \dim(V/V^{G_j}),$$

where G is a finite quotient of I through which the restriction of σ to I factors, and the G_j are the higher ramification subgroups. The following hold (see §10 of[R1]).

(a1) $a(\sigma)$ is additive in short exact sequences.

(a2) Let L be a finite extension of K, with relative discriminant $\pi_K^{d(L/K)}$ and residue degree $f(L/K)$. Let ρ be a representation of $\mathcal{W}(\overline{K}/L)$. Then

$$a(\mathrm{ind}_K^L \rho) = \dim(\rho) d(L/K) + f(L/K) a(\rho).$$

(a3) Let χ be a one-dimensional representation of $\mathcal{W}(\overline{K}/K)$, viewed as a character of $K^\times$. If χ is unramified then $a(\chi) = 0$. If χ is ramified then $a(\chi)$ is the smallest positive integer m such that χ is trivial on $1 + \pi_K^m O_K$.

3.3. **Root numbers.** Let dx be a choice of Haar measure on K, and $\psi : K \to \mathbb{C}^\times$ a choice of continuous, unitary character. Then for $\sigma' = (\sigma, N)$ a representation of $\mathcal{W}'(\overline{K}/K)$ on a finite dimensional complex vector space V, there is defined an epsilon factor $\epsilon(\sigma', \psi, dx)$. This factorises as

$$\epsilon(\sigma', \psi, dx) = \epsilon(\sigma, \psi, dx) \delta(\sigma'),$$

where $\delta(\sigma') = \det(-\Phi | V^I / V_N^I)$, which is 1 if $N = 0$. We shall be concerned mainly with $\epsilon(\sigma, \psi, dx)$, which has the following properties.
(ϵ1) It is multiplicative for σ in short exact sequences.
(ϵ2) For a finite extension L/K, Haar measure dx_L, and representation ρ of $\mathcal{W}(\overline{K}/L)$,

$$\epsilon(\mathrm{ind}_K^L \rho, \psi, dx) = \epsilon(\rho, \psi \circ \mathrm{tr}_K^L, dx_L) \theta(L/K, \psi, dx, dx_L)^{\dim \rho},$$

where

$$\theta(L/K, \psi, dx, dx_L) = \frac{\epsilon(\mathrm{ind}_K^L 1_L, \psi, dx)}{\epsilon(1_L, \psi \circ \mathrm{tr}_K^L, dx_L)}.$$

(ϵ3) Let χ be a one-dimensional representation of $\mathcal{W}(\overline{K}/K)$, viewed as a character of $K^\times$. Let ψ_K be an additive unitary character of K, and $n(\psi_K)$ the largest integer with ψ_K trivial on $\pi_K^{-n(\psi_K)} O_K$. Let c be any element of valuation $n(\psi_K) + a(\chi)$.

$$\epsilon(\chi, \psi_K, dx_L) = \begin{cases} \int_{c^{-1} O_K^\times} \chi^{-1}(x) \psi_K(x)\, dx_K & \text{if } \chi \text{ is ramified;} \\ \chi \omega^{-1}(c) \int_{O_K} dx_K & \text{if } \chi \text{ is unramified.} \end{cases}$$

It is a difficult theorem of Langlands and Deligne (Theorem 4.1 of [D1]) that a function ϵ with these properties exists. Further properties are
(ϵ4) $\epsilon(\sigma, \psi_\alpha, dx) = (\det \sigma)(\alpha)\ \omega(\alpha)^{-\dim \sigma} \epsilon(\sigma, \psi, dx)$, where, for any $\alpha \in K^\times$, we have $\psi_\alpha(x) := \psi(\alpha x)$. (All additive unitary characters of K are of this form.)
(ϵ5) $\epsilon(\sigma, \psi, r\, dx) = r^{\dim \sigma} \epsilon(\sigma, \psi, dx)$.
(ϵ6) $\epsilon(\sigma \otimes \omega^s, \psi, dx) = \epsilon(\sigma, \psi, dx) q^{-s(n(\psi) \dim(\sigma) + a(\sigma))}$.

See §11 of [R1]. More generally, for χ unramified,
(ϵ6') $\epsilon(\sigma \otimes \chi, \psi, dx) = \epsilon(\sigma, \psi, dx)\chi(\pi)^{n(\psi)\dim(\sigma)+a(\sigma)}$.
This is from 3.4.6 of [T1]. Given ψ, there is a unique choice dx_ψ of Haar measure which is "self-dual" relative to ψ. Let χ be a character of $K^\times$. We shall also use the following fact, which can be viewed as a consequence of the appearance of $\epsilon(\chi, \psi, dx_\psi)$ in Tate's local functional equation for $L(\chi, s)$.
(ϵ7) $\epsilon(\chi\omega^s, \psi, dx_\psi)\epsilon(\chi^{-1}\omega^{1-s}, \psi, dx_\psi) = \chi(-1)$.

The root number associated to σ' and ψ is

$$W(\sigma', \psi) := \frac{\epsilon(\sigma', \psi, dx)}{|\epsilon(\sigma', \psi, dx)|}.$$

By (ϵ5) it does not depend on the choice of dx; note that any two Haar measures on K are (positive) multiples of one another.

For most of our purposes, we only care about W. Below we will note that W is independent of ψ for representations attached to elliptic curves; even without this fact, we could simply fix a canonical additive character ψ_K for each local field K (see p. 315 of [R3]) with $\psi_K = \psi_p \circ \mathrm{tr}_{K/\mathbb{Q}_p}$ where $\psi_p(x) = \exp\bigl(2\pi i\eta(x,p)\bigr)$ and $\eta(x,p)$ is the image of x under $\mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z} \hookrightarrow \mathbb{R}/\mathbb{Z}$.

4. The representations attached to elliptic curves

Let $K/\mathbb{Q}_p$ be a finite extension as above, and E/K an elliptic curve. For any prime $\ell \neq p$ there is a natural continuous representation of $\mathrm{Gal}(\overline{K}/K)$ on the 2-dimensional ℓ-adic vector space $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, where $T_\ell(E) = \varprojlim E[\ell^n]$ is the ℓ-adic Tate module. Let $V'_\ell := V_\ell(E)(-1) \simeq H^1_\ell(E/\overline{K}, \mathbb{Q}_\ell)$. In fact, thanks to the Weil pairing, V'_ℓ and $V_\ell(E)$ are dual as representations of $\mathrm{Gal}(\overline{K}/K)$. Choose an embedding $\iota : \mathbb{Q}_\ell \to \mathbb{C}$. Let $\sigma'_{\ell,\iota}$ be the associated representation of $\mathcal{W}'(\overline{K}/K)$.

It turns out that $\sigma'_{\ell,\iota}$ is independent of the choices of ℓ and ι, so we will denote it σ'. For any integer $n \geq 1$, let σ'_n be the symmetric n^{th} power of the representation σ'. Again from the Weil pairing, we have $\det\sigma \simeq \omega^{-1}$, and it follows that $\det\sigma_n$ is always some power of ω. It then follows from (ϵ4) that $W(\sigma'_n, \psi)$ is independent of the choice of ψ, so we just denote it $W(\sigma'_n)$.

4.1. **Potential multiplicative reduction.** In this case, it is well-known that there is a character χ of $\mathrm{Gal}(\overline{K}/K)$, with $\chi^2 = 1$, such that the twist E^χ/K

has split multiplicative reduction, so is isomorphic to a Tate curve E_t, for some $t \in K^\times$ of positive valuation. Then there is an isomorphism of abelian groups, respecting the action of $\mathrm{Gal}(\overline{K}/K)$:

$$E(\overline{K}) \simeq (\overline{K}^\times / t^{\mathbb{Z}}) \otimes \chi.$$

The character χ is trivial if E/K has split multiplicative reduction, unramified quadratic if E/K has non-split multiplicative reduction, and ramified quadratic if E/K has additive, but potentially multiplicative, reduction. This isomorphism allows us to get an explicit description of $T_\ell(E)$ with its $\mathrm{Gal}(\overline{K}/K)$-action, hence of $\sigma'_{\ell,\iota}$. One finds, as in §15 of [R1], that $\sigma'_{\ell,\iota} \simeq \chi\omega^{-1} \otimes \mathrm{sp}(2)$, where in general $\mathrm{sp}(k)$ has a basis $\{e_0, e_1, \ldots, e_{k-1}\}$ with $\sigma(g)e_j = \omega(g)^j e_j$ for all $g \in \mathcal{W}(\overline{K}/K)$ and $0 \le j \le k-1$, and $Ne_j = e_{j+1}$ for $0 \le j \le k-2$, $Ne_{k-1} = 0$.

In particular, $\sigma'_{\ell,\iota} = \sigma'$ is independent of the choices of ℓ and ι. For σ'_n we have

$$N(e_0^{n-j}e_1^j) = (n-j)e_0^{n-j-1}N(e_0)e_1^j + e_0^{n-j}je_1^{j-1}N(e_1) = (n-j)e_0^{n-j-1}e_1^{j+1}.$$

Clearly then $\sigma'_n \simeq \chi^n\omega^{-n} \otimes \mathrm{sp}(n+1)$.

Proposition 4.1. (1) *The L-function is given by*

$$L(\sigma'_n, s) = \begin{cases} (1-q^{-s})^{-1} & \text{if } n \text{ is even or reduction is split multiplicative;} \\ (1+q^{-s})^{-1} & \text{if } n \text{ is odd and reduction is non-split multiplicative;} \\ 1 & \text{if } n \text{ is odd and reduction is additive, potentially multiplicative.} \end{cases}$$

(2) *The symmetric power conductor is given by*

$$a(\sigma'_n) = \begin{cases} n & \text{if reduction is multiplicative or } n \text{ is even;} \\ (n+1)a(\chi) & \text{if reduction is additive, potentially multiplicative, and } n \text{ odd.} \end{cases}$$

(3) *Let* $w := W(\sigma'_1)$.

$$W(\sigma'_n) = \begin{cases} W(\chi)^{n+1} = w^{(n+1)/2} & \text{if } n \text{ is odd and reduction is additive,} \\ & \text{potentially multiplicative;} \\ (-\chi(\Phi))^n = w^n & \text{otherwise.} \end{cases}$$

Proof. The proposition in §8 of [R1] tells us that $L(\sigma'_n, s) = L(\chi^n\omega^{-n}, s+n) = L(\chi^n, s)$, from which (1) follows. The proposition in §10 of [R1] gives us (2), while (iii) of the corollary to the proposition in §12 of [R1] leads to (3). Note that, in the multiplicative reduction case, $a(\sigma') = b(\sigma')$ and $a(\sigma) = 0$. □

4.2. **Potential good reduction.** By the criterion of Néron-Ogg-Shafarevich, this is the case that (for any prime $\ell \neq p$) the image in $\mathrm{Aut}(V_\ell)$ of the inertia subgroup I is finite. In particular, $N_\ell = 0$. By Theorem 2(ii) of [ST], the restriction to I of σ_ℓ has kernel J independent of ℓ, and rational character, also independent of ℓ. Let $\mathcal{I} := I/J$. Let $\mathcal{G} := \mathcal{W}(\overline{K}/K)/J$, so that $\mathcal{W}(\overline{K}/K)$ acts on V through $\mathcal{G}$. By Theorem 3 of [ST], the characteristic polynomial of $\sigma'_\ell(\Phi)$ has integer coefficients, independent of ℓ. It follows from all this that $\sigma'_{\ell,\iota} = \sigma'$ is independent of ℓ and ι.

Let M be a totally ramified finite extension over which E attains good reduction (this could be the "K'" in the proof of Theorem 3 of [ST]). The characteristic polynomial referred to above is the characteristic polynomial of the Frobenius endomorphism of the reduction $\overline{E}/k_M$. Its roots are complex numbers $\alpha, \overline{\alpha}$ with $\alpha\overline{\alpha} = q$. The proof of Theorem 2 of [ST] shows that $\mathcal{I}$ injects naturally into the automorphism group of $\overline{E}/\overline{k}$. This leads to the following possibilities for $\mathcal{I}$, as noted in 5.6(a) of [Se1].

(1) $\mathcal{I}$ is trivial (case of good reduction).
(2) $\mathcal{I}$ is cyclic of order $e = 2, 3, 4$ or 6.
(3) $p = 3$ and $\mathcal{I} \simeq C_4 \ltimes C_3$, the non-abelian semi-direct product.
(4) $p = 2$ and $\mathcal{I} \simeq Q_8$, the quaternion group of order 8.
(5) $p = 2$ and $\mathcal{I} \simeq \mathrm{SL}_2(\mathbb{F}_3)$.

When $p \geq 5$ (so $\mathcal{I}$ is necessarily cyclic), $e = \frac{12}{\gcd(12, v_p(\Delta))}$, where Δ is a minimal discriminant for E/K. If also $K = \mathbb{Q}_p$, $\mathcal{G}$ is abelian precisely when $p \equiv 1 \pmod{e}$, by Proposition 2.2 of [R2].

When $K = \mathbb{Q}_p$ and $p = 2$ or 3, see §§3.3, 3.4 of [MW] for the determination of $\mathcal{I}$ and (in Case (2)) $\mathcal{G}$. This involves various conductor exponents that can be found using Tate's algorithm, and congruence conditions on Weierstrass coefficients.

In Case (1), $L(\sigma'_n, s) = \prod_{j=0}^{n}(1 - \alpha^j\overline{\alpha}^{n-j}q^{-s})^{-1}$, $a(\sigma'_n) = 0$ and $W(\sigma'_n) = 1$. In the following sections we examine the remaining cases.

Let $\beta_n(\mathcal{I})$ be the degree of the Euler factor (i.e. the dimension of $(\mathrm{Sym}^n V)^I$). Its value will be evident each time we prove the formula for an Euler factor, and may be read off from Table 1 of [MW]. When n is odd, the Euler factor is trivial ($\beta_n(\mathcal{I}) = 0$), except in the case that $\mathcal{I} = C_3$.

When $p \geq 5$ the ramification is tame and $a(\sigma_n) = n + 1 - \beta_n(\mathcal{I})$. When $p = 2$ or 3 and $K = \mathbb{Q}_p$, the $a(\sigma_n)$ may be deduced from the Tables 2 and 3 of [MW]. In fact, this still works for general K when $\mathcal{I}$ is cyclic, but for non-cyclic $\mathcal{I}$ it depends on the analysis of higher ramification groups in the appendix to [CS], which is specific to $K = \mathbb{Q}_p$. However, $a(\sigma_n)$ should be computable in any given case. Since conductor exponents are dealt with already in [MW], we shall have little more to say about them in this paper, and shall concentrate on Euler factors and local root numbers.

5. Cyclic inertia group, $\mathcal{G}$ abelian

The group $\mathcal{G}$ is generated by an inverse Frobenius element Φ and a generator i for $\mathcal{I}$. Let ζ be a fixed primitive e^{th} root of unity. Choose a basis $\{x, y\}$ for V such that $i(x) = \zeta x$ and $i(y) = \zeta^{-1} y$. (Note that $\det(\sigma) \simeq \omega^{-1}$ is trivial on I.) Let ν be the character via which $\mathcal{W}(\overline{K}/K)$ acts on x.

Proposition 5.1. (1) $L(\sigma_n', s) = \displaystyle\prod_{\substack{j=0 \\ e \mid (n-2j)}}^{n} (1 - \alpha^j \overline{\alpha}^{n-j} q^{-s})^{-1}$.

(2)
$$W(\sigma_n) = \begin{cases} \nu(-1) & \text{if } n \equiv 1 \pmod 4; \\ 1 & \text{otherwise.} \end{cases}$$

Note that if n is odd, $L(\sigma_n', s) = 1$ unless $\mathcal{I} \simeq C_3$. This follows from the impossibility of $e \mid (n - 2j)$ when n is odd but e is even.

Proof. (1) We have a basis $\{x^j y^{n-j} : 0 \leq j \leq n,\ e \mid (n-2j)\}$ for $(\mathrm{Sym}^n V)^I = (\mathrm{Sym}^n V)^I_N$. Since Φ commutes with i it preserves the eigenspaces for i on V. We can take $\Phi(x) = \alpha x$ and $\Phi(y) = \overline{\alpha} y$ without loss of generality. The result follows.

(2) The Weil group $\mathcal{W}(\overline{K}/K)$ acts on y via $\omega^{-1}\nu^{-1}$. Hence $\sigma_n \simeq \oplus_{j=0}^n \nu^{n-2j}\omega^{-j}$ and $W(\sigma_n) = \prod_{j=0}^n W(\nu^{n-2j}\omega^{-j}) = \prod_{j=0}^n W(\nu^{n-2j})$. Pairing the j and $(n-j)$ terms (except $j = n/2$ if n is even, but $W(\mathrm{id}) = 1$) and using $(\epsilon 7)$, we find
$$W(\sigma_n) = \prod_{j=0}^{[(n-1)/2]} \nu^{n-2j}(-1) = \begin{cases} \nu(-1)^{((n+1)/2)^2} & \text{if } n \text{ is odd;} \\ \nu(-1)^{(n/2)((n/2)+1)} & \text{if } n \text{ is even.} \end{cases}$$

The proposition follows.

□

Note that when $n \equiv 1 \pmod 4$, $W(\sigma_n) = W(\sigma_1)$. If $K = \mathbb{Q}_p$ and E comes from an elliptic curve over $\mathbb{Q}$, this is the same as the eigenvalue of the Atkin-Lehner involution W_p acting on the associated newform.

When $K = \mathbb{Q}_p$ and $p \geq 5$ we can compute α up to an e^{th} root of unity via first writing E as $y^2 = x^3+ax+b$, then scaling (a, b) to $(a/g^2, b/g^3)$ where $g = p^{v_p(\Delta)/6}$, and finally counting points modulo $p^{2/e}$ on the resulting curve.[1] For $p = 2, 3$ and the case of $\mathcal{I} \simeq C_2$, the curve E acquires good reduction over a quadratic extension, and we can determine α by counting points on the twist. For $K = \mathbb{Q}_2$ and $\mathcal{I} \simeq C_4$ we find that [MW, §§3.4] claims $\alpha = \zeta_8\sqrt{2}$ up to a fourth root of unity — this can be checked simply by enumerating such curves up to sufficient 2-adic precision, or by noting that the norm of α is 2 and the traces of $\zeta_4^i\alpha$ must all be integral.[2] Similarly, for $K = \mathbb{Q}_3$ and $\mathcal{I} \supseteq C_3$ we find that $\alpha = \zeta_{12}\sqrt{3}$ up to a sixth root of unity, with the above footnote being adaptable to the general case.

6. Cyclic inertia group, $\mathcal{G}$ non-abelian

The inertia subgroup $\mathcal{I}$ of $\mathcal{G}$ is necessarily normal. The group $\mathcal{G}$ is generated by an inverse Frobenius element Φ and a generator i for $\mathcal{I}$, with $\Phi^{-1}i\Phi$ a generator of $\mathcal{I}$ different from i. Hence $e \neq 2$ and (since $e = 3, 4$ or 6), $\Phi^{-1}i\Phi = i^{-1}$. Let ζ be a fixed primitive e^{th} root of unity. Choose a basis $\{x, y\}$ for V such that $i(x) = \zeta x$ and $i(y) = \zeta^{-1}y$. Since $\Phi^{-1}i\Phi = i^{-1}$, Φ swaps the eigenspaces for i, and by re-scaling if necessary, we may assume that $\Phi(x) = y$. Since $\det(\sigma) = \omega^{-1}$, necessarily $\Phi(y) = -qx$. For $0 \leq j \leq [(n-1)/2]$, we have a $\mathcal{G}$-stable subspace V_j of $\mathrm{Sym}^n V$, spanned by $x^j y^{n-j}$ and $x^{n-j}y^j$. Let $\sigma^{(j)}$ be the representation by

[1] This can be generalised to other K by taking a uniformising element $\mathfrak{p}$ in place of p — the main point is to find a curve with good reduction that is isomorphic to E over some extension.

[2] This latter argument also implies that for K with $f(K/\mathbb{Q}_2)$ odd, we must have $\alpha = \zeta_8\sqrt{q}$, while $\alpha = \zeta_4\sqrt{q}$ when $f(K/\mathbb{Q}_2)$ is even.

which $\mathcal{W}(\overline{K}/K)$ acts on V_j. Then

$$\sigma_n \simeq \begin{cases} \bigoplus_{j=0}^{[(n-1)/2]} \sigma^{(j)} & \text{if } n \text{ is odd;} \\ \chi_{-q}^{n/2} \oplus \left(\bigoplus_{j=0}^{[(n-1)/2]} \sigma^{(j)} \right) & \text{if } n \text{ is even,} \end{cases}$$

where χ_{-q} is the unramified character mapping Φ to $-q$. In the case that n is even, the one-dimensional summand is spanned by $x^{n/2}y^{n/2}$.

The subgroup $\mathcal{H}$ of index 2 in $\mathcal{G}$ generated by i and Φ^2 is abelian. This is the quotient through which $\mathcal{W}(\overline{K}/L)$ acts on V, where L is the unramified quadratic extension of K. Let ν be the character of $\mathcal{W}(\overline{K}/L)$ that maps Φ^2 to 1 and i to ζ. Let ϕ_{-q} be the unramified character of $\mathcal{W}(\overline{K}/L)$ that maps Φ^2 to $-q$. Then the restriction of $\sigma^{(j)}$ to $\mathcal{W}(\overline{K}/L)$ is a direct sum of characters $\nu^{2j-n} \otimes \phi_{-q}^n$ and $\nu^{n-2j} \otimes \phi_{-q}^n$. Clearly $\sigma^{(j)} \simeq \mathrm{ind}_K^L(\nu^{n-2j} \otimes \phi_{-q}^n)$.

Proposition 6.1. (1)

$$L(\sigma_n, s) = \begin{cases} (1-(-q)^n q^{-2s})^{-\beta_n(\mathcal{I})/2} & \textit{if } n \textit{ is odd;} \\ (1-(-q)^{n/2}q^{-s})^{-1}(1-(-q)^n q^{-2s})^{-(\beta_n(\mathcal{I})-1)/2} & \textit{if } n \textit{ is even.} \end{cases}$$

(2) *If n is even then $W(\sigma_n) = 1$. If $e = 4$, or $e = 3$ and $K = \mathbb{Q}_3$, or $e = 6$ and $p \neq 3$, then*

$$W(\sigma_n) = \begin{cases} W(\sigma) & \textit{if } n \equiv 1 \pmod 4; \\ 1 & \textit{otherwise.} \end{cases}$$

If $e = 3$ and $p \neq 3$, or $e = 6$ and $K = \mathbb{Q}_3$, then (letting $w := W(\sigma)$)

$n \pmod{12}$	1	3	5	7	9	11
$W(\sigma_n)$	w	-1	$-w$	-1	w	1

In the remaining cases ($e = 3$ or 6 with $p = 3$ but $K \neq \mathbb{Q}_3$), $W(\sigma_n)$ (for n odd) is given by the tables in the proof below, and is determined by w and $a(\sigma)$.

Note that if n is odd, $\beta_n(\mathcal{I}) = 0$ and $L(\sigma'_n, s) = 1$ unless $\mathcal{I} \simeq C_3$. In the proof below, this follows from the impossibility of $e \mid (n-2j)$ when n is odd but e is even.

Proof. (1)

$$(\mathrm{Sym}^n V)^I \simeq \begin{cases} \bigoplus_{\substack{j=0 \\ e|(n-2j)}}^{[(n-1)/2]} \sigma^{(j)} & \text{if } n \text{ is odd;} \\ \chi_{-q}^{n/2} \oplus \left(\bigoplus_{\substack{j=0, \\ e|(n-2j)}}^{[(n-1)/2]} \sigma^{(j)} \right) & \text{if } n \text{ is even.} \end{cases}$$

We have selected the summands such that ν^{n-2j} is trivial. For all these summands, $\sigma^{(j)} \simeq \mathrm{ind}_K^L \phi_{-q}^n$. Using (L1) and (L2),

$$L(\sigma_n, s) = \begin{cases} \prod_{\substack{j=0 \\ e|(n-2j)}}^{[(n-1)/2]} L(\sigma^{(j)}, s) & \text{if } n \text{ is odd;} \\ L(\chi_{-q}^{n/2}, s) \prod_{\substack{j=0 \\ e|(n-2j)}}^{[(n-1)/2]} L(\sigma^{(j)}, s) & \text{if } n \text{ is even} \end{cases}$$

$$= \begin{cases} \prod_{\substack{j=0 \\ e|(n-2j)}}^{[(n-1)/2]} L(\phi_{-q}^n, s) & \text{if } n \text{ is odd;} \\ L(\chi_{-q}^{n/2}, s) \prod_{\substack{j=0 \\ e|(n-2j)}}^{[(n-1)/2]} L(\phi_{-q}^n, s) & \text{if } n \text{ is even.} \end{cases}$$

The result follows directly from these.

(2) We choose ψ_K as indicated at the end of Section 3.3, so that we have $n(\psi_K) = d(K/\mathbb{Q}_p)/f(K/\mathbb{Q}_p)$. This choice is important, as it enables us to apply Theorem 3 of [FQ] below. By $(\epsilon 3)$ or $(\epsilon 6')$, we have $W(\chi_{-q}^{n/2}) = \big((-1)^{n(\psi_K)}\big)^{(n/2)}$ for n even. We let $A_n^\psi = W(\chi_{-q}^{n/2})$ for n even and $A_n^\psi = 1$ for n odd.

Hence, whether n is odd or even,

$$W(\sigma_n) = A_n^\psi \prod_{j=0}^{[(n-1)/2]} W(\sigma^{(j)}) = A_n^\psi \prod_{j=0}^{[(n-1)/2]} W(\mathrm{ind}_K^L(\nu^{n-2j} \otimes \phi_{-q}^n))$$

$$= A_n^{\psi} \prod_{j=0}^{[(n-1)/2]} \left(W(\nu^{n-2j}) \big((-1)^n\big)^{n(\psi_L)+a(\nu^{n-2j})} \frac{W(\mathrm{ind}_K^L 1_L)}{W(1_L)} \right),$$

by (ϵ2) and (ϵ6'). Now $\mathrm{ind}_K^L 1_L \simeq 1_K + \eta$, where η is the quadratic character attached to L/K. By (ϵ3), we get that $W(1_L) = W(1_K) = 1$, and also $W(\eta) = (-1)^{n(\psi_K)}$. Since L/K is unramified we have $n(\psi_K) = n(\psi_L)$, so

$$W(\sigma_n) = (-1)^{f_n n(\psi_K)} \prod_{j=0}^{[(n-1)/2]} \left(W(\nu^{n-2j}) \big((-1)^n\big)^{a(\nu^{n-2j})} \right),$$

where we have that $f_n = (n/2) + (n+1)\cdot(n/2)$ when n is even while $f_n = (n+1)\cdot(n+1)/2$ when n is odd. In both cases we have that f_n is even, so that this leading term can be omitted.

What follows is inspired by the proof of Proposition 2(v) in [R2]. One easily checks that the determinant of $\mathrm{ind}_K^L \nu^{n-2j}$ is η. According to the formula given in the proof of Proposition 1.2 of [D1], $\det(\mathrm{ind}_K^L \nu^{n-2j}) = \eta \cdot (\nu^{n-2j} \circ \mathrm{Ver})$, where $\mathrm{Ver} : \mathcal{G}^{\mathrm{ab}} \to \mathcal{H}^{\mathrm{ab}}$ is the transfer map. Hence $\nu^{n-2j} \circ \mathrm{Ver}$ is trivial. Using the local reciprocity maps to identify $\mathcal{G}^{\mathrm{ab}}$ with $K^\times$ and $\mathcal{H}^{\mathrm{ab}}$ with $L^\times$, Ver is compatible with inclusion of $K^\times$ in $L^\times$ (5.9 in Chapter IV of [N]). Hence $\nu^{n-2j}|_{K^\times}$ is trivial. By Theorem 3 of [FQ], our choice of ψ_L gives us $W(\nu^{n-2j}) = \nu^{n-2j}(u)$, where $u \in L$ is any element such that $u^2 \in K$ and $L = K(u)$. Hence

$$W(\sigma_n) = \prod_{j=0}^{[(n-1)/2]} \left(\nu^{n-2j}(u) \big((-1)^n\big)^{a(\nu^{n-2j})} \right).$$

Now $u^2 \in K^\times$ and $\nu|_{K^\times}$ is trivial, so $\nu^2(u) = 1$. Hence

$$W(\sigma_n) = \begin{cases} 1 & \text{if } n \text{ is even;} \\ \nu(u)(-1)^{\sum a(\nu^{n-2j})} & \text{if } n \equiv 1 \pmod 4; \\ (-1)^{\sum a(\nu^{n-2j})} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Henceforth suppose that n is odd.

Case e = 4. All odd powers of ν have the same conductor, so $\sum_{j=0}^{(n-1)/2} a(\nu^{n-2j}) = a(\nu)(n+1)/2$. Hence

$$W(\sigma_n) = \begin{cases} \nu(u)(-1)^{a(\nu)} & \text{if } n \equiv 1 \pmod 4; \\ 1 & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

If $p \neq 2$ then $a(\nu) = 1$. By (a2), $a(\sigma) = 2a(\nu)$. This allows us to determine $a(\nu)$ even if $p = 2$, as long as we know the conductor of E (which may be calculated using Tate's algorithm given a Weierstrass equation, and for a modular elliptic curve $E/\mathbb{Q}$, is the level N). But this is not really necessary if we know $W(\sigma)$, since what we have found overall is that

$$W(\sigma_n) = \begin{cases} W(\sigma) & \text{if } n \equiv 1 \pmod 4; \\ 1 & \text{otherwise.} \end{cases}$$

Case e = 3. This time

$$a(\nu^r) = \begin{cases} a(\nu) & \text{if } r \equiv 1 \text{ or } 5 \pmod 6; \\ 0 & \text{if } r \equiv 3 \pmod 6. \end{cases}$$

Letting $a = a(\nu)$ and $w = W(\sigma)$, we find the following.

$n \pmod{12}$	1	3	5	7	9	11
$W(\sigma_n)$	w	$(-1)^a$	$(-1)^a w$	$(-1)^a$	w	1

Again, a may be determined by $a(\sigma) = 2a$, if one knows the conductor of E. If $p \neq 3$ then $a = 1$. If $p = 3$ and $K = \mathbb{Q}_3$ then necessarily $a = 2$ (so that $a(\sigma) = 2a = 4$), see §3.3 of [MW].

Case e = 6. If we let $w = W(\sigma), a = a(\nu)$ and $b = a(\nu^3)$ (a quadratic character) then we find the following.

$n \pmod{12}$	1	3	5	7	9	11
$W(\sigma_n)$	w	$(-1)^{a+b}$	$(-1)^{a+b} w$	$(-1)^{a+b}$	w	1

If $p \neq 2$ then $b = 1$. If $p \geq 5$ then also $a = 1$. If $p = 2$ then surjectivity of the cubing map on the 1-units of K implies that $a = b$. If $p = 3$ and $K = \mathbb{Q}_3$ then necessarily $a = 2$ (so that $a(\sigma) = 2a = 4$), see §3.3 of [MW].

□

When $\mathcal{I}$ is cyclic, whether or not $\mathcal{G}$ is abelian, if $K = \mathbb{Q}_p$ and $p \geq 5$ then $w = W(\sigma)$ is determined by Proposition 2 of [R2]:

$$w = \begin{cases} \left(\frac{-1}{p}\right) & \text{if } e = 2 \text{ or } 6; \\ \left(\frac{-3}{p}\right) & \text{if } e = 3; \\ \left(\frac{-2}{p}\right) & \text{if } e = 4. \end{cases}$$

To complement the results of this section and the last, we now calculate w when $\mathcal{I}$ is cyclic and $K = \mathbb{Q}_3$.

Case $\mathcal{G}$ abelian. We have $w = \nu(-1)$. If $e = 2$ then $w = \left(\frac{-1}{3}\right) = -1$. Since $(-1)^2 = 1$, $\nu^2(-1) = 1$, so $w = \nu^3(-1)$. Hence if $e = 3$ then $w = 1$. If $e = 6$ then $w = \left(\frac{-1}{3}\right) = -1$. The case $e = 4$ cannot occur, as $\mathbb{Z}_3^\times$ has no order 4 characters.

Case $\mathcal{G}$ non-abelian. The case $e = 2$ does not occur. Recall that $w = \nu(u)(-1)^a$. Since $u^2 \in \mathbb{Q}_3$ and $\nu|_{\mathbb{Q}_3^\times}$ is trivial, $w = \nu^3(u)(-1)^a$. If $e = 3$ then $\nu^3(u) = 1$ and $a = 2$ so $w = 1$. Since $L/\mathbb{Q}_3$ is unramified, we may take u to be a unit, in $O_L^\times$. Whether $e = 6$ or 4, the character ν^3, restricted to $O_L^\times$, must factor through $\mathbb{F}_9^\times$, which is a cyclic group of order 8. Let g be a generator. Then so is any odd power of g. Without loss of generality, the residue class of u is g^2. (It must be something whose square is in $\mathbb{F}_3^\times = \langle g^4 \rangle$, but that is not itself in $\mathbb{F}_3^\times$.) If $e = 6$ then the quadratic character ν^3 sends g to -1, so $\nu^3(u) = 1$. Since $a = 2$, we find $w = 1$. If $e = 4$ then $\nu(g)$ has order 4, so $\nu(u) = -1$. But now $a = 1$, so again $w = 1$.

Summary for $\mathcal{I}$ cyclic, $\mathbf{K} = \mathbb{Q}_3$. If $e = 2$ then $W(\sigma_n) = (-1)^{(n+1)/2}$ (for all odd n). If $e = 3$ or 4 then $W(\sigma_n) = 1$ for all n. If $e = 6$ then

n (mod 12)	1	3	5	7	9	11
$W(\sigma_n)$, $\mathcal{G}$ abelian	-1	$+1$	-1	$+1$	-1	$+1$
$W(\sigma_n)$, $\mathcal{G}$ non-abelian	$+1$	-1	-1	-1	$+1$	$+1$

This agrees perfectly with experiment; see Table 5 of [MW].

7. Signs for even symmetric powers

Before turning to the cases of non-cyclic inertia group, we first note that we can show $W(\sigma_n) = +1$ for all even symmetric powers via a simple adaption of an argument that traces back to Deligne's re-interpretation of orthogonal root numbers in terms of Stiefel-Whitney classes, and its subsequent use first by Rohrlich [R3] and then by Prasad and Ramakrishnan [PR] for various tensor product representations.

Proposition 7.1. *$W(\sigma_n) = +1$ for all even n.*

Proof. Let $\sigma^\xi = \sigma \otimes \omega^{1/2}$, so that $\det(\sigma^\xi) = 1$. By (ϵ6) we have $W(\sigma^\xi) = W(\sigma)$. For all $n \geq 1$ let $\sigma_n^\xi = \mathrm{Sym}^n(\sigma^\xi)$. The Weil pairing gives a symplectic form on V, the space of the representation σ, invariant under the action of $\mathcal{W}(\overline{K}/K)$ via σ^ξ. For even n, this induces a natural $\mathcal{W}(\overline{K}/K)$-invariant symmetric bilinear form on $\mathrm{Sym}^n V$. Hence we may regard $\sigma_n^\xi : \mathcal{W}(\overline{K}/K) \to \mathrm{SO}(n+1, \mathbb{C})$. But this factors through $\sigma^\xi : \mathcal{W}(\overline{K}/K) \to \mathrm{SL}(2, \mathbb{C})$ via the symmetric n^{th}-power representation. Since $\mathrm{SL}(2, \mathbb{C})$ is simply-connected, this forces σ_n^ξ to lift to the simply-connected double cover $\mathrm{Spin}(n+1, \mathbb{C})$ of $\mathrm{SO}(n+1, \mathbb{C})$, hence its second Stiefel-Whitney class is trivial, so by Proposition 5.2 of [D2], $W(\sigma_n^\xi) = 1$. (One may subtract a multiple of the trivial representation to get something virtual of dimension 0.) □

8. $p = 2$ the Q_8 case, $f(K/\mathbb{Q}_2)$ odd

8.1. **Setup.** The quaternion group Q_8 has generators τ, λ of order 4, with $\tau^2 = \lambda^2$ and $\lambda^{-1}\tau\lambda = \tau^{-1}$. Choose a basis $\{x, y\}$ for V such that $\tau(x) = ix$ and $\tau(y) = -iy$ Since $\lambda^{-1}\tau\lambda = \tau^{-1}$, it follows that λ swaps the eigenspaces of τ. We can choose the basis in such a way that $\lambda(x) = y$ and $\lambda(y) = -x$. By Corollary 2(a) to Theorem 2 of [ST], $\mathcal{I}$ acts faithfully on $E[3]$. The Galois group of $K(E[3])/K$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ and contains the unramified extension $K(\mu_3)$ (since $\det \sigma = \omega^{-1}$). Since $f(K/\mathbb{Q}_2)$ is odd, this is a quadratic extension of K. On the other hand, $\mathrm{GL}_2(\mathbb{F}_3)$ has no cyclic quotient of order 6, so $K(\mu_3)$ must be the maximal unramified subextension of $K(E[3])/K$. Hence the image of $\mathcal{G}$ in $\mathrm{Aut}(E[3])$ must be a Sylow 2-subgroup, isomorphic to the semi-dihedral group SD_{16}. (The argument above is adapted from the top of p. 153 of [CS], where a dihedral group is used by mistake.) Any inverse Frobenius element Φ normalises $\mathcal{I}$, so relations holding in $\mathrm{Aut}(E[3])$ lift to $\mathcal{G}$. We may choose Φ in such a way

that Φ commutes with τ but $\lambda^{-1}\Phi\lambda = \Phi\tau^{-1}$ (equivalently $\Phi^{-1}\lambda\Phi = \lambda\tau$). Let α be such that $\Phi(x) = \alpha x$ (then $\Phi(y) = \overline{\alpha}y$). Let β be the complex number of absolute value 1 such that $\alpha = \beta q^{1/2}$. Since $\lambda^{-1}\Phi\lambda = \Phi\tau^{-1}$, we have $\overline{\alpha} = \alpha/i$, so $\beta = e^{\pi i/4}$ or $e^{5\pi i/4}$. In particular, $\beta^2 = i$. Replacing Φ by $\Phi\lambda^2$ if necessary, we may assume that $\beta = e^{\pi i/4} =: \zeta_8$.

8.2. **Character calculations.** In the remainder of this paper, the following formula for the trace of a symmetric power of a 2×2 matrix (applied to $A = \sigma^{\xi}(g)$ with $g \in \mathcal{W}(\overline{K}/K)$) will sometimes be useful (with the convention that $0^0 = 1$):

$$\operatorname{tr}(\operatorname{Sym}^n A) = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} \operatorname{tr}(A)^{n-2k}(-\det A)^k. \tag{1}$$

As in the previous section, we re-normalise σ by letting $\xi = \omega^{1/2}$ be the unramified character that is $1/\sqrt{q}$ on an inverse Frobenius element Φ, and consider $\sigma^{\xi} = \sigma \otimes \xi$. The above analysis and computation of β shows that the action of the Weil group on σ^{ξ} factors through the quaternionic 2-extension Q_{16} of Q_8 given by adjoining $\mu = \operatorname{diag}(\zeta_8, \zeta_8^{-1})$ so that $\mu^2 = \tau$. We give the character table for Q_{16}.

TABLE 1. Character table of Q_{16}

reps	id	λ^2	μ^2	λ	$\mu\lambda$	μ	μ^3
size	1	1	2	4	4	2	2
order	1	2	4	4	4	8	8
id	1	1	1	1	1	1	1
ρ_c	1	1	1	-1	-1	1	1
ρ_u	1	1	1	1	-1	-1	-1
ρ_q	1	1	1	-1	1	-1	-1
κ	2	2	-2	0	0	0	0
σ^{ξ}	2	-2	0	0	0	$\sqrt{2}$	$-\sqrt{2}$
$\bar{\sigma}^{\xi}$	2	-2	0	0	0	$-\sqrt{2}$	$\sqrt{2}$

We note that Q_{16} becomes the Klein 4-group under abelianisation. The character ρ_u is unramified, as it takes the value 1 on the generators λ and μ^2 of the subgroup $\mathcal{I} \simeq Q_8$ inside Q_{16}. The character ρ_c corresponds to the C_8 subgroup of Q_{16}, while ρ_q corresponds to the other (ramified) Q_8 subgroup.

In Table 2 we list the decomposition of $\sigma_n^\xi := \sigma_n \otimes \xi^n$ for the various symmetric powers. These follow immediately from the trace formula (1) for symmetric powers and the 1-1 correspondence between characters and representations. Note that ρ_u and ρ_q always appear together, as σ_n does not distinguish the conjugacy classes represented by λ and $\mu\lambda$, while ρ_u and ρ_q agree outside those two conjugacy classes, and each has character values summing to zero over the two classes. Note also that in the odd symmetric powers only the symplectic irreducible representations occur, while in the even symmetric powers only the orthogonal irreducible representations occur.

TABLE 2. Decomposition of σ_n^ξ

$n \equiv 1 \pmod 8$:	σ^ξ	$\oplus$	$[(n-1)/4]\ (\sigma^\xi \oplus \bar\sigma^\xi)$
$n \equiv 5 \pmod 8$:	$\bar\sigma^\xi$	$\oplus$	$[(n-1)/4]\ (\sigma^\xi \oplus \bar\sigma^\xi)$
$n \equiv 3 \pmod 4$:			$[(n+1)/4]\ (\sigma^\xi \oplus \bar\sigma^\xi)$
$n \equiv 0 \pmod 8$:	id	$\oplus$	$[n/8]\ (\mathrm{id} \oplus \rho_c \oplus \rho_q \oplus \rho_u \oplus 2\kappa)$
$n \equiv 2 \pmod 8$:	$\rho_c \oplus \kappa$	$\oplus$	$[(n-2)/8]\ (\mathrm{id} \oplus \rho_c \oplus \rho_q \oplus \rho_u \oplus 2\kappa)$
$n \equiv 4 \pmod 8$:	$\mathrm{id} \oplus \rho_u \oplus \rho_q \oplus \kappa$	$\oplus$	$[(n-4)/8]\ (\mathrm{id} \oplus \rho_c \oplus \rho_q \oplus \rho_u \oplus 2\kappa)$
$n \equiv 6 \pmod 8$:	$\rho_u \oplus 2\kappa \oplus \rho_c \oplus \rho_q$	$\oplus$	$[(n-6)/8]\ (\mathrm{id} \oplus \rho_c \oplus \rho_q \oplus \rho_u \oplus 2\kappa)$

These decompositions may also be obtained by a careful examination of the $V_j := \langle x^j y^{n-j}, x^{n-j} y^j \rangle$, some of which are irreducible while others break up into one-dimensional pieces.

8.3. *L*-function.

Proposition 8.1.

$$L(\sigma_n, s) = \begin{cases} 1 & \text{if } n \text{ is odd;} \\ \left(1 - (-q)^{n/2}/q^s\right)^{-a_n} \left(1 + (-q)^{n/2}/q^s\right)^{-b_n} & \text{if } n \text{ is even,} \end{cases}$$

where $a_n, b_n = \lceil \beta_n(\mathcal{I})/2 \rceil, \lfloor \beta_n(\mathcal{I})/2 \rfloor$ *respectively.*

Proof. The only irreducible representations of Q_{16} having a trivial component when restricted to $\mathcal{I}$ are id and ρ_u. Remembering the twist, and recalling that the image of Φ in Q_{16} is μ, id corresponds to factors of the L-function with $q^{n/2}$ as an eigenvalue, while ρ_u corresponds to those with $-q^{n/2}$ as an eigenvalue. The multiplicities may be read off from the table. □

The $-q$ is natural, since $-q \equiv 1 \pmod 3$, so that a_n is the dimension of the fixed space for SD_{16} acting on $\mathrm{Sym}^n(E[3])$.

8.4. **Signs for odd powers.**

Proposition 8.2. *For n odd, $W(\sigma_n) = W(\sigma)^{(n+1)/2}$ except when $n \equiv 3 \pmod 8$ and $a(\sigma)$ is odd.*

Proof. We have $\bar\sigma^\xi = \sigma^\xi \otimes \rho_u$ and so, since ρ_u is unramified, from $(\epsilon 6')$ we get $W(\bar\sigma^\xi) = W(\sigma \otimes \rho_u) = W(\sigma)(-1)^{a(\sigma)}$ (note that $\dim \sigma = 2$, so the parity of $n(\psi)$ does not matter). Since σ_n^ξ has $(n+1)/2$ irreducible factors, each isomorphic to σ^ξ or $\bar\sigma^\xi$, we have

$$W(\sigma_n) = W(\sigma)^{(n+1)/2}(-1)^{e_n a(\sigma)} \qquad \text{for odd } n,$$

where e_n is the multiplicity of $\bar\sigma^\xi$ in the irreducible decomposition of σ_n; this e_n is odd exactly when $n \equiv 3 \pmod 8$. □

This agrees with experiment for $K = \mathbb{Q}_2$, see §4.3 of [MW].

9. $p = 2$, THE Q_8 CASE, $f(K/\mathbb{Q}_2)$ EVEN

Since $\det(\sigma(\Phi)) = q = 2^{f(K/\mathbb{Q}_2)} \equiv 1 \pmod 3$, the image of $\mathcal{W}(\overline{K}/K)$ in $\mathrm{Aut}(E[3])$ is contained in $\mathrm{SL}_2(\mathbb{F}_3)$, so is either Q_8 or $\mathrm{SL}_2(\mathbb{F}_3)$. The image is Q_8 precisely when the resolvent cubic $x^3 - \Delta/3^3$ of the (irreducible) 3-torsion polynomial F_3 splits — this corresponds to the case where the Galois group of F_3 is V_4, and this group is A_4 when the image is $\mathrm{SL}_2(\mathbb{F}_3)$ (note that the discriminant of F_3 is square and the cube roots of unity are contained in K, as $f(K/\mathbb{Q}_2)$ is even). An example of the latter is the curve $Y^2 = X^3 + X + 2\zeta_3$ over $\mathbb{Q}_2(\zeta_3)$; the discriminant $\Delta = 2^6(26 + 27\zeta_3)$ becomes a cube upon making the unramified extension to $\mathbb{Q}_2(\zeta_9)$.

9.1. L**-function.**

Proposition 9.1. (1) *If the image of $\mathcal{W}(\overline{K}/K)$ in $\mathrm{Aut}(E[3])$ is Q_8 then*

$$L(\sigma_n, s) = \begin{cases} 1 & \text{if } n \text{ is odd;} \\ \left(1 - q^{n/2}/q^s\right)^{-\beta_n(\mathcal{I})} & \text{if } n \text{ is even.} \end{cases}$$

(2) *If the image of* $\mathcal{W}(\overline{K}/K)$ *in* $\mathrm{Aut}(E[3])$ *is* $\mathrm{SL}_2(\mathbb{F}_3)$ *then*

$$L(\sigma_n, s) = \begin{cases} 1 & \text{if } n \text{ is odd;} \\ \left(1-(q^3)^{(n/2)-s}\right)^{-\lfloor \beta_n(\mathcal{I})/3 \rfloor}(1-q^{(n/2)-s})^{-1} & \text{if } n \equiv 0 \pmod 6; \\ \left(1-(q^3)^{(n/2)-s}\right)^{-\beta_n(\mathcal{I})/3} & \text{if } n \equiv 2 \pmod 6; \\ \left(1-(q^3)^{(n/2)-s}\right)^{-\lceil \beta_n(\mathcal{I})/3 \rceil}(1-q^{(n/2)-s}) & \text{if } n \equiv 4 \pmod 6; \end{cases}$$

Proof. (1) The statement for n odd is clear, as the $\mathcal{I}$-fixed subspace of $\mathrm{Sym}^n V$ is trivial in that case. (Looking at Table 1, the character values for an odd power of σ^ξ, summed over the subgroup Q_8, produce 0.) To deal with even n, we may choose Φ to act trivially on $E[3]$ (adjusting by an element of $\mathcal{I}$ if necessary). In particular, the image of Φ in $\mathrm{Aut}(E[3])$ commutes with the image of each element of $\mathcal{I}$. These relations lift to $\mathcal{G}$, as before. Looking at the matrices representing τ and λ on V (via σ), the Φ-representing matrix is a scalar, necessarily $\pm q^{1/2}$ since its determinant is q. Hence, for even n, Φ acts as $q^{n/2}$ on $\mathrm{Sym}^n V$, in particular on its $\mathcal{I}$-fixed part.

(2) We may choose Φ so that Φ^3 acts as the identity on $E[3]$, since the non-trivial cosets of Q_8 in $\mathrm{SL}_2(\mathbb{F}_3)$ are represented by elements of order 3. As above, this forces Φ^3 to act as a scalar on V. Replacing Φ by $\lambda^2\Phi$ if necessary, we may assume that $\sigma^\xi(\Phi^3)$ is the identity, where $\sigma^\xi = \sigma \otimes \omega^{1/2}$. Hence σ^ξ factors through the quotient $Q_8 \rtimes C_3 \cong \mathrm{SL}_2(\mathbb{F}_3)$. There are three linear characters of $\mathrm{SL}_2(\mathbb{F}_3)$ that are trivial on the Q_8 subgroup, and thus correspond to $\mathcal{I}$-fixed subspaces. Referring to the character table of $\mathrm{SL}_2(\mathbb{F}_3)$ below, we have $\sigma_n^\xi = a_n \cdot \mathrm{id} \oplus b_n \cdot (\chi \oplus \bar{\chi}) \oplus c_n \cdot \kappa$, where χ and its conjugate are trivial on Q_8 and take the value of a primitive cube root of unity (ζ_3 or ζ_3^2) on a Frobenius element. We have that $c_n = \lceil n/4 \rceil$, while

$$a_n = \begin{cases} 1 + \lfloor n/12 \rfloor & n \equiv 0, 6, 8 \pmod{12} \\ \lfloor n/12 \rfloor & n \equiv 2, 4, 10 \pmod{12}, \end{cases}$$

$$b_n = \begin{cases} 1 + \lfloor n/12 \rfloor & n \equiv 4, 8, 10 \pmod{12} \\ \lfloor n/12 \rfloor & n \equiv 0, 2, 6 \pmod{12}. \end{cases}$$

Thus we get $(1-q^{n/2}/q^s)^{-a_n}(1-\zeta_3 q^{n/2}/q^s)^{-b_n}(1-\zeta_3^2 q^{n/2}/q^s)^{-b_n}$ for the L-function, which can be rewritten as above.

□

9.2. **Signs for odd powers.**

Proposition 9.2. *$W(\sigma_n) = W(\sigma)^{(n+1)/2}$ for all odd $n \geq 1$.*

Proof. (1) First suppose that the image of $\mathcal{W}(\overline{K}/K)$ in $\mathrm{Aut}(E[3])$ is Q_8. As σ^ξ is the only symplectic irreducible representation of Q_8, we get that $\sigma_n^\xi = \left(\frac{n+1}{2}\right)\sigma^\xi$ for odd n, so that $W(\sigma_n) = W(\sigma)^{(n+1)/2}$.

(2) If the image of $\mathcal{W}(\overline{K}/K)$ in $\mathrm{Aut}(E[3])$ is $\mathrm{SL}_2(\mathbb{F}_3)$, let K'/K be the unramified cubic extension. This is a Galois extension, with associated characters id, χ and χ^{-1}, say, and $\mathrm{ind}_K^{K'}(\sigma_n|_{K'}) \simeq \sigma_n \oplus (\sigma_n \otimes \chi) \oplus (\sigma_n \otimes \chi^{-1})$. Using $(\epsilon 2)$ and $(\epsilon 6')$, we confirm readily that $W(\sigma_n) = W(\sigma_n|_{K'})$. This puts us in the other case.

□

TABLE 3. Character table of $\mathrm{SL}_2(\mathbb{F}_3)$

	id	λ^2	υ	υ^{-1}	λ	$(\upsilon\tau)^{-1}$	$\upsilon\tau$
size	1	1	4	4	6	4	4
order	1	2	3	3	4	6	6
id	1	1	1	1	1	1	1
χ	1	1	ζ_3	ζ_3^2	1	ζ_3^2	ζ_3
$\bar{\chi}$	1	1	ζ_3^2	ζ_3	1	ζ_3	ζ_3^2
$\sigma^\xi\|_{K_u}$	2	−2	−1	−1	0	1	1
$\sigma^\xi\|_{K_u} \otimes \chi$	2	−2	$-\zeta_3$	$-\zeta_3^2$	0	ζ_3^2	ζ_3
$\sigma^\xi\|_{K_u} \otimes \bar{\chi}$	2	−2	$-\zeta_3^2$	$-\zeta_3$	0	ζ_3	ζ_3^2
κ	3	3	0	0	−1	0	0

10. $p = 2$, THE $\mathrm{SL}_2(\mathbb{F}_3)$ CASE

Note that we have Q_8 as a normal subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$, with an additional action (in the previously given basis) of

$$\upsilon = \frac{1}{\sqrt{2}}\begin{pmatrix} \zeta_8^3 & \zeta_8^3 \\ \zeta_8 & \zeta_8^5 \end{pmatrix},$$

which has order 3. Since $\det(\sigma(\Phi)) = q = 2^{f(K/\mathbb{Q}_2)} \equiv (-1)^{f(K/\mathbb{Q}_2)} \pmod 3$, the image of $\mathcal{W}(\overline{K}/K)$ in $\mathrm{Aut}(E[3])$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$ if $f(K/\mathbb{Q}_2)$ is even, and

$\mathrm{GL}_2(\mathbb{F}_3)$ if $f(K/\mathbb{Q}_2)$ is odd. The result for the L-function is exactly the same as in Propositions 8.1 and 9.1(1) (with $\beta_n(\mathcal{I})$ for $\mathrm{SL}_2(\mathbb{F}_3)$, as in Table 1 of [MW], being used), depending on the parity of $f(K/\mathbb{Q}_2)$. For $f(K/\mathbb{Q}_2)$ even, the argument is identical to that in the proof of Proposition 9.1(1). For $f(K/\mathbb{Q}_2)$ odd, we imitate the proof of Proposition 8.1. We consider the 2-extension G_{48} of $\mathrm{SL}_2(\mathbb{F}_3)$ given by adjoining $\mu = \mathrm{diag}(\zeta_8, \zeta_8^{-1})$, and since $\mathcal{I}$ is normal of index 2 in G_{48}, we see that there are two irreducible representations of G_{48} that are trivial upon restricting to $\mathcal{I}$, with the eigenvalues being $q^{n/2}$ and $-q^{n/2}$. A character calculation then gives the multiplicity of these representations in the decomposition of σ_n^ξ.

10.1. **Signs for odd powers, $f(K/\mathbb{Q}_2)$ odd.** Presumably we could work with some 2-extension of $\mathrm{SL}_2(\mathbb{F}_3)$ in this case, but we argue differently. Let K_u be the unramified quadratic extension of K. Let K'_u/K_u be the cubic extension[3] corresponding to the Q_8 subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$, and let K'/K be any (necessarily non-Galois) cubic extension whose compositum with K_u is K'_u. We let $\chi_{K_u}^{K'_u}$ be a cubic character associated to the extension K'_u/K_u. Again we let $\sigma^\xi = \sigma \otimes \omega^{1/2}$, and relate $W(\sigma_n^\xi)$ to $W(\sigma_n^\xi|_{K'})$ via work of Kutzko; since the inertia group upon restriction to K' is Q_8, this will reduce us to the previous case. However, to apply the proposition of Kutzko directly, we must ensure that K contains the cube roots of unity, and this leads us naturally to restrict σ_n^ξ to the Weil group for K_u. Since this restriction squares the Frobenius element, we get (by a similar argument to the proof of Proposition 9.1(1)) that $\sigma_n^\xi|_{K_u}$ is a representation of $\mathrm{SL}_2(\mathbb{F}_3)$. Here is our generalization of Kutzko's result:

Lemma 10.1. *For odd n we have $W(\sigma_n|_{K_u}) = \zeta W(\sigma_n|_{K_u} \otimes \chi_{K_u}^{K'_u})$ for some ζ (possibly depending on n) with $\zeta^3 = 1$. By symmetry, the same is true when twisting by the conjugate character.*

Proof. For odd n, the character table for $\mathrm{SL}_2(\mathbb{F}_3)$ implies that $\sigma_n^\xi|_{K_u}$ decomposes as a sum of irreducible 2-dimensional representations given by $\sigma^\xi|_{K_u}$ and its twists by both $\chi_{K_u}^{K'_u}$ and its conjugate. In more detail, looking at Table 3, it is clear that the inner product of κ with any odd power of $\sigma^\xi|_{K_u}$ is 0, while $\mathrm{tr}(\sigma_n^\xi(\lambda)) = 0$ implies that id, χ and $\bar{\chi}$ cannot appear either. Since K_u contains the cube roots of unity we can apply Proposition 5.1.2 of Kutzko [K] and get that $W(\sigma^\xi|_{K_u})$ is

[3]Since this is necessarily totally tamely ramified, the standard classification of such extensions [Has, Chapter 16] gives us that $K'_u = K_u(\sqrt[3]{\mathfrak{p}})$ where $\mathfrak{p}$ is a uniformising element of K_u.

multiplied by a third root of unity when twisting the representation by $\chi_{K_u}^{K_u'}$. So all three representations have W-values that differ by a cube root of unity, and from this we deduce the result. □

Proposition 10.2. *For odd n we have that*

$$W(\sigma_n|_{K'}) = W(\sigma_n)(-1)^{a(\sigma_n)}.$$

Proof. Using $(\epsilon 2)$ we have that

$$W(\sigma_n|_{K'}) = W\big(\mathrm{ind}_K^{K'}(\sigma_n|_{K'})\big)/\theta(K'/K)^{n+1}.$$

We first turn to the θ-factor, noting that

$$\theta(K'/K) = W(\mathrm{ind}_K^{K'} 1_{K'})/W(1_{K'})$$

where we have $W(1_{K'}) = 1$. Expanding the top as with 5.1.8 of Kutzko, we get

$$\mathrm{ind}_K^{K'}(1_{K'}) = 1_K \oplus \mathrm{ind}_K^{K_u}(\chi_{K_u}^{K_u'})$$

where $\chi_{K_u}^{K_u'}$ is a nontrivial cubic character for K_u'/K_u. So we get

$$\theta(K'/K) = W\big(1_K \oplus \mathrm{ind}_K^{K_u}(\chi_{K_u}^{K_u'})\big) = W(\chi_{K_u}^{K_u'})\theta(K_u/K)$$

again using $(\epsilon 2)$ and $W(1_K) = 1$. Since K_u/K is unramified and quadratic we have $\theta(K_u/K) = W(\chi_K^{K_u}) = (-1)^{n(\psi_K)}$ by $(\epsilon 6')$, while Kutzko in 5.1.9 shows directly that $W(\chi_{K_u}^{K_u'})^2 = 1$. Since $n+1$ is even, we get $\theta(K'/K)^{n+1} = 1$.

Similar to 5.1.8 of Kutzko (or by comparing characters), we have

$$\mathrm{ind}_K^{K'}(\sigma_n|_{K'}) = \sigma_n \oplus \mathrm{ind}_K^{K_u}(\sigma_n|_{K_u} \otimes \chi_{K_u}^{K_u'}).$$

So the multiplicativity of ϵ-factors gives us that

$$W(\sigma_n|_{K'}) = W(\sigma_n)W\big(\mathrm{ind}_K^{K_u}(\sigma_n|_{K_u} \otimes \chi_{K_u}^{K_u'})\big) = W(\sigma_n)W\big(\sigma_n|_{K_u} \otimes \chi_{K_u}^{K_u'}\big),$$

the second step by using $(\epsilon 2)$ again, with $\theta(K_u/K)^{n+1} = 1$. Now we use the above lemma that $W\big(\sigma_n|_{K_u} \otimes \chi_{K_u}^{K_u'}\big) = \zeta W\big(\sigma_n|_{K_u}\big)$ for ζ with $\zeta^3 = 1$ to get

$$W(\sigma_n|_{K'}) = \zeta W(\sigma_n)W\big(\sigma_n|_{K_u}\big),$$

and use $(\epsilon 2)$ and $\theta(K_u/K)^{n+1} = 1$ again to get

$$W(\sigma_n|_{K'}) = \zeta W(\sigma_n)W\big(\mathrm{ind}_K^{K_u}(\sigma_n|_{K_u})\big).$$

Also, we have that

$$\mathrm{ind}_K^{K_u}(\sigma_n|_{K_u}) = \sigma_n \oplus (\sigma_n \otimes \chi_K^{K_u})$$

and thus we get

$$W(\sigma_n|_{K'}) = \zeta W(\sigma_n)^2 W(\sigma_n \otimes \chi_K^{K_u}),$$

and now $(\epsilon 6')$ can be used to relate $W(\sigma_n \otimes \chi_K^{K_u})$ to $W(\sigma_n)$ to get

$$W(\sigma_n|_{K'}) = \zeta W(\sigma_n)^3\ (-1)^{n(\psi)(n+1)+a(\sigma_n)} = \zeta W(\sigma_n)^3\ (-1)^{a(\sigma_n)},$$

the last step since $n+1$ is even. Since the two W-signs are real, we can eliminate ζ and the cubing to get

$$W(\sigma_n|_{K'}) = W(\sigma_n)(-1)^{a(\sigma_n)}.$$

□

Of course, we may rewrite the formula as $W(\sigma_n) = W(\sigma_n\ |_{K'})(-1)^{a(\sigma_n)}$, showing that, in principle, we have reduced to the Q_8 case. Using Proposition 8.2, we can make this more explicit:

$$W(\sigma_n) = \begin{cases} W(\sigma\ |_{K'})(-1)^{a(\sigma_n)} & n \equiv 1 \pmod 8; \\ (-1)^{a(\sigma|_{K'})+a(\sigma_n)} & n \equiv 3 \pmod 8; \\ W(\sigma\ |_{K'})(-1)^{a(\sigma_n)} & n \equiv 5 \pmod 8; \\ (-1)^{a(\sigma_n)} & n \equiv 7 \pmod 8. \end{cases}$$

We note that for $K = \mathbb{Q}_2$ the formulae in Tables 1 and 2 of [MW] imply that $a(\sigma_n)$ has the same parity as $a(\sigma)$ for $n \equiv 1 \pmod 4$, and is even for other n. Hence for $K = \mathbb{Q}_2$,

$$W(\sigma_n) = \begin{cases} W(\sigma) & n \equiv 1 \pmod 8; \\ (-1)^{a(\sigma|_{K'})} & n \equiv 3 \pmod 8; \\ W(\sigma) & n \equiv 5 \pmod 8; \\ 1 & n \equiv 7 \pmod 8. \end{cases}$$

10.2. **Signs for odd powers, $f(K/\mathbb{Q}_2)$ even.** This time let K'/K be the cubic extension corresponding to the Q_8 subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$. This is a Galois extension of odd degree, so using an extension of Proposition 3.4 of [KT], we get $W(\sigma_n) = W(\sigma_n|_{K'})$ for n odd. (Their proof uses the evenness of the dimension.) Hence $W(\sigma_n) = W(\sigma)^{(n+1)/2}$, by Proposition 9.2.

11. $p = 3$ NONABELIAN INERTIA, $f(K/\mathbb{Q}_3)$ ODD

11.1. **Setup.** Let τ be a generator of the normal subgroup C_3 of $\mathcal{I}$, and λ a generator of C_4. Choose a basis $\{x, y\}$ for V such that $\tau(x) = \zeta x$ and $\tau(y) = \zeta^{-1}y$, where $\zeta = e^{2\pi i/3}$. Then $\lambda^{-1}\tau\lambda = \tau^{-1}$, so λ swaps the eigenspaces of τ. We can choose the basis in such a way that $\lambda(x) = y$ and $\lambda(y) = -x$. (Recall that since $\lambda \in \mathcal{I}$, the determinant of the matrix representing λ must be 1. In fact, the same observation for τ justifies the existence of x and y.) Then λ^2 acts on V as -1, so commutes with everything in $\mathcal{G}$. If Φ is (the image in $\mathcal{G}$ of) any inverse Frobenius element then, since $\mathcal{I}$ is a normal subgroup of $\mathcal{G}$ and τ, τ^{-1} are the only elements of $\mathcal{I}$ of exact order 3, we must have $\Phi^{-1}\tau\Phi = \tau$ or τ^{-1}. But if Φ does not commute with τ then $\lambda\Phi$ is another choice of inverse Frobenius element which does commute with τ. Hence, without loss of generality we may assume that Φ commutes with τ, so it preserves the eigenspaces. Let α be such that $\Phi(x) = \alpha x$ (then $\Phi(y) = \overline{\alpha}y$). Let β be the complex number of absolute value 1 such that $\alpha = \beta q^{1/2}$.

If $3 \mid (n - 2j)$ then τ fixes both $x^j y^{n-j}$ and $y^j x^{n-j}$. If n is even then, for $3 \mid (n - 2j)$ (in which case $6 \mid (n - 2j)$), the element $x^j y^{n-j} + (-1)^j y^j x^{n-j}$ is also fixed by λ (because j and $n - j$ have the same parity), hence is I-fixed. The I-fixed elements above must be eigenvectors for Φ (note that Φ maps V_j to itself and normalises I). Hence $\alpha^j\overline{\alpha}^{n-j} = \overline{\alpha}^j\alpha^{n-j}$ is real, so $\beta^{n-2j} = \pm 1$. Varying n and j, we see that $\beta^6 = \pm 1$. Since $\alpha + \overline{\alpha} \in \mathbb{Z}$, $\beta^6 \neq 1$ (here we use the fact that q is an odd power of 3), so $\beta^6 = -1$. Adjusting Φ by an element of $\langle \tau, \lambda^2 \rangle$, we may choose $\beta = \zeta_{12} = e^{\pi i/6}$.

So, in the basis $\{x, y\}$, by adjoining $\mu = \mathrm{diag}(\zeta_{12}, \zeta_{12}^{-1})$ to $\mathcal{I}$ we get $\mu^2 = \lambda\tau\lambda$, and this gives us the 2-extension G_{24} through which $\mathcal{W}(\overline{K}/K)$ acts on V via $\sigma^\xi = \sigma \otimes \omega^{1/2}$.

11.2. **L-function.** Similar to the previous cases, we can map Φ to $\mathrm{Aut}(E[4])$, and since $f(K/\mathbb{Q}_3)$ is odd, the image is not contained in $\mathcal{I}$ and has determinant -1. The only subgroups of $\mathrm{GL}_2(\mathbb{Z}/4)$ which contain $C_3 \rtimes C_4$ as a normal subgroup with cyclic quotient are $C_3 \rtimes C_4$ and its 2-extension, say H_{24}. Since the image of Φ has determinant -1, we must be in the latter case. Just as before, a character argument with H_{24} gives that the L-function (for even n) is

$$\big(1 - (-q)^{n/2}/q^s\big)^{-a_n}\big(1 + (-q)^{n/2}/q^s\big)^{-b_n} \quad \text{where} \quad a_n, b_n = \lceil \beta_n(\mathcal{I})/2 \rceil, \lfloor \beta_n(\mathcal{I})/2 \rfloor.$$

TABLE 4. Decomposition of σ_n^ξ for G_{24} for odd n

$n \equiv 1 \pmod{12}$:	σ^ξ	$\oplus$	$\frac{n-1}{6}(\sigma^\xi \oplus \bar\sigma^\xi \oplus \kappa)$
$n \equiv 3 \pmod{12}$:	$\sigma^\xi \oplus \kappa$	$\oplus$	$\frac{n-3}{6}(\sigma^\xi \oplus \bar\sigma^\xi \oplus \kappa)$
$n \equiv 7 \pmod{12}$:	$\bar\sigma^\xi$	$\oplus$	$\frac{n-1}{6}(\sigma^\xi \oplus \bar\sigma^\xi \oplus \kappa)$
$n \equiv 9 \pmod{12}$:	$\bar\sigma^\xi \oplus \kappa$	$\oplus$	$\frac{n-3}{6}(\sigma^\xi \oplus \bar\sigma^\xi \oplus \kappa)$
$n \equiv 5 \pmod{6}$:			$\frac{n+1}{6}(\sigma^\xi \oplus \bar\sigma^\xi \oplus \kappa)$

11.3. **Signs for odd powers.** The three irreducible symplectic representations of G_{24} are σ^ξ and its conjugate, and another 2-dimensional representation κ which, restricted to $\mathcal{I}$, factors through the C_4 quotient. Viewing κ as a representation of $\mathcal{W}(\overline{K}/K)$ by composition, it does not factor through an abelian quotient. Noting also that I has a unique quotient of order 4 (tamely ramified), we see that κ is precisely the same representation of $\mathcal{W}(\overline{K}/K)$ that would arise in the previously considered case $\mathcal{I} = C_4, \mathcal{G}$ non-abelian. The argument of the penultimate paragraph of §6 is easily adapted from $K = \mathbb{Q}_3$ to any K with $f(K/\mathbb{Q}_3)$ odd. (In general, the residue class of u may be taken to be $g^{(q+1)/2}$. Since $(q+1)/2 \equiv 2 \pmod 4$, we still have $\nu(u) = -1$.) It follows that $W(\kappa) = 1$. Alternatively, apply Theorem 1.1(ii) (see also Theorem 3.1(iii)) of [Ko]. This immediately gives us that $W(\kappa) = +1$ as -2 is square modulo 3.

As with the Q_8 case, we find that $\sigma^\xi = \bar\sigma^\xi \otimes \rho_u$ for an unramified character ρ_u, and thus we get $W(\sigma^\xi) = (-1)^{a(\sigma)} W(\bar\sigma^\xi)$. We get $W(\sigma_n^\xi)$ in terms of $W(\sigma^\xi)$ and the parity of $a(\sigma)$:

$$W(\sigma_n) = \begin{cases} W(\sigma) & n \equiv 1, 3 \pmod 6 \\ (-1)^{a(\sigma)(n+1)/6} & n \equiv 5 \pmod 6. \end{cases}$$

12. $p = 3$ NONABELIAN INERTIA, $f(K/\mathbb{Q}_3)$ EVEN

12.1. **L-function.** As noted above, the only subgroups of $\mathrm{GL}_2(\mathbb{Z}/4)$ which contain $C_3 \rtimes C_4$ as a normal subgroup with cyclic quotient are $C_3 \rtimes C_4$ and its 2-extension, say H_{24}. Since we have $\det(\sigma(\Phi)) = q = 3^{f(K/\mathbb{Q}_3)} \equiv 1 \pmod 4$ and H_{24} has no 2-dimensional representation of determinant 1, we get that the image of the Weil group in $\mathrm{Aut}(E[4])$ is just $C_3 \rtimes C_4$, the same as the image of I. From

this it follows, as in the proof of Proposition 9.1, that

$$L(\sigma_n, s) = \left(1 - q^{n/2}/q^s\right)^{-\beta_n(\mathcal{I})}.$$

12.2. **Signs for odd powers.** Here we get non-real constituents ρ and its conjugate (these factor through the C_4 quotient and are of order 4) in the decomposition for odd powers, but they appear in pairs and by the functional equation ($\epsilon 7$) we have that $W(\rho)W(\bar{\rho}) = \rho(-1) = -1$.

TABLE 5. Decomposition of σ_n^ξ for $C_3 \rtimes C_4$ for odd n

$n \equiv 1 \pmod 6$:	σ^ξ	$\oplus$	$\frac{n-1}{6}(\rho \oplus \bar{\rho} \oplus 2\sigma^\xi)$
$n \equiv 3 \pmod 6$:	$\rho \oplus \bar{\rho} \oplus \sigma^\xi$	$\oplus$	$\frac{n-3}{6}(\rho \oplus \bar{\rho} \oplus 2\sigma^\xi)$
$n \equiv 5 \pmod 6$:			$\frac{n+1}{6}(\rho \oplus \bar{\rho} \oplus 2\sigma^\xi)$

We get the sign for odd n to be

$$W(\sigma_n) = \begin{cases} (-1)^{(n-1)/6} W(\sigma) & n \equiv 1 \pmod 6 \\ (-1)^{(n+3)/6} W(\sigma) & n \equiv 3 \pmod 6 \\ (-1)^{(n+1)/6} & n \equiv 5 \pmod 6. \end{cases}$$

REFERENCES

[CS] J. Coates, C.G. Schmidt, Iwasawa theory for the symmetric square of an elliptic curve, *J. Reine Angew. Math.* **375/376** (1987), 104–156.

[CHT] L. Clozel, M. Harris, R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations, preprint, http://abel.math.harvard.edu/~rtaylor/

[D1] P. Deligne, Les constantes des équations functionelles des fonctions L, *Modular Functions of One Variable II*, 55–105, SLN 349, Springer-Verlag, New York, 1973.

[D2] P. Deligne, Les constantes locales de l'equation fonctionnelle de la fonction L d'Artin d'une representation orthogonale. (French) *Invent. Math.* **35** (1976), 299–316.

[D3] P. Deligne, Valeurs de Fonctions L et Périodes d'Intégrales, *Automorphic Forms, Representations and L-functions,* 313–346, Proc. Symp. Pure Math. Vol. 33, Part 2, Amer. Math. Soc., Providence, RI, 1979.

[DW] N. Dummigan, M. Watkins, Critical values of symmetric power L-functions, *Pure and Appl. Math. Q.* **5**, no.1, J.-P. Serre special issue (2009), 127–161.

[FQ] A. Fröhlich, J. Queyrut, On the functional equation of the Artin L-function for characters of real representations, *Invent. Math.* **20** (1973), 125-138.

[Hal] E. Halberstadt, Signes locaux des courbes elliptiques en 2 et 3, *C. R. Acad. Sci. Paris, Série I Math.* **326** (1998), 1047–1052.

[HSBT] M. Harris, N. Shepherd-Barron, R. Taylor, A family of Calabi-Yau varieties and potential automorphy, preprint, http://abel.math.harvard.edu/~rtaylor/

[Has] H. Hasse, Number Theory, Grundlehren der mathematischen Wissenschaften **229**, Springer-Verlag, Berlin, 1980. [Corrected and enlarged translation of the third edition of Zahlentheorie, Akademie-Verlag, Berlin, 1969, edited and prepared for publication by H. G. Zimmer].

[He] E. Hecke, *Analysis und Zahlentheorie: Vorlesung Hamburg 1920* (German). [Analysis and Number Theory: Hamburg Lectures 1920.] Edited and with a foreword by P. Roquette. Dokumente zur Geschichte der Mathematik [Documents on the History of Mathematics], **3**. Friedr. Vieweg & Sohn, Braunschweig, (1987), 234pp.

[Ko] S. Kobayashi, The local root number of elliptic curves with wild ramification, *Math. Ann.* **323** (2002), 609–623.

[KT] K. Kramer, J. Tunnell, Elliptic curves and local ϵ-factors, *Compositio Math.* **46** (1982), 307–352.

[K] P. Kutzko, The Langlands conjecture for Gl_2 of a local field, *Ann. of Math.* (2) **112** (1980), no. 2, 381–412.

[LRS] P. Lockhart, M. Rosen, J. Silverman, An upper bound for the conductor of an abelian variety, *J. Algebraic Geom.* **2** (1993), 569–601.

[MW] P. Martin, M. Watkins, Symmetric powers of elliptic curve L-functions. In *Algorithmic Number Theory*, Proceedings of the 7th International Symposium, ANTS-VII, Berlin, Germany, July 2006, edited by F. Hess, S. Pauli, and M. Pohst, Springer Lecture Notes in Computer Science **4076**, 377–392.

[N] J. Neukirch, *Algebraic Number Theory,* Grund. Math. Wiss., Vol. 322, Springer-Verlag, Berlin, Heidelberg, New York, 1999.

[PR] D. Prasad, D. Ramakrishnan, On the global root numbers of $GL(n) \times GL(m)$, in *Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996),* Proceedings of Symposia in Pure Maths of the AMS, vol. **66** part 2, (1999), 311-330.

[R1] D. E. Rohrlich, Elliptic curves and the Weil-Deligne group. *Elliptic Curves and Related Topics,* 125–157, CRM Proc. Lecture Notes, 4, Amer. Math. Soc., Providence, RI, 1994.

[R2] D. E. Rohrlich, Variation of the root number in families of elliptic curves, *Compositio Math.* **87** (1993), 119–151.

[R3] D. E. Rohrlich, Galois theory, elliptic curves, and root numbers, *Compositio Math.* **100** (1993), no. 3, 311–349.

[Se1] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[Se2] J.-P. Serre, Abelian l-adic representations and elliptic curves. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam (1968), xvi+177 pp. (not consecutively paged). Second edition, Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. xxiv+184 pp. Revised reprint of the 1968 original. Research Notes in Mathematics, **7**. A K Peters, Ltd., Wellesley, MA, 1998. 199 pp.

[ST] J.-P. Serre, J. Tate, Good reduction of abelian varieties, *Ann. of Math.* **88** (1968), 492–517.

[Sh] F. Shahidi, Symmetric power L-functions for GL_2. *Elliptic Curves and Related Topics,* 159–182, CRM Proc. Lecture Notes, 4, Amer. Math. Soc., Providence, RI, 1994.

[T1] J. Tate, Number theoretic background, *Automorphic Forms, Representations and L-functions,* 3–26, Proc. Symp. Pure Math. Vol. 33, Part 2, Amer. Math. Soc., Providence, RI, 1979.

[T2] J. Tate, Algebraic cycles and poles of zeta functions. *Arithmetical Algebraic Geometry,* 93–110, O.F.G. Schilling (ed.), Harper and Row, New York, 1965.

[Tay] R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations. II, preprint, http://abel.math.harvard.edu/~rtaylor/

[W] M. Watkins, Computing the modular degree of an elliptic curve, *Experiment. Math.* **11** (2002), 487–502.

[Wh] D. Whitehouse, Root numbers of elliptic curves over 2-adic fields, preprint, http://www.ihes.fr/~dw/maths/research.html

Neil Dummigan
University of Sheffield
Department of Pure Mathematics
Hicks Building, Hounsfield Road, Sheffield, S3 7RH, U.K.
E-mail: n.p.dummigan@shef.ac.uk

Mark Watkins
MAGMA Computer Algebra Group
University of Sydney, Department of Mathematics
University of Sydney NSW 2006, AUSTRALIA
E-mail: watkins@maths.usyd.edu.au