COMPOSITIO MATHEMATICA

Compatibility of arithmetic and algebraic local constants (the case $\ell \neq p$)

Jan Nekovář

Compositio Math. **151** (2015), 1626–1646.

doi:10.1112/S0010437X14008069

Compositio Math. 151 (2015) 1626–1646
doi:10.1112/S0010437X14008069

Compatibility of arithmetic and algebraic local constants (the case $\ell \neq p$)

Jan Nekovář

Abstract

We show that arithmetic local constants attached by Mazur and Rubin to pairs of self-dual Galois representations which are congruent modulo a prime number $p > 2$ are compatible with the usual local constants at all primes not dividing p and in two special cases also at primes dividing p. We deduce new cases of the p-parity conjecture for Selmer groups of abelian varieties with real multiplication (Theorem 4.14) and elliptic curves (Theorem 5.10).

Introduction

Let M be a motive (in an old-fashioned sense) over a number field F with coefficients in another number field L. For every finite prime $\mathfrak{p} \mid p$ of L the $\mathfrak{p}$-adic realisation $V = M_{\mathfrak{p}}$ of M is a representation of the Galois group $G_F = \mathrm{Gal}(\overline{F}/F)$, which is finite-dimensional over $\mathcal{K} = L_{\mathfrak{p}}$ and geometric in the sense of Fontaine and Mazur [FM95].

The L-function $L(M, s) = \sum_{n \geqslant 1} a_n n^{-s}$ (if well defined) is a Dirichlet series with coefficients in L. It gives rise to complex-valued L-functions $L(\iota M, s) = \sum_{n \geqslant 1} \iota(a_n) n^{-s}$ for various embeddings $\iota : L \hookrightarrow \mathbf{C}$.

The conjectures of Bloch and Kato [BK90] (generalised by Fontaine and Perrin-Riou [FPR94]) predict that the order of vanishing

$$r_{an}(\iota M) := \mathrm{ord}_{s=0} L(\iota M, s)$$

should be equal to

$$\chi_f(F, V^*(1)) := h^1_f(F, V^*(1)) - h^0(F, V^*(1)) = \dim_{\mathcal{K}} H^1_f(F, V^*(1)) - \dim_{\mathcal{K}} H^0(F, V^*(1)),$$

where H^1_f is the Bloch–Kato Selmer group [BK90, Definition 5.1] and

$$V^*(1) = \mathrm{Hom}_{\mathcal{K}}(V, \mathbf{Z}_p(1) \otimes_{\mathbf{Z}_p} \mathcal{K}).$$

If the motive M is *self-dual* in the sense that L is totally real and there exists a skew-symmetric L-linear isomorphism $M \simeq M^\vee(1)$ (inducing a skew-symmetric isomorphism of $\mathcal{K}[G_F]$-modules $V \simeq V^*(1)$), then the completed L-function of ιM is expected to satisfy a symmetric functional equation

$$(L_\infty \cdot L)(\iota M, s) = a^s \, \varepsilon(M) (L_\infty \cdot L)(\iota M, -s), \tag{0.1}$$

Received 17 December 2013, accepted in final form 25 November 2014, published online 8 April 2015.
2010 Mathematics Subject Classification 11G05, 11G40, 11S40 (primary).
Keywords: local constants, Selmer groups, parity conjecture, elliptic curves.
The author's research was supported in part by the grant ANR-BLAN-0114.

where $\varepsilon(M) = \prod_v \varepsilon_v(M)$ is a product of local constants $\varepsilon_v(M) = \pm 1$ ($\varepsilon_v(M)$ does not depend on ι if v is a finite prime of F; the product $\varepsilon_\infty(M) = \prod_{v\,|\,\infty} \varepsilon_v(M)$ does not depend on ι either). The functional equation (0.1) implies that

$$\varepsilon(M) = (-1)^{r_{an}(\iota M)+r_\infty(\iota M)}, \quad r_\infty(\iota M) := \mathrm{ord}_{s=0} L_\infty(\iota M, s).$$

In particular, in the presence of (0.1) the mod-2 version of the Bloch–Kato conjecture

$$r_{an}(\iota M) \stackrel{?}{\equiv} \chi_f(F, V) \pmod 2 \tag{0.2}$$

is equivalent to

$$\varepsilon(M)(-1)^{r_\infty(\iota M)} \stackrel{?}{=} (-1)^{\chi_f(F,V)}. \tag{0.3}$$

In the special case where the motive M is pure (necessarily of weight -1),

$$r_\infty(\iota M) = 0, \quad \chi_f(F, V) = h^1_f(F, V),$$

the local constant $\varepsilon_v(M) = \varepsilon_v(V)$ for $v \nmid \infty$ depends only on the restriction $V|_{G_v}$ of V to the local Galois group $G_v = \mathrm{Gal}(\overline{F}_v/F_v)$ and the archimedean term $\varepsilon_\infty(M)$ depends only on $V|_{G_w}$ for all $w\,|\,p$ (see [Nek07, Erratum]). Consequently, in the pure case both sides of the conjectural equality (0.3), which boils down to

$$\varepsilon(V) \stackrel{?}{=} (-1)^{h^1_f(F,V)}, \tag{0.4}$$

depend only on V.

Several authors [DD09, DD11, MR07, MR08, Nek07] have tried to establish a relative version of (0.3), namely, an equality

$$(-1)^{\chi_f(F,V)}/(-1)^{\chi_f(F,V')} \stackrel{?}{=} (-1)^{r_\infty(\iota M)-r_\infty(\iota M')}\, \varepsilon(M)/\varepsilon(M'), \tag{0.5}$$

or its special case when M and M' are pure,

$$(-1)^{h^1_f(F,V)}/(-1)^{h^1_f(F,V')} \stackrel{?}{=} \varepsilon(V)/\varepsilon(V'), \tag{0.6}$$

for suitably related pairs of self-dual motives M and M'.

If $p \neq 2$ and if there are G_F-stable self-dual lattices $T \subset V$, $T' \subset V'$ whose reductions $\overline{T} = T/\mathfrak{p}T$ and $\overline{T}' = T'/\mathfrak{p}T'$ are (symplectically) isomorphic G_F-modules, a formula of Mazur and Rubin [MR07, Theorem 1.4] (combined with Flach's generalisation of the Cassels–Tate pairing [Fla90]) expresses

$$\chi_f(F, V) - \chi_f(F, V') \equiv \sum_v d(\mathscr{F}_v, \mathscr{F}'_v) \pmod 2 \in \mathbf{Z}/2\mathbf{Z}$$

as a sum of local terms, each of which depends only on the restrictions $T|_{G_v}$ and $T'|_{G_v}$ (only finite primes v of F dividing p or those at which V or V' are ramified contribute to the formula). Mazur and Rubin expect these local terms ('arithmetic local constants') to reflect the local decomposition of

$$\varepsilon(M)/\varepsilon(M') = \prod_v \varepsilon_v(M)/\varepsilon_v(M').$$

Our first main result (Theorem 2.17) confirms this intuition. We show that $\varepsilon_v(V)/\varepsilon_v(V') = (-1)^{d(\mathscr{F}_v, \mathscr{F}'_v)}$ for all $v \nmid p$. In fact, we prove a purely local version of this statement for pairs of

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

self-dual representations of the local Galois group G_v. A special case of this result was proved by Chetty [Che10], who also treated some cases when $v \mid p$.

The case of $v \mid p$ is much more complicated, in general. In § 3 we give an example of two situations in which arithmetic local constants at $v \mid p$ can be shown to match $\varepsilon_v(V)/\varepsilon_v(V')$.

In § 4 we make explicit the relations (0.5), (0.6) in two global cases whose local behaviour at primes above p is covered by results of § 3.

In § 5 we combine one of the main results of § 4 (Theorem 4.12) with techniques of [Nek13] in order to relax the assumptions of [Nek13, Theorem A] as follows.

THEOREM. *If E is an elliptic curve defined over a totally real number field F and if $\mathrm{End}_{\overline{\mathbf{Q}}}(E) \otimes \mathbf{Q} \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-3})$, then the p-parity conjecture*

$$\mathrm{ord}_{s=1} L(E/F, s) \equiv \mathrm{rk}_{\mathbf{Z}} E(F) + \mathrm{cork}_{\mathbf{Z}_p} Ш(E/F)[p^\infty] \pmod 2$$

holds for all primes $p \neq 2$.

COROLLARY. *Under the same assumptions the p-parity conjecture*

$$\mathrm{ord}_{s=1} L(E/F', s) \equiv \mathrm{rk}_{\mathbf{Z}} E(F') + \mathrm{cork}_{\mathbf{Z}_p} Ш(E/F')[p^\infty] \pmod 2$$

holds (if $p \neq 2$) for any tower of finite extensions $F \subset F_1 \subset F'$, where F_1/F is abelian and F'/F_1 is a Galois extension of odd degree.

See 5.12–5.13 for a more precise version of these statements (which also covers certain cases when $\mathrm{End}_{\overline{\mathbf{Q}}}(E) \otimes \mathbf{Q} = \mathbf{Q}(i), \mathbf{Q}(\sqrt{-3})$ or $p = 2$).

Notation and conventions. All representations (in particular, characters) are continuous. For a number field F we denote by h_F (respectively, Cl_F) the class number (respectively, the ideal class group) of the ring of integers $\mathcal{O}_F$ of F. We abbreviate $\otimes_{\mathbf{Z}}$ as $\otimes$. For an abelian group A we let $\widehat{A} = A \otimes \widehat{\mathbf{Z}}$, where $\widehat{\mathbf{Z}}$ is the pro-finite completion of $\mathbf{Z}$.

1. Bilinear algebra

1.1 Let $\mathcal{O}$ be a discrete valuation ring with fraction field $\mathcal{K}$, uniformiser π and residue field $k = \mathcal{O}/\pi\mathcal{O}$ of characteristic $\mathrm{char}(k) \neq 2$. Let X be an $\mathcal{O}$-module of finite length equipped with a non-degenerate symmetric bilinear pairing

$$(\,,\,) : X \times X \longrightarrow \mathcal{K}/\mathcal{O}.$$

1.2 The k-vector space $X[\pi]$ has a canonical decreasing exhaustive filtration

$$F^0 = X[\pi] \supset F^1 = \pi X[\pi^2] \supset F^2 = \pi^2 X[\pi^3] \supset \cdots$$

whose graded quotients $gr_F^i = F^i/F^{i+1}$ $(i \geqslant 0)$ are equipped with non-degenerate symmetric pairings

$$(\,,\,)_i : gr_F^i \times gr_F^i \longrightarrow k, \quad (\pi^i x, \pi^i y)_i = \pi^i (x, y) \pmod{\pi\mathcal{O}}$$

(which depend not only on $(\,,\,)$ but also on π).

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

1.3 The filtration F^i is stable by any $\mathcal{O}$-linear automorphism $f : X \longrightarrow X$. If f is an isometry (i.e., if $(f(x), f(y)) = (x, y)$ for all $x, y \in X$), then the induced automorphisms $gr^i(f) : gr^i_F \longrightarrow gr^i_F$ are also isometries.

Proposition 1.4. *If $f : X \longrightarrow X$ is an isometry, then:*

(i) $\dim_k \mathrm{Im}(X^{f=1} \longrightarrow X/\pi X) \equiv \sum_{i\geqslant 0} \dim_k \mathrm{Ker}(gr^i(f) - 1) \pmod 2$.

(ii) *[Nek07, Lemma 2.2.2] If $\pi X = 0$ (in other words, if $(X, (\ ,\ ))$ is a quadratic space over k), then*

$$(-1)^{\dim_k(X^{f=1})} = \det(-f).$$

Proof. (i) There is an orthogonal decomposition $X = X_1 \oplus X_1^{\perp}$, where $f - 1$ is nilpotent (respectively, invertible) on X_1 (respectively, on $X_1^{\perp}$):

$$X_1 = \bigcup_{n\geqslant 1} \mathrm{Ker}\,(f-1)^n, \quad X_1^{\perp} = \bigcap_{n\geqslant 1} \mathrm{Im}\,(f-1)^n.$$

Statement (i) is trivial for $X_1^{\perp}$; we can replace X by X_1 and assume that $f = 1 + N$, where $N : X \longrightarrow X$ is nilpotent. The formula

$$\{x, y\} = (Nx, y) + (Nx, Ny)/2 = (Nx, (1 + N/2)y) \quad (x, y \in X) \tag{1.4.1}$$

defines a skew-symmetric (hence alternating, since $2 \in \mathcal{O}^{\times}$ by assumption) bilinear form $X \times X \longrightarrow \mathcal{K}/\mathcal{O}$ with kernel equal to $\mathrm{Ker}(N) = X^{f=1}$. The structure theory of symplectic $\mathcal{O}$-modules of finite length implies that there is an exact sequence

$$0 \longrightarrow X^{f=1} \longrightarrow X \longrightarrow Z \oplus Z \longrightarrow 0,$$

for a suitable $\mathcal{O}$-module Z. As a result,

$$\begin{aligned}\dim_k \mathrm{Im}(X^{f=1} \longrightarrow X/\pi X) &= \dim_k(X/\pi X) - 2\dim_k(Z/\pi Z) \equiv \dim_k(X/\pi X)\\ &= \dim_k X[\pi] = \sum_{i\geqslant 0} \dim_k gr^i_F \pmod 2.\end{aligned}$$

Finally, applying statement (ii) to the unipotent isometry $gr^i(f)$ of gr^i_F, we obtain

$$\dim_k gr^i_F \equiv \dim_k \mathrm{Ker}(gr^i(f) - 1) \pmod 2.$$

(ii) In [Nek07, Lemma 2.2.2] we reproduced a proof of this statement due to Oesterlé (it relied on a decomposition of f into a product of reflections). Alternatively, one can use the orthogonal decomposition into generalised eigenspaces of f (after replacing k by its algebraic closure $\overline{k}$ and X by $X \otimes_k \overline{k}$),

$$X = \bigoplus_{\lambda} X_\lambda, \quad X_\lambda = \bigcup_{n\geqslant 1} \mathrm{Ker}\,(f - \lambda)^n.$$

The orthogonality relation $X_\lambda \perp X_\mu$ for $\lambda\mu \neq 1$ implies that $\dim_k X_\lambda = \dim_k X_{1/\lambda}$, hence

$$\det(-f) = \det(-f \mid X_1) \prod_{\lambda\neq 1} (-\lambda)^{\dim_k X_\lambda} = \det(-f \mid X_1) = (-1)^{\dim_k X_1}.$$

As $f-1$ is nilpotent on X_1, formula (1.4.1) defines a skew-symmetric bilinear form $X_1 \times X_1 \longrightarrow k$ with kernel $X_1^{f=1}$. It follows that

$$\dim_k X_1 \equiv \dim_k X_1^{f=1} = \dim_k X^{f=1} \pmod 2. \qquad \square$$

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

COROLLARY 1.5. *If $f : X \longrightarrow X$ is an isometry, then*

$$(-1)^{\dim_k \mathrm{Im}(X^{f=1} \longrightarrow X/\pi X)} = \det(-f \mid X[\pi]).$$

Proof. The right-hand side is equal to $\prod_{i \geqslant 0} \det(-gr^i(f))$; the result follows from combining (i) with (ii) applied to each gr^i_F. □

2. Arithmetic local constants (the case $\ell \neq p$)

2.1 Let $\mathcal{O}$ be the ring of integers in a finite extension $\mathcal{K}$ of $\mathbf{Q}_p$, where $p \neq 2$. Fix a uniformiser $\pi \in \mathcal{O}$ and denote by $k = \mathcal{O}/\pi\mathcal{O}$ the residue field of $\mathcal{K}$.

2.2 Let K be a finite extension of $\mathbf{Q}_\ell$. In 2.6–2.17 we assume that $\ell \neq p$. Denote by $G = \mathrm{Gal}(\overline{K}/K) \supset I \supset I_w$ the absolute Galois group, the inertia group and the wild inertia group of K, respectively.

2.3 Let V be a finite-dimensional $\mathcal{K}$-vector space equipped with a continuous linear action of G and a non-degenerate G-equivariant skew-symmetric pairing

$$\langle\,,\rangle : V \times V \longrightarrow \mathcal{K}(1) = \mathcal{K} \otimes_{\mathbf{Z}_p} \mathbf{Z}_p(1).$$

2.4 For any G-stable $\mathcal{O}$-lattice $T \subset V$, denote by $\overline{T} = T/\pi T$ its reduction modulo π. We say that T is *self-dual* with respect to $\langle\,,\rangle$ if $\langle\,,\rangle$ induces a pairing $T \times T \longrightarrow \mathcal{O}(1)$ whose reduction $\overline{T} \times \overline{T} \longrightarrow k(1) = \mu_p \otimes k$ is non-degenerate.

2.5 Note that T is self-dual with respect to a multiple of $\langle\,,\rangle$ by a suitable scalar $a \in \mathcal{K}^\times$ if $\dim_{\mathcal{K}}(V) = 2$ (or if $\overline{T}$ is an irreducible $k[G]$-module).

2.6 From now on until the end of § 2 we assume that T is self-dual with respect to $\langle\,,\rangle$ and that $\ell \neq p$.

According to Tate's local duality the pairings

$$H^i(\overline{T}) \times H^{2-i}(\overline{T}) \xrightarrow{\cup} H^2(k(1)) \simeq k \quad (H^i(-) = H^i(G, -))$$

are non-degenerate (and symmetric if $i = 1$). The local Euler characteristic formula implies that the dimensions $h^i(\overline{T}) = \dim_k H^i(\overline{T})$ satisfy

$$h^1(\overline{T}) = h^0(\overline{T}) + h^2(\overline{T}) = 2\,h^0(\overline{T}).$$

The unramified cohomology $H^1_{\mathrm{ur}}(\overline{T}) = H^1(G/I, \overline{T}^I) \subset H^1(\overline{T})$ is an isotropic subspace of the quadratic space $(H^1(\overline{T}), \cup)$ (since $cd_p(G/I) = 1$) of dimension $h^1_{\mathrm{ur}}(\overline{T}) = h^0(\overline{T}) = h^1(\overline{T})/2$. It follows that $H^1_{\mathrm{ur}}(\overline{T})$ is a *Lagrangian* subspace of $H^1(\overline{T})$, i.e., a subspace equal to its own orthogonal complement (which is equivalent to being an isotropic subspace of dimension $h^1(\overline{T})/2$).

2.7 Similarly, the unramified cohomology $H^1_{\mathrm{ur}}(V) = H^1(G/I, V^I) \subset H^1(V)$ is a Lagrangian subspace of $H^1(V)$. The space $H^1(V)$ is equipped with a non-degenerate symmetric pairing $\cup : H^1(V) \times H^1(V) \longrightarrow H^2(\mathcal{K}(1)) \simeq \mathcal{K}$ and its dimension is equal to $\dim_{\mathcal{K}} H^1(V) = 2\,\dim_{\mathcal{K}} H^0(V)$.

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

By propagation [MR04, Example 1.1.2], $H^1_{\mathrm{ur}}(V)$ defines subspaces

$$\begin{aligned} H^1_f(T) &= \mathrm{Ker}(H^1(T) \longrightarrow H^1(V)/H^1_{\mathrm{ur}}(V)) \\ &= H^1_{\mathrm{ur}}(T) + H^1(T)_{\mathrm{tors}} \subset H^1(T), \\ H^1_{\mathrm{ur}}(T) &= H^1(G/I, T^I), \\ \mathscr{F} &= \mathrm{Im}(H^1_f(T) \longrightarrow H^1(\overline{T})) \subset H^1(\overline{T}). \end{aligned}$$

The subspace $\mathscr{F}$ is again Lagrangian in $H^1(\overline{T})$. If $V = V^I$ is unramified, then $\mathscr{F} = H^1_{\mathrm{ur}}(\overline{T})$.

DEFINITION 2.8. For Lagrangian subspaces $L, L' \subset H^1(\overline{T})$, define

$$d(L, L') = \dim_k(L/L \cap L') \pmod 2 \in \mathbf{Z}/2\mathbf{Z}$$

(of course, $d(L, L') = d(L', L)$, since $\dim_k(L) = \dim_k(L') = h^0(\overline{T})$).

PROPOSITION 2.9 [KMR13, Corollary 2.5]. *If $L_0, L_1, L_2 \subset H^1(\overline{T})$ are Lagrangian subspaces, then*

$$d(L_0, L_1) - d(L_0, L_2) + d(L_1, L_2) = 0 \in \mathbf{Z}/2\mathbf{Z}.$$

2.10 Denote by

$$H^1_{/\mathrm{ur}}(-) = H^1(-)/H^1_{\mathrm{ur}}(-) \quad (- = V, T, \overline{T})$$

the 'ramified part' of $H^1(-)$. The restriction map induces an isomorphism

$$H^1_{/\mathrm{ur}}(-) \simeq H^1(I, -)^{f=1} \quad (- = V, T, \overline{T}),$$

where $f \in G$ is any lift of the geometric Frobenius element generating G/I topologically.

PROPOSITION 2.11. *There is a canonical isomorphism*

$$\mathscr{F}/(\mathscr{F} \cap H^1_{\mathrm{ur}}(\overline{T})) \simeq \mathrm{Im}(H^1_{/\mathrm{ur}}(T)_{\mathrm{tors}} \longrightarrow H^1_{/\mathrm{ur}}(\overline{T})).$$

Proof. The left-hand side is isomorphic to

$$\mathrm{Im}(\mathscr{F} \longrightarrow H^1_{/\mathrm{ur}}(\overline{T})) = \mathrm{Im}(H^1_f(T) \longrightarrow H^1_{/\mathrm{ur}}(T) \longrightarrow H^1_{/\mathrm{ur}}(\overline{T})).$$

On the other hand,

$$\begin{aligned} \mathrm{Im}(H^1_f(T) \longrightarrow H^1_{/\mathrm{ur}}(T)) &= H^1_f(T)/H^1_{\mathrm{ur}}(T) = (H^1_{\mathrm{ur}}(T) + H^1(T)_{\mathrm{tors}})/H^1_{\mathrm{ur}}(T) \\ &= \mathrm{Im}(H^1(T)_{\mathrm{tors}} \longrightarrow H^1_{/\mathrm{ur}}(T)). \end{aligned}$$

The statement of the proposition follows from the fact that $\mathrm{Im}(H^1(T)_{\mathrm{tors}} \longrightarrow H^1_{/\mathrm{ur}}(T)) = H^1_{/\mathrm{ur}}(T)_{\mathrm{tors}}$ (the inclusion '$\subset$' is automatic; the opposite inclusion '$\supset$' is a consequence of the fact that $H^1(T)/H^1_f(T)$ is torsion-free). □

PROPOSITION 2.12. *There exists a non-degenerate symmetric bilinear pairing*

$$(\,,\,) : H^1(I, T)_{\mathrm{tors}} \times H^1(I, T)_{\mathrm{tors}} \longrightarrow \mathcal{K}/\mathcal{O}$$

for which f is an isometry.

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

Proof. This is a local version of the Cassels–Tate pairing, attached to the duality isomorphism $R\Gamma(I,T) \simeq R\mathrm{Hom}_{\mathcal{O}}(R\Gamma(I,T),\mathcal{O}[-1])$ (cf. the discussion in [Nek06, 10.1]). It can be described explicitly as follows. There is an orthogonal decomposition (with respect to $\langle\,,\rangle$) $T = T_{\mathrm{tame}} \oplus T_{\mathrm{wild}}$, in which $T_{\mathrm{tame}} = T^{I_w}$, $T_{\mathrm{wild}}^{I_w} = 0$ and $H^i(I,T) = H^i(I/I_w, T_{\mathrm{tame}})$. We can replace T by T_{tame} and assume that T is a representation of the group G/I_w, which is topologically generated by f and any fixed topological generator t of the tame inertia group I/I_w. If q denotes the cardinality of the residue field of K (which is prime to p, by assumption), then $tf = ft^q$.

Consider $\langle\,,\rangle$ as a pairing $\langle\,,\rangle : T \times T \longrightarrow \mathcal{O}$ satisfying

$$\forall x,y \in T\ \langle tx,ty\rangle = \langle x,y\rangle, \quad \langle fx,fy\rangle = q^{-1}\langle x,y\rangle.$$

If $c,c' \in Z^1(I/I_w,T)$ are 1-cocycles whose cohomology classes $[c],[c']$ lie in $H^1(I/I_w,T)[\pi^m]$ $(m \geqslant 0)$, then $\pi^m c(t) = (t-1)a$ for some $a \in T$. We define

$$([c],[c']) = (\pi^{-m}\langle a, c'(t)\rangle) \pmod{\mathcal{O}} \in \pi^{-m}\mathcal{O}/\mathcal{O} \subset \mathcal{K}/\mathcal{O}.$$

It is an elementary exercise to check that this formula defines a pairing with the required properties. □

PROPOSITION-DEFINITION 2.13. *The invariant*

$$e(T) := d(\mathscr{F}, H^1_{\mathrm{ur}}(\overline{T})) = \dim_k \mathscr{F}/(\mathscr{F} \cap H^1_{\mathrm{ur}}(\overline{T})) \pmod 2 \in \mathbf{Z}/2\mathbf{Z}$$

satisfies

$$(-1)^{e(T)} \det(-f \,|\, V^I) \equiv \det(-f \,|\, \overline{T}^I) \pmod{\pi\mathcal{O}}.$$

Proof. According to Proposition 2.11 we have

$$\mathscr{F}/(\mathscr{F} \cap H^1_{\mathrm{ur}}(\overline{T})) \simeq \mathrm{Im}(X^{f=1} \longrightarrow H^1(I,\overline{T})) = \mathrm{Im}(X^{f=1} \longrightarrow X/\pi X), \quad X = H^1(I,T)_{\mathrm{tors}}$$

(since both maps $X/\pi X \longrightarrow H^1(I,T)/\pi H^1(I,T) \longrightarrow H^1(I,\overline{T})$ are injective). Combining Proposition 2.12 with Corollary 1.5, we obtain

$$(-1)^{e(T)} = \det(-f \,|\, X[\pi]) \in \{\pm 1\} \subset k^\times,$$

hence

$$\begin{aligned}(-1)^{e(T)} \det(-f \,|\, V^I) &\equiv (-1)^{e(T)} \det(-f \,|\, T^I/\pi T^I) = \det(-f \,|\, T^I/\pi T^I)\det(-f \,|\, X[\pi]) \\ &= \det(-f \,|\, \overline{T}^I) \pmod{\pi\mathcal{O}},\end{aligned}$$

where the last equality follows from the exact sequence

$$0 \longrightarrow T^I/\pi T^I \longrightarrow \overline{T}^I \longrightarrow X[\pi] \longrightarrow 0.$$ □

2.14 Deligne [Del73] defined local constants $\varepsilon(V,\psi,dx)$ depending on V (more precisely, on the corresponding representation of the Weil–Deligne group of K), a non-trivial additive character ψ of K and a Haar measure dx on K. If dx_ψ is the Haar measure which is self-dual with respect to ψ, then the value of $\varepsilon(V) = \varepsilon(V,\psi,dx_\psi)$ does not depend on ψ and is equal to ± 1 [Nek07, Proposition 2.2.1].

Deligne [Del73, (5.1)] also introduced modified local constants

$$\varepsilon_0(V) = \varepsilon(V)\det(-f \,|\, V^I) \in \mathcal{O}^\times$$

and showed [Del73, Theorem 6.5] that the value of $\varepsilon_0(V) \pmod{\pi\mathcal{O}} \in k^\times$ depends only on $\overline{T}$; we denote it by $\varepsilon_0(\overline{T})$. The congruence in Proposition 2.13 can be restated as follows.

COROLLARY 2.15. $(-1)^{e(T)}\varepsilon(V) \equiv \det(-f \,|\, \overline{T}^I)\,\varepsilon_0(\overline{T})^{-1} \pmod{\pi\mathcal{O}}$.

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

2.16 Let V' be another representation of G with coefficients in $\mathcal{K}$, equipped with a non-degenerate G-equivariant skew-symmetric pairing $\langle\,,\rangle' : V' \times V' \longrightarrow \mathcal{K}(1)$. Assume that $T' \subset V'$ is a self-dual lattice with respect to $\langle\,,\rangle'$ and that there exists an isomorphism of $k[G]$-modules $\overline{T} \simeq \overline{T}' = T'/\pi T'$ compatible with the pairings $\overline{T} \times \overline{T} \longrightarrow k(1)$ and $\overline{T}' \times \overline{T}' \longrightarrow k(1)$ induced by $\langle\,,\rangle$ and $\langle\,,\rangle'$, respectively.

Fix such an isomorphism $\overline{T} \simeq \overline{T}'$; it induces an isomorphism $H^1(\overline{T}) \simeq H^1(\overline{T}')$ under which

$$\mathscr{F}' = \mathrm{Im}(H^1_f(T') \longrightarrow H^1(\overline{T}')) \subset H^1(\overline{T}')$$

becomes a Lagrangian subspace of $H^1(\overline{T})$. The invariant $d(\mathscr{F}, \mathscr{F}') \in \mathbf{Z}/2\mathbf{Z}$ is the *arithmetic local constant* of Mazur and Rubin [MR07].

THEOREM 2.17 (Compatibility of arithmetic and algebraic local constants in the case $\ell \neq p$). *In the situation of 2.16 we have* $(-1)^{d(\mathscr{F},\mathscr{F}')} = \varepsilon(V)/\varepsilon(V')$.

Proof. Applying Corollary 2.15 to T and T', we obtain

$$(-1)^{e(T)}\varepsilon(V) \equiv (-1)^{e(T')}\varepsilon(V') \pmod{\pi\mathcal{O}},$$

hence $(-1)^{e(T)}\varepsilon(V) = (-1)^{e(T')}\varepsilon(V')$, since $1 \not\equiv -1 \pmod{\pi\mathcal{O}}$. We conclude by noting that $e(T) - e(T') + d(\mathscr{F}, \mathscr{F}') = 0 \in \mathbf{Z}/2\mathbf{Z}$, thanks to Proposition 2.9. □

3. Arithmetic local constants (the case $\ell = p$)

3.1 Assume now that $\ell = p$ ($\neq 2$) in the situation of 2.2 and that we are given $T \subset V$ and $T' \subset V'$ as in 2.16 (with T self-dual, too).

3.2 Tate's local duality still holds; the corresponding quadratic space $(H^1(\overline{T}), \cup)$ has (even) dimension $h^1(\overline{T}) = 2\,h^0(\overline{T}) + [K : \mathbf{Q}_p] \dim_k \overline{T}$. In order to produce suitable Lagrangian subspaces of $H^1(\overline{T})$ we need to assume that both V and V' are potentially semistable representations of G.

The Bloch–Kato subspaces

$$H^1_f(-) = \mathrm{Ker}(H^1(-) \longrightarrow H^1(- \otimes_{\mathbf{Q}_p} B_{\mathrm{cris}})) \quad (- = V, V')$$

are then Lagrangian subspaces of $H^1(V)$ and $H^1(V')$, respectively [BK90, Proposition 3.8]. They define, by propagation, subspaces

$$H^1_f(T) = \mathrm{Ker}(H^1(T) \longrightarrow H^1(V)/H^1_f(V)) \subset H^1(T)$$

and $H^1_f(T') \subset H^1(T')$. Their images

$$\mathscr{F} = \mathrm{Im}(H^1_f(T) \longrightarrow H^1(\overline{T})) \subset H^1(\overline{T}),$$
$$\mathscr{F}' = \mathrm{Im}(H^1_f(T') \longrightarrow H^1(\overline{T}')) \subset H^1(\overline{T}') \simeq H^1(\overline{T})$$

are Lagrangian subspaces of $H^1(\overline{T})$.

3.3 One can attach to Fontaine's module $D_{\mathrm{pst}}(V)$ a representation $WD(V)$ of the Weil–Deligne group of K [Fon94], [FPR94, I.1.3.2], which is self-dual in the same way as V is. The local constant $\varepsilon(V) := \varepsilon(WD(V), \psi, dx_\psi) \in \{\pm 1\}$ is again independent of ψ (and similarly for $\varepsilon(V')$).

It would be highly desirable to relate $\varepsilon(V)/\varepsilon(V')$ to the arithmetic local constant $d(\mathscr{F}, \mathscr{F}')$. We will discuss two special cases in which this can be done, but it is not clear in what generality one can expect such a relation to hold.

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

3.4 In the first case the local conditions are given by flat cohomology, as in the pioneering work of Mazur [Maz72]. Assume that $\mathbf{Q}_p \subset K_1 \subset K$ is a subfield and that T and T' have the following properties.

(3.4.1) The ramification index of $K_1/\mathbf{Q}_p$ satisfies $e(K_1/\mathbf{Q}_p) < p-1$.

(3.4.2) The action of G on T and T' extends to an action of $G_1 = \mathrm{Gal}(\overline{K}/K_1)$.

(3.4.3) All the data $\langle\,,\rangle, \langle\,,\rangle'$ and $\overline{T} \simeq \overline{T}'$ are G_1-equivariant.

(3.4.4) There exist π-divisible $\mathcal{O}$-modules $\mathcal{H}$ and $\mathcal{H}'$ over the ring of integers $O_{K_1} \subset K_1$ and $\mathcal{O}[G_1]$-equivariant isomorphisms $T \simeq T_\pi\mathcal{H}(\overline{K})$, $T' \simeq T_\pi\mathcal{H}'(\overline{K})$.

3.5 Assumptions (3.4.2)–(3.4.4) imply that V and V' are crystalline representations of G_1, hence $WD(V)$, $WD(V')$ are unramified representations of the Weil–Deligne group of K_1 (which are self-dual, up to the Tate twist). As a result, the local constants of both V and V' over any extension of K_1 are equal to 1.

PROPOSITION 3.6. *Under assumptions (3.4.1)–(3.4.4) we have $\mathscr{F} = \mathscr{F}'$ and $d(\mathscr{F}, \mathscr{F}') = 0$.*

Proof. In this situation $\overline{T} = \mathcal{H}[\pi](\overline{K})$, $\overline{T}' = \mathcal{H}'[\pi](\overline{K})$ and

$$\mathscr{F} = \mathrm{Im}(H^1_{\mathrm{fppf}}(O_K, \mathcal{H}[\pi]) \longrightarrow H^1(\overline{T})), \quad \mathscr{F}' = \mathrm{Im}(H^1_{\mathrm{fppf}}(O_K, \mathcal{H}'[\pi]) \longrightarrow H^1(\overline{T}')) \tag{3.6.1}$$

(see [Nek12, Proposition A.2.6]). Assumption (3.4.1) implies, by Raynaud's theorem [Ray74, Corollary 3.3.6], that the fixed isomorphism $\overline{T} \simeq \overline{T}'$ in (3.4.3) comes from a unique isomorphism $\mathcal{H}[\pi] \simeq \mathcal{H}'[\pi]$ of finite flat k-vector space schemes over $\mathcal{O}_{K_1}$. The statement of the theorem then follows from the functoriality of the morphisms in (3.6.1). □

3.7 In the second case we fix two representations $\rho, \rho' : G \longrightarrow \mathrm{GL}_n(\mathcal{O})$ with open kernel whose reductions $\overline{\rho} = \overline{\rho}' : G \longrightarrow \mathrm{GL}_n(\mathcal{O}/\pi\mathcal{O}) = \mathrm{GL}_n(k)$ modulo π coincide. In order to simplify the notation, write $\rho_+ = \rho$, $\rho'_+ = \rho'$ and denote by $\rho_- = \rho^*, \rho'_- = (\rho')^* : G \longrightarrow \mathrm{GL}_n(\mathcal{O})$ the dual representations. Instead of the pair T, T' as in 3.1 we consider the pair $T \otimes (\rho_+ \oplus \rho_-)$ and $T \otimes (\rho'_+ \oplus \rho'_-)$.

3.8 The subspaces

$$\mathscr{F} \subset H^1(\overline{T} \otimes (\overline{\rho}_+ \oplus \overline{\rho}_-)) = H^1(\overline{T} \otimes (\overline{\rho}'_+ \oplus \overline{\rho}'_-)) \supset \mathscr{F}'$$

are respectively equal to $\mathscr{F} = Y_+ \oplus Y_-$ and $\mathscr{F}' = Y'_+ \oplus Y'_-$, where

$$\begin{aligned} Y_\pm &= \mathrm{Im}(H^1_f(T \otimes \rho_\pm) \otimes_{\mathcal{O}} k \hookrightarrow H^1(\overline{T} \otimes \overline{\rho}_\pm)), \\ Y'_\pm &= \mathrm{Im}(H^1_f(T \otimes \rho'_\pm) \otimes_{\mathcal{O}} k \hookrightarrow H^1(\overline{T} \otimes \overline{\rho}'_\pm) = H^1(\overline{T} \otimes \overline{\rho}_\pm)), \end{aligned}$$

hence

$$d(\mathscr{F}, \mathscr{F}') \equiv \dim_k(Y_+/(Y_+ \cap Y'_+)) + \dim_k(Y_-/(Y_- \cap Y'_-)) \pmod 2.$$

The following proposition is a generalisation of [Nek13, Lemma 1.2].

PROPOSITION 3.9. *In the situation of 3.7 we have $\varepsilon(V \otimes (\rho \oplus \rho^*)) = \varepsilon(V \otimes (\rho' \oplus \rho'^*))$ and $d(\mathscr{F}, \mathscr{F}') = 0$.*

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

Proof. Tate's local duality gives rise to a perfect pairing

$$X_+ \times X_- = H^1(\overline{T} \otimes \overline{\rho}_+) \times H^1(\overline{T} \otimes \overline{\rho}_-) \longrightarrow H^2(k(1)) \simeq k$$

(thus $\dim_k(X_+) = \dim_k(X_-)$) under which $Y_+^\perp = Y_-$ and $(Y'_+)^\perp = Y'_-$ [BK90, Proposition 3.8]. As in [Nek13, proof of Lemma 1.2], we have

$$\begin{aligned}\dim_k(Y_\pm) - \dim_k H^0(\overline{T} \otimes \overline{\rho}_\pm) &= \dim_{\mathcal{K}} H^1_f(V \otimes \rho_\pm) - \dim_{\mathcal{K}} H^0(V \otimes \rho_\pm) \\ &= \dim_{\mathcal{K}} D_{dR}(V \otimes \rho_\pm)/Fil^0,\end{aligned}$$

which does not depend on the sign $\pm$. Together with an analogous formula for $\rho'_\pm$ this implies that $\dim_k(Y_\pm) = \dim_k(X_\pm)/2 = \dim_k(Y'_\pm)$. As a result,

$$\begin{aligned}\dim_k(Y_+ \cap Y'_+) &= \dim_k(Y_+) + \dim_k(Y'_+) - \dim_k(Y_+ + Y'_+) = \dim_k(X_+) - \dim_k(Y_+ + Y'_+) \\ &= \dim_k(Y_+ + Y'_+)^\perp = \dim_k(Y_+^\perp \cap (Y'_+)^\perp) = \dim_k(Y_- \cap Y'_-),\end{aligned}$$

hence $d(\mathscr{F}, \mathscr{F}') = 0$. The local constants satisfy

$$\varepsilon = \varepsilon(V \otimes (\rho \oplus \rho^*)) = \det(V \otimes \rho)(-1) \equiv \det(V \otimes \rho')(-1) = \varepsilon(V \otimes (\rho' \oplus \rho'^*)) = \varepsilon' \pmod{\pi\mathcal{O}},$$

which implies that $\varepsilon = \varepsilon'$ (since $p \neq 2$). □

4. The global case

4.1 Let $\mathbf{Q}_p \subset \mathcal{K} \supset \mathcal{O} \longrightarrow \mathcal{O}/\pi\mathcal{O} = k$ be as in 2.1 (in particular, $p \neq 2$).

4.2 Let F be a number field and S a finite set of primes of F containing all infinite primes and all primes above p. Denote by $G_{F,S} = \mathrm{Gal}(F_S/F)$ the Galois group of the maximal extension of F unramified outside S.

4.3 Consider a global version of 2.16: let T (respectively, T') be a free $\mathcal{O}$-module of finite rank equipped with a continuous $\mathcal{O}$-linear action of $G_{F,S}$ and a skew-symmetric bilinear $G_{F,S}$-equivariant pairing $\langle\,,\rangle : T \times T \longrightarrow \mathcal{O}(1)$ (respectively, $\langle\,,\rangle' : T' \times T' \longrightarrow \mathcal{O}(1)$) whose reduction $\overline{T} \times \overline{T} \longrightarrow k(1)$ (respectively, $\overline{T}' \times \overline{T}' \longrightarrow k(1)$) modulo π is non-degenerate. Assume that there exists an isomorphism of $k[G_{F,S}]$-modules $\overline{T} \simeq \overline{T}'$ compatible with the above pairings; we fix it and use it to identify various cohomology groups of $\overline{T}'$ with those of $\overline{T}$. Set $V = T \otimes_{\mathcal{O}} \mathcal{K}$, $V' = T' \otimes_{\mathcal{O}} \mathcal{K}$ and assume that V and V' are potentially semistable representations of $G_v = \mathrm{Gal}(\overline{F}_v/F_v)$, for all $v \,|\, p$.

4.4 For finite primes $v \nmid p$ (respectively, $v \,|\, p$) of F we have the submodules $H^1_f(G_v, T) \subset H^1(G_v, T)$ and $H^1_f(G_v, T') \subset H^1(G_v, T')$ defined in 2.7 (respectively, in 3.2) and their images $\mathscr{F}_v, \mathscr{F}'_v \subset H^1(G_v, \overline{T})$, which are Lagrangian subspaces of $H^1(G_v, \overline{T})$. For $v \notin S$ the representations V and V' are unramified, hence $\mathscr{F}_v = \mathscr{F}'_v = H^1_{\mathrm{ur}}(G_v, \overline{T})$.

In other words, these subspaces define two *self-dual Selmer structures* [MR07, 1.2] $\mathscr{F} = \{\mathscr{F}_v\}$ and $\mathscr{F}' = \{\mathscr{F}'_v\}$ for the self-dual $k[G_{F,S}]$-module $\overline{T}$.

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

4.5 The corresponding Selmer groups are

$$H^1_{\mathscr{F}}(F,\overline{T}) = \mathrm{Ker}\Big(H^1(G_{F,S},\overline{T}) \longrightarrow \bigoplus_{v\in S_f} H^1(G_v,\overline{T})/\mathscr{F}_v\Big),$$
$$H^1_{\mathscr{F}'}(F,\overline{T}) = \mathrm{Ker}\Big(H^1(G_{F,S},\overline{T}) \longrightarrow \bigoplus_{v\in S_f} H^1(G_v,\overline{T})/\mathscr{F}'_v\Big),$$

where $S_f = S\backslash\{v \mid \infty\}$. Denote by $h^1_{\mathscr{F}}(F,\overline{T})$ (respectively, $h^1_{\mathscr{F}'}(F,\overline{T})$) their respective dimensions over k and let $h^0(F,\overline{T}) = \dim_k H^0(G_{F,S},\overline{T})$.

The existence of Flach's generalisation of the Cassels–Tate pairing [Fla90] implies [Nek13, (1.1.3)] that

$$\chi_f(F,V) \equiv h^1_{\mathscr{F}}(F,\overline{T}) - h^0(F,\overline{T}) \pmod 2,$$
$$\chi_f(F,V') \equiv h^1_{\mathscr{F}'}(F,\overline{T}) - h^0(F,\overline{T}) \pmod 2,$$

hence

$$\chi_f(F,V) - \chi_f(F,V') \equiv h^1_{\mathscr{F}}(F,\overline{T}) - h^1_{\mathscr{F}'}(F,\overline{T}) \pmod 2. \tag{4.5.1}$$

4.6 The right-hand side of (4.5.1) is given by a formula of Mazur and Rubin [MR07, Theorem 1.4]:

$$h^1_{\mathscr{F}}(F,\overline{T}) - h^1_{\mathscr{F}'}(F,\overline{T}) \equiv \sum_{v\in S_f} d(\mathscr{F}_v,\mathscr{F}'_v) \pmod 2, \tag{4.6.1}$$

where $d(\mathscr{F}_v,\mathscr{F}'_v) \equiv \dim_k \mathscr{F}_v/(\mathscr{F}_v\cap\mathscr{F}'_v) \pmod 2$, as in 2.8. Combining (4.6.1) with (4.5.1), we obtain

$$\chi_f(F,V) - \chi_f(F,V') \equiv \sum_{v\in S_f} d(\mathscr{F}_v,\mathscr{F}'_v) \pmod 2. \tag{4.6.2}$$

4.7 For each finite prime v of F, there are local constants $\varepsilon_v(V) = \varepsilon(V|_{G_v}) = \pm 1$ and $\varepsilon_v(V') = \varepsilon(V'|_{G_v}) = \pm 1$, equal to 1 for $v \notin S$. If V and V' are $\mathfrak{p}$-adic realisations of self-dual motives M and M' over F with isomorphic real Hodge realisations, then the archimedean L- and ε-factors of M and M' coincide and the conjectural equality (0.5) becomes

$$\prod_{v\in S_f} \varepsilon_v(V)/\varepsilon_v(V') \stackrel{?}{=} (-1)^{\chi_f(F,V)-\chi_f(F,V')} = \prod_{v\in S_f} (-1)^{d(\mathscr{F}_v,\mathscr{F}'_v)}, \tag{4.7.1}$$

which is equivalent, thanks to Theorem 2.17, to

$$\prod_{v\,|\,p} \varepsilon_v(V)/\varepsilon_v(V') \stackrel{?}{=} \prod_{v\,|\,p} (-1)^{d(\mathscr{F}_v,\mathscr{F}'_v)}. \tag{4.7.2}$$

If the discussion in § 3 applies at each $v\,|\,p$, then (4.7.2) holds term by term and we can go backwards from (4.7.2) to (4.7.1) and (0.5). Let us make this explicit in two cases corresponding to Propositions 3.6 and 3.9, respectively. The first case is covered in paragraphs 4.8 to 4.14 and the second case in paragraphs 4.15 and 4.16.

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

4.8 The first case involves abelian varieties with real multiplication. Let L be a totally real number field and A an abelian variety over F equipped with a ring morphism $\mathcal{O}_L \hookrightarrow \mathrm{End}_F(A)$. For each rational prime p, the decomposition $O_L \otimes \mathbf{Z}_p = \prod_{\mathfrak{p}\,|\,p} \mathcal{O}_{L,\mathfrak{p}}$ induces decompositions

$$T_p(A) = \prod_{\mathfrak{p}\,|\,p} T_{\mathfrak{p}}(A), \quad V_p(A) = \prod_{\mathfrak{p}\,|\,p} V_{\mathfrak{p}}(A)$$

($V_p(A)$ is a free $L \otimes \mathbf{Q}_p$-module). An $\mathcal{O}_L$-linear polarisation $\lambda : A \longrightarrow A^t$ defines skew-symmetric Weil pairings

$$T_{\mathfrak{p}}(A) \times T_{\mathfrak{p}}(A) \longrightarrow T_{\mathfrak{p}}(A) \otimes_{\mathcal{O}_{L,\mathfrak{p}}} T_{\mathfrak{p}}(A) \longrightarrow \mathbf{Z}_p(1),$$

hence $\mathcal{O}_{L,\mathfrak{p}}$-bilinear skew-symmetric pairings

$$\langle\,,\rangle : T_{\mathfrak{p}}(A) \times T_{\mathfrak{p}}(A) \longrightarrow \mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{O}_{L,\mathfrak{p}}, \mathbf{Z}_p)(1) \simeq \mathcal{O}_{L,\mathfrak{p}}(1).$$

If $\mathrm{Ker}(\lambda)[\mathfrak{p}] = 0$, then $T_{\mathfrak{p}}(A)$ is self-dual with respect to $\langle\,,\rangle$ in the sense of 2.4.

4.9 We consider $M = h^1(A)(1)$ as a (self-dual) motive with coefficients in L. Its $\mathfrak{p}$-adic realisations are $M_{\mathfrak{p}} = V_{\mathfrak{p}}(A)^*(1) \simeq V_{\mathfrak{p}}(A)$ and the Euler factors of its L-function

$$L_v(M,s) = \det(1 - \mathrm{Fr}_{\mathrm{geom}}(v)(Nv)^{-s} \mid M_{\mathfrak{p}}^{I_v})^{-1} \quad (v \nmid p)$$

have coefficients in L and do not depend on $\mathfrak{p}$. The L-functions $L(\iota M, s) = L(\iota A/F, s+1)$ for various embeddings $\iota : L \hookrightarrow \mathbf{R}$ are defined for $\mathrm{Re}(s) > 1/2$ and are related to the usual L-function of A (when we consider $h^1(A)$ as a motive with coefficients in $\mathbf{Q}$) by

$$L(A/F, s) = \prod_{\iota : L \hookrightarrow \mathbf{R}} L(\iota A/F, s). \tag{4.9.1}$$

The archimedean L- and ε-factors of $L(\iota M, s)$ are equal to

$$L_\infty(\iota M, s) = ((2\pi)^{-s}\Gamma(s))^{[F:\mathbf{Q}]\dim(A)/[L:\mathbf{Q}]}, \quad \varepsilon_\infty(\iota M) = (-1)^{(r_1(F)+r_2(F))\dim(A)/[L:\mathbf{Q}]}.$$

The global ε-factor $\varepsilon(\iota A/F) := \varepsilon(M) \in \{\pm 1\}$ does not depend on ι, but we keep ι in the notation in order not to confuse $\varepsilon(\iota A/F)$ with the ε-factor of the product L-function (4.9.1).

4.10 The representation $V_{\mathfrak{p}}(A)$ of G_F is pure of weight -1 at each finite prime of F, which implies that $h^0(F', V_{\mathfrak{p}}(A)) = 0$, for every finite extension F'/F. The rank of the Bloch–Kato Selmer group of $V_{\mathfrak{p}}(A)$ is equal to

$$h^1_f(F', V_{\mathfrak{p}}(A)) = \mathrm{rk}_{O_L} A(F') + \mathrm{cork}_{\mathcal{O}_{L,\mathfrak{p}}} Ш(A/F')[\mathfrak{p}^\infty].$$

4.11 Fix a prime $\mathfrak{p}$ of L dividing a rational prime $p \neq 2$ and let $\mathcal{K} = L_{\mathfrak{p}}$, $\mathcal{O} = \mathcal{O}_{L,\mathfrak{p}}$ and $k = \mathcal{O}/\mathfrak{p}$. Assume that

(4.11.1) A and A' are abelian varieties over F of the same dimension equipped with embeddings $\mathcal{O}_L \hookrightarrow \mathrm{End}_F(A), \mathrm{End}_F(A')$;

(4.11.2) there are $\mathcal{O}_L$-linear polarisations $\lambda : A \longrightarrow A^t$ and $\lambda' : A' \longrightarrow A'^t$ such that $\mathrm{Ker}(\lambda)[\mathfrak{p}] = \mathrm{Ker}(\lambda')[\mathfrak{p}] = 0$. As in 4.8, they give rise to self-dual $\mathcal{O}[G_{F,S}]$-modules (for suitable S) $T \times T \longrightarrow \mathcal{O}(1)$, $T' \times T' \longrightarrow \mathcal{O}(1)$, where $T = T_{\mathfrak{p}}(A) \subset V = V_{\mathfrak{p}}(A)$ and $T' = T_{\mathfrak{p}}(A') \subset V' = V_{\mathfrak{p}}(A')$;

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

(4.11.3) there exists an isomorphism of $k[G_{F,S}]$-modules $\overline{T} = T/\mathfrak{p}T \simeq \overline{T}' = T'/\mathfrak{p}T'$ compatible with the reductions modulo $\mathfrak{p}$ of the pairings from (4.11.2);

(4.11.4) the absolute ramification index of each prime $v \,|\, p$ of F satisfies $e(v \,|\, p) < p - 1$;

(4.11.5) A and A' have good reduction at all primes $v \,|\, p$ of F.

These assumptions imply that, for each $v \,|\, p$, the restrictions of T and T' to G_v satisfy (3.4.1)–(3.4.4) with $K_1 = K = F_v$.

THEOREM 4.12. *In the situation of 4.11, let F' be a finite extension of F and $\alpha : G_{F'} = \mathrm{Gal}(\overline{F}/F') \longrightarrow \{\pm 1\}$ a quadratic (or trivial) character. We have, for each $\iota : L \hookrightarrow \mathbf{R}$,*

$$(-1)^{h^1_f(F', V_{\mathfrak{p}}(A)\otimes\alpha)}/\varepsilon(\iota A \otimes \alpha/F') = (-1)^{h^1_f(F', V_{\mathfrak{p}}(A')\otimes\alpha)}/\varepsilon(\iota A' \otimes \alpha/F'),$$

where we have denoted by $A \otimes \alpha$ the quadratic twist of $A \otimes_F F'$ by α (and similarly for A').

Proof. Let $c(F', \alpha)$ be the quotient of the left-hand side by the right-hand side. If $\alpha \neq 1$, then $c(F', \alpha) = c(F'^{(\alpha)}, 1)/c(F', 1)$, where $F'^{(\alpha)} = \overline{F}^{\mathrm{Ker}(\alpha)}$. It follows that it is sufficient to prove the claim for $\alpha = 1$ (and varying F'). As explained in 4.7, this follows from Theorem 2.17 and Proposition 3.6 applied to T and T' over various completions of F'. □

4.13 If, in addition, $\dim(A) = \dim(A') = [L : \mathbf{Q}]$ and the field F' is totally real, then the abelian varieties A and A' (as well as their quadratic twists) are potentially modular over F' [BLGGT14, Corollary 5.4.2]. In particular, their L-functions over F' have meromorphic continuation to $\mathbf{C}$ and satisfy the expected functional equations [BLGGT14, Corollary 5.4.3]

$$(L_\infty \cdot L)(\iota A \otimes \alpha/F', s) = a^{s-1}\,\varepsilon(\iota A \otimes \alpha/F')(L_\infty \cdot L)(\iota A \otimes \alpha/F', 2-s),$$
$$(L_\infty \cdot L)(\iota A' \otimes \alpha/F', s) = b^{s-1}\,\varepsilon(\iota A' \otimes \alpha/F')(L_\infty \cdot L)(\iota A' \otimes \alpha/F', 2-s).$$

In particular, the analytic rank

$$r_{an}(\iota A \otimes \alpha/F') := \mathrm{ord}_{s=1} L(\iota A \otimes \alpha/F', s) \in \mathbf{Z}$$

is defined and satisfies

$$(-1)^{r_{an}(\iota A\otimes\alpha/F')} = \varepsilon(\iota A \otimes \alpha/F')$$

(and similarly for A'). The statement of Theorem 4.12 can be rewritten, therefore, as follows:

$$r_{an}(\iota A \otimes \alpha/F') - h^1_f(F', V_{\mathfrak{p}}(A) \otimes \alpha) \equiv r_{an}(\iota A' \otimes \alpha/F') - h^1_f(F', V_{\mathfrak{p}}(A') \otimes \alpha) \pmod 2. \quad (4.13.1)$$

THEOREM 4.14. *If, in the situation of Theorem 4.12, $\dim(A) = \dim(A') = [L : \mathbf{Q}]$, the field F' is totally real and A' does not have potentially good reduction everywhere, then we have, for each $\iota : L \hookrightarrow \mathbf{R}$,*

$$r_{an}(\iota A \otimes \alpha/F') \equiv h^1_f(F', V_{\mathfrak{p}}(A) \otimes \alpha) \pmod 2.$$

Proof. The assumption on A' implies, by [Nek13, Theorem 4.3(b)], that the right-hand side of (4.13.1) is equal to $0 \in \mathbf{Z}/2\mathbf{Z}$. □

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

4.15 We now consider a global situation in which Proposition 3.9 applies. Let T be as in 4.3 and let $F \subset F' \subset F_1$ be Galois extensions with Galois groups $\mathrm{Gal}(F_1/F) = D_{2n} \supset \mathrm{Gal}(F_1/F') = C_n$ (dihedral and cyclic group, respectively).

Assume that $\chi, \chi' : \mathrm{Gal}(F_1/F') \longrightarrow \mathcal{O}^\times$ are characters such that $(\chi'/\chi)^{p^m} = 1$ for some $m \geqslant 0$; then $\overline{\chi}' = \overline{\chi}$. Consider the induced representations $I(\chi) = \mathrm{Ind}_{C_n}^{D_{2n}}(\chi)$ and $I(\chi')$ as representations $G_{F,S} \longrightarrow \mathrm{GL}_2(\mathcal{O})$, for suitable S. They are self-dual in the sense that there exist symmetric isomorphisms $I(\chi) \simeq I(\chi)^*$ and $I(\chi') \simeq I(\chi')^*$. Again, $\overline{I(\chi)} = \overline{I(\chi')}$.

The following theorem is a generalisation of [Nek13, Theorem 1.1].

THEOREM 4.16. *In the situation of 4.15, assume that, for each prime $w \,|\, p$ of F' which is stable by $\mathrm{Gal}(F'/F)$, the character χ'/χ is unramified at w. Then we have*

$$(-1)^{h_f^1(F, V \otimes I(\chi))} \Big/ \prod_{v \nmid \infty} \varepsilon_v(V \otimes I(\chi)) = (-1)^{h_f^1(F, V \otimes I(\chi'))} \Big/ \prod_{v \nmid \infty} \varepsilon_v(V \otimes I(\chi')).$$

Proof. We apply the discussion in 4.7 to the pair of representations $T \otimes I(\chi)$ and $T \otimes I(\chi')$ of $G_{F,S}$. As before, we need to analyse the individual terms for $v \,|\, p$ in (4.7.2). If there is only one prime $w \,|\, v$ in F', our assumption implies that χ'/χ is trivial on the inertia group of w in F_1/F', hence on the full decomposition group of w in F_1/F', by [MR07, Lemma 6.5(i)]. Thus $I(\chi)|_{G_v} = I(\chi')|_{G_v}$, which implies that $\mathscr{F}_v = \mathscr{F}'_v$ and $\varepsilon_v(V \otimes I(\chi)) = \varepsilon_v(V \otimes I(\chi'))$. If $v\mathcal{O}_{F'} = ww'$, then $F'_w = F_v = F'_{w'}$ and $I(\chi)|_{G_v} = \chi_w \oplus \chi_w^{-1}$ (where $\chi_w = \chi|_{G_w}$), $I(\chi')|_{G_v} = \chi'_w \oplus \chi'^{-1}_w$. Proposition 3.9 then yields $d(\mathscr{F}_v, \mathscr{F}'_v) = 0$ and $\varepsilon_v(V \otimes I(\chi)) = \varepsilon_v(V \otimes I(\chi'))$. As a result, equality (4.7.2) holds in our situation, hence so does (4.7.1), as claimed. □

5. Elliptic curves with complex multiplication

5.1 Let $\overline{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, let $c \in G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be the complex conjugation. Fix an imaginary quadratic field $K \subset \overline{\mathbf{Q}}$.

5.2 Denote by H (respectively, by $H_g = H \cap \mathbf{Q}^{\mathrm{ab}}$) the Hilbert class field (respectively, the genus field) of K. If we write the discriminant of K in the form $D_K = -2^a p_1 \cdots p_r q_1 \cdots q_s$, where $p_j \equiv 1 \pmod 4$ and $q_k \equiv 3 \pmod 4$ are distinct primes, then

$$H_g = \begin{cases} H_0 & \text{if } a = 0, \\ H_0(i) & \text{if } a = 2, \\ H_0(\sqrt{(-1)^{s-1}2}) & \text{if } a = 3, \end{cases} \qquad H_0 = \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r}, i\sqrt{q_1}, \ldots, i\sqrt{q_s}).$$

The set of finite primes of the maximal real subfield H_g^+ of H_g which are ramified in H_g/H_g^+ is equal to

$$\mathrm{Ram}_f(H_g/H_g^+) = \begin{cases} \{v \,|\, 2\} & \text{if } s = 0 \ (\Longrightarrow a \neq 0), \\ \{v \,|\, q_1\} & \text{if } s = 1 \ (\Longrightarrow a \neq 2), \\ \emptyset & \text{if } s \geqslant 2. \end{cases}$$

5.3 The Galois group $\mathrm{Gal}(H/\mathbf{Q})$ is a semi-direct product $\mathrm{Gal}(H/K) \rtimes \{1, c\} \simeq Cl_K \rtimes \{1, c\}$, where $c^2 = 1$ and $cgc^{-1} = g^{-1}$ for each $g \in \mathrm{Gal}(H/K)$. This implies that the following properties are equivalent:

$$\begin{aligned} H \text{ is a CM field} &\Longleftrightarrow c \in Z(\mathrm{Gal}(H/\mathbf{Q})) \iff Cl_K^2 = \{1\} \\ &\Longleftrightarrow \mathrm{Gal}(H/\mathbf{Q}) \text{ is abelian} \iff H = H_g. \end{aligned}$$

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

There are 65 known imaginary quadratic fields K for which $H = H_g$, with the largest value of $|D_K|$ being equal to $5460 = 4 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. There is at most one additional K with $H = H_g$, but its existence would contradict the generalised Riemann hypothesis [Wei73].

PROPOSITION 5.4. *If E_1 is a elliptic curve defined over a subfield F of $\overline{\mathbf{Q}}$ for which $\mathcal{O} = \mathrm{End}_{\mathbf{Q}}(E_1)$ is an order in K, then there exists an isogeny $E_1 \longrightarrow E$ defined over F such that $\mathrm{End}_{\mathbf{Q}}(E) = \mathcal{O}_K$.*

Proof. If $\mathcal{O} = \mathbf{Z} + f\mathcal{O}_K$ is the order of conductor $f \geqslant 1$, then $E = E_1/\{P \in E_1(\overline{\mathbf{Q}}) \,|\, (f\mathcal{O}_K) \cdot P = 0\}$ has the required property. □

5.5 If E is an elliptic curve over $F \subset \overline{\mathbf{Q}}$ such that $\mathrm{End}_{\overline{\mathbf{Q}}}(E) = \mathcal{O}_K$ and $j(E) \in \mathbf{R}$, then $FK \supset K(j(E)) = H$, $F \supsetneq H^+ := \mathbf{Q}(j(E))$ and there exists an elliptic curve E_0 over H^+ such that $E_0 \otimes_{H^+} \overline{\mathbf{Q}} \simeq E \otimes_F \overline{\mathbf{Q}}$.

The set of H^+-isomorphism classes of such curves E_0 (modulo quadratic twists with respect to the quadratic extension H/H^+) is in a bijection with the set of algebraic Hecke characters

$$\psi : \mathbf{A}_H^\times \twoheadrightarrow \mathbf{A}_H^\times/(H \otimes \mathbf{R})^\times = \widehat{H}^\times \longrightarrow K^\times, \quad \psi|_{H^\times} = N_{H/K} \tag{5.5.1}$$

which are c-equivariant ($\psi \circ c = c \circ \psi$). See [Shi71, Corollary, Theorem 10] and [Gro80, Theorems 10.1.3 and 10.2.1].

Each of the two curves corresponding to ψ has bad reduction at a prime v of H^+ if and only if v is ramified in H/H^+ or there is $w \,|\, v$ in H at which ψ is ramified (i.e. $\psi_w(\mathcal{O}_{H,w}^\times) \neq \{1\}$).

Note that a prime v ramified in H/H^+ always lies above a prime in $\mathrm{Ram}_f(H_g/H_g^+)$, since $H^+ \cap H_g = H_g^+$ and H/H_g is unramified.

PROPOSITION 5.6. *Let E be as in 5.5. If $K \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-3})$ and if p is a rational prime not dividing $2D_K$, then there exists E_0 as in 5.5 (which is equivalent to E being a quadratic twist of $E_0 \otimes_{H^+} F$, since $\mathrm{Aut}_{\overline{\mathbf{Q}}}(E) = \{\pm 1\}$) with good reduction at all primes above p.*

Proof. Let E_1 be any elliptic curve over H^+ such that $E_1 \otimes_{H^+} \overline{\mathbf{Q}} \simeq E \otimes_F \overline{\mathbf{Q}}$. Denote by ψ the Hecke character (5.5.1) corresponding to E_1. Its p-component $\psi_p : (H \otimes \mathbf{Q}_p)^\times \longrightarrow K^\times$ maps $(\mathcal{O}_H \otimes \mathbf{Z}_p)^\times$ to $(K^\times)_{\mathrm{tors}} = \{\pm 1\}$, hence factors through $(\mathcal{O}_H \otimes \mathbf{F}_p)^\times \longrightarrow \{\pm 1\}$ (since $p \neq 2$). It is also trivial on ${}^{1-c}(\mathcal{O}_H \otimes \mathbf{F}_p)^\times$, which coincides, by Hilbert's Theorem 90, with the kernel of the surjective norm map $N_{H/H^+} : (\mathcal{O}_H \otimes \mathbf{F}_p)^\times \twoheadrightarrow (\mathcal{O}_{H^+} \otimes \mathbf{F}_p)^\times$ (the assumption $p \nmid D_K$ implies that p is unramified in $H/\mathbf{Q}$). It follows that the restriction of ψ_p to $(\mathcal{O}_H \otimes \mathbf{Z}_p)^\times$ factors as $\eta_p \circ N_{H/H^+}$ for some $\eta_p : (\mathcal{O}_{H^+} \otimes \mathbf{F}_p)^\times \longrightarrow \{\pm 1\}$. There exists $\eta : \mathbf{A}_{H^+}^\times/(H^+)^\times \longrightarrow \{\pm 1\}$ whose p-component is equal to η_p. The character $\psi \cdot (\eta \circ N_{H/H^+})$ then corresponds to an elliptic curve E_0 with the desired properties. □

5.7 It may be worthwhile to recall that there are much sharper results than Proposition 5.6 (even though they will not be needed in the proof of Theorem 5.10 below). Let E and K be as in Proposition 5.6.

(A) [Shi71, Example 3], [Gro80, Theorem 11.2.4]. If there is a prime $q \,|\, D_K$ such that $q \equiv 3 \pmod 4$, then $q\mathcal{O}_K = Q^2$ and the character

$$\varphi : (\widehat{\mathcal{O}}_K)^\times \twoheadrightarrow \mathcal{O}_{K,Q}^\times \twoheadrightarrow (\mathcal{O}/Q)^\times = (\mathbf{Z}/q\mathbf{Z})^\times \xrightarrow{\chi_q} \{\pm 1\}$$

(where $\chi_q(a) = \left(\frac{a}{q}\right)$ is the Legendre symbol) satisfies

$$\varphi \circ c = \varphi, \quad \varphi|_{(\widehat{\mathcal{O}}_K)^\times \cap K^\times} = \varphi|_{\mathcal{O}_K^\times} = \varphi|_{\{\pm 1\}} = \mathrm{id}.$$

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

It extends, therefore (in a unique way) to a morphism $\varphi : K^\times(\widehat{\mathcal{O}}_K)^\times \longrightarrow K^\times$ such that $\varphi|_{K^\times} = \mathrm{id}$ (and $\varphi \circ c = \varphi$, by uniqueness). The Hecke character

$$\psi = \varphi \circ N_{H/K} : \mathbf{A}_H^\times \twoheadrightarrow \widehat{H}^\times \xrightarrow{N_{H/K}} K^\times(\widehat{\mathcal{O}}_K)^\times \xrightarrow{\varphi} K^\times \tag{5.7.1}$$

then corresponds to an elliptic curve E_0 over H^+ (together with its quadratic twist with respect to H/H^+) as in 5.5, which has good reduction at all primes $v \nmid q$ of H^+.

A more refined argument [Roh82] shows that if D_K is divisible by two distinct primes q_1, $q_2 \equiv 3 \pmod 4$, then there exists E_0 as in 5.5 with good reduction at all primes of H^+.

(B) If $8 \mid D_K$, then $2\mathcal{O}_K = P^2$ and $K_P = \mathbf{Q}_2(x)$ with $x^2 = -2$ or -10. We claim that there exists a character

$$\varphi : (\widehat{\mathcal{O}}_K)^\times \twoheadrightarrow \mathcal{O}_{K,P}^\times \xrightarrow{\alpha} \mathcal{O}_{K,P}^\times / {}^{1-c}(\mathcal{O}_{K,P}^\times)(\mathcal{O}_{K,P}^\times)^2 \longrightarrow \{\pm 1\}$$

such that $\varphi(-1) = -1$. It is enough to check that $\alpha(-1) \neq 1$, which follows from the fact that

$$\begin{aligned} {}^{1-c}(\mathcal{O}_{K,P}^\times) \pmod 8 &= \{1, 1+4x, -3 \pm 2x \pmod 8\}, \\ (\mathcal{O}_{K,P}^\times)^2 \pmod 8 &= \{1, 1+4x, -1 \pm 2x \pmod 8\}. \end{aligned}$$

As in (A), it follows that φ extends in a unique way to $\varphi : K^\times(\widehat{\mathcal{O}}_K)^\times \longrightarrow K^\times$ such that $\varphi|_{K^\times} = \mathrm{id}$. Formula (5.7.1) then defines a Hecke character corresponding to a pair of elliptic curves E_0 as in 5.5 with good reduction at all primes $v \nmid 2$ of H^+.

(C) Both constructions (A) and (B) yield $\mathbf{Q}$-curves, but no such curves exist if $D_K = -4p_1 \cdots p_r$, where $p_j \equiv 1 \pmod 4$ are distinct primes [Gro80, § 11], [Nak04, Proposition 5]. For reasons explained in 5.8 below we are particularly interested in imaginary quadratic fields K for which $H = H_g$. Among the 65 known fields of this type there are four whose discriminant is of the form $D_K = -4p_1 \cdots p_r$, namely,

$$\begin{cases} D_K = -4p, & p \in \{5, 13, 37\}; \\ D_K = -4 \cdot 5 \cdot 17. \end{cases}$$

In each of the first three cases $D_K = -4p$ we have $H^+ = \mathbf{Q}(\sqrt{p})$, $H = H^+(i)$, $h_K = 2$ and $h_{H^+} = 1$, which implies that $h_H = 1$ [FT93, Theorem 74, Corollary 1]. The group of units is equal to $\mathcal{O}_H^\times = \mu_4 \cdot \varepsilon^{\mathbf{Z}}$, where $\varepsilon = (1+\sqrt{5})/2$, $(3+\sqrt{13})/2$ and $6+\sqrt{37}$, respectively. The prime 2 remains inert in $H^+/\mathbf{Q}$ and $\mathrm{Ram}_f(H/H^+) = \{(2)\}$: $2\mathcal{O}_H = P^2$.

We claim that there is a c-equivariant Hecke character (5.5.1) of the form

$$\psi : \mathbf{A}_H^\times \twoheadrightarrow \widehat{H}^\times = H^\times(\widehat{\mathcal{O}}_H)^\times \xrightarrow{\varphi} K^\times, \tag{5.7.2}$$

where $\varphi|_{H^\times} = N_{H/K}$ and

$$\begin{aligned} \varphi|_{(\widehat{\mathcal{O}}_H)^\times} : (\widehat{\mathcal{O}}_H)^\times \twoheadrightarrow \mathcal{O}_{H,P}^\times \xrightarrow{\alpha} \mathcal{O}_{H,P}^\times / {}^{1-c}\mathcal{O}_{H,P}^\times (\mathcal{O}_{H,P}^\times)^2 \mu_4 \\ \xrightarrow{N_{H/H^+}} N_{H/H^+}(\mathcal{O}_{H,P}^\times)/N_{H/H^+}(\mathcal{O}_{H,P}^\times)^2 \xrightarrow{\overline{\varphi}} \{\pm 1\}. \end{aligned}$$

It is enough to check that the composite map $\beta = \overline{\varphi} \circ N_{H/H^+} \circ \alpha : \mathcal{O}_{H,P}^\times \longrightarrow \{\pm 1\}$ satisfies, for a suitable choice of $\overline{\varphi}$,

$$\beta|_{(\widehat{\mathcal{O}}_H)^\times \cap H^\times} = \beta|_{\mathcal{O}_H^\times} = N_{H/K}|_{\mathcal{O}_H^\times}.$$

This is equivalent to $N_{H/H^+}(\alpha(\varepsilon)) \neq 1$, since $N_{H/K}(\varepsilon) = -1$ and $N_{H/K}(\mu_4) = \{1\}$.

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

If $N_{H/H^+}(\alpha(\varepsilon)) = 1$, then $\varepsilon^2 \in N_{H/H^+}(\mathcal{O}_{H,P}^\times)^2$ and there exists $u = \pm 1$ such that $u\varepsilon \in N_{H/H^+}(\mathcal{O}_{H,P}^\times)$. However, the quadratic Hilbert symbols $(u\varepsilon, -1)_v$ over various completions of H^+ are given by

$$(\pm\varepsilon, -1)_v = \begin{cases} 1 & \text{if } v \nmid 2\infty, \\ \pm 1 & \text{if } v = \infty_1, \\ \mp 1 & \text{if } v = \infty_2. \end{cases}$$

The quadratic reciprocity law over H^+ then implies that $(\pm\varepsilon, -1)_{(2)} = -1$, hence $\pm\varepsilon \notin N_{H/H^+}(\mathcal{O}_{H,P}^\times)$. It follows that there exists $\overline{\varphi}$ such that $\beta(\varepsilon) = -1$. This yields a Hecke character ψ as in (5.7.2), which corresponds to a pair of elliptic curves E_0 as in 5.5 with good reduction at all primes $v \nmid 2$ of H^+.

5.8 Assume that E is an elliptic curve defined over a *totally real* field $F \subset \overline{\mathbf{Q}}$ and $\mathrm{End}_{\overline{\mathbf{Q}}}(E) = \mathcal{O}_K$. The field $H^+ = \mathbf{Q}(j(E)) \subset F$ is then totally real and $H = K(j(E))$ is a CM field, hence $H = H_g$ and $H^+ = H_g^+$ (in particular, if $2 \nmid [F : \mathbf{Q}]$, then $H^+ = \mathbf{Q}$ and $h_K = 1$).

The discussion in 5.7 implies that if $D_K \neq -3, -4$ is not equal to $-4 \cdot 5 \cdot 17$ (nor to the mythical 66th discriminant) and if there exists a prime $q \equiv 3 \pmod 4$ dividing D_K (respectively, if no such prime q exists), then there exists a quadratic twist of E of the form $E_0 \otimes_{H_g^+} F$, where E_0 is an elliptic curve over H_g^+ with good reduction outside primes above q (respectively, with good reduction outside primes above 2). However, this statement will not be used in the proof of Theorem 5.10 below (Proposition 5.6 will suffice).

5.9 If E is an elliptic curve defined over a totally real field $F \subset \overline{\mathbf{Q}}$, then E is potentially modular [Win09, Theorem A.1] and the analytic rank

$$r_{an}(E/F) = \mathrm{ord}_{s=1} L(E/F, s) \in \mathbf{Z}$$

is well defined (cf. the discussion in [Nek13, 4.2]). For each rational prime p, the rank of the Bloch–Kato Selmer group $h^1_f(F', V_p(E))$ over any finite extension F' of F coincides with

$$s_p(E/F') = \mathrm{rk}_{\mathbf{Z}} E(F') + \mathrm{cork}_{\mathbf{Z}_p} Ш(E/F')[p^\infty].$$

The mod-2 version of the Bloch–Kato conjecture (0.2) boils down to

$$r_{an}(E/F) \equiv s_p(E/F) \pmod 2 \qquad (\star)$$

(the 'p-parity conjecture' for E over F). As shown in [Nek13, Theorem A], the congruence $(\star)$ holds in the following cases.

(5.9.1) E does not have complex multiplication.

(5.9.2) E has complex multiplication and $2 \nmid [F : \mathbf{Q}]$ (this can happen only if the class number of $K = \mathrm{End}_{\overline{\mathbf{Q}}}(E) \otimes \mathbf{Q}$ is equal to 1).

(5.9.3) $p \neq 2$ and E does not acquire good reduction everywhere over any cyclic extension of F [Nek13, Theorem 1.4(c)].

(5.9.4) E has complex multiplication by $K = \mathrm{End}_{\overline{\mathbf{Q}}}(E) \otimes \mathbf{Q}$ and p splits in $K/\mathbf{Q}$.

(5.9.5) E has complex multiplication by $K = \mathrm{End}_{\overline{\mathbf{Q}}}(E) \otimes \mathbf{Q}$ and p is ramified in $K/\mathbf{Q}$.

As (5.9.5) was not stated explicitly in [Nek13], here is the argument. The conjecture $(\star)$ is invariant under isogeny, so we can assume that $\mathrm{End}_{\overline{\mathbf{Q}}}(E) = \mathcal{O}_K$, by Proposition 5.4. The p-torsion

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

$E[p]$ is a reducible $\mathbf{F}_p[G_F]$-module, since the cyclic subgroup $E[P]$ (where $p\mathcal{O}_K = P^2$) is stable under G_F. However, in the reducible case the p-parity conjecture is known: [DD11, Corollary 5.8] if $p = 2, 3$; [CFKS10, Theorem 2.1] if $p > 3$ and the reduction type of E at primes above p is not too bad; the remaining cases follow from (5.9.3) (or from [Čes14]).

The case $p = 2$ is somewhat special. The argument in [Nek13] used in a crucial way the fact proved in [DD11, Corollary 4.8] that ($\star$) holds for $p = 2$ over any quadratic extension of F.

We will now prove ($\star$) in most of the remaining cases (for $p \neq 2$).

THEOREM 5.10. *Let F be a totally real number field and E an elliptic curve defined over F with complex multiplication by $K = \mathrm{End}_{\overline{\mathbf{Q}}}(E) \otimes \mathbf{Q} \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-3})$. Then the p-parity conjecture*

$$r_{an}(E/F) \equiv s_p(E/F) \pmod 2$$

holds for all primes $p \nmid 2D_K$ (note that the case $p \mid D_K$ is covered by (5.9.5)).

Proof. Thanks to Proposition 5.4 we can assume that $\mathrm{End}_{\overline{\mathbf{Q}}}(E) = \mathcal{O}_K$. Recall from 5.8 that $H = H_g$. According to Proposition 5.6 there exists an elliptic curve E_0 over the real abelian field $F_0 = H^+ = H_g^+$ with good reduction at all primes above p such that E is the twist of $E_0 \otimes_{F_0} F$ by a suitable character $\alpha : G_F \longrightarrow \{\pm 1\}$. The p-torsion $E_0[p]$ is an absolutely irreducible $\mathbf{F}_p[G_{F_0}]$-module, since $\mathrm{Im}(G_{F_0} \longrightarrow \mathrm{Aut}(E_0[p]) \simeq \mathrm{GL}_2(\mathbf{F}_p))$ is the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$.

We now apply the level-raising machinery to the cuspidal Hilbert modular eigenform with complex multiplication g_0 over F_0 attached to E_0. It has parallel weight 2, trivial character and level $\mathfrak{n}$ prime to p. If v is a finite prime of F_0 not dividing $p\mathfrak{n}$, the Hecke operator $T(v)$ acts on g_0 with an eigenvalue $\lambda_{g_0}(v) \in \mathbf{Z}$ satisfying

$$\det(1 - X\,\mathrm{Fr}_{\mathrm{geom}}(v) \mid V_p(E_0)(-1)) = 1 - \lambda_{g_0}(v)X + (Nv)X^2. \tag{5.10.1}$$

According to [Rib90, Theorem 1] if $F_0 = \mathbf{Q}$ (respectively, [Tay89] combined with [DS74, Lemme 6.11] and the Jacquet–Langlands correspondence if $2 \mid [F_0 : \mathbf{Q}]$), there exist a prime v_0 of F_0 not dividing $p\mathfrak{n}$, and a cuspidal eigenform g of parallel weight 2, trivial character and level dividing $v_0\mathfrak{n}$, which is new at v_0 and whose Hecke eigenvalues satisfy

$$\forall v \nmid pv_0\mathfrak{n}, \quad \lambda_g(v) \equiv \lambda_{g_0}(v) \pmod{\mathfrak{p}}, \tag{5.10.2}$$

for some prime $\mathfrak{p} \mid p$ in the (totally real) number field L generated by the Hecke eigenvalues of g. Moreover, the $\mathfrak{p}$-adic Galois representation attached to g is of the form $V_{\mathfrak{p}}(A')(-1)$, where A' is an abelian variety over F_0 with $\mathcal{O}_L \subset \mathrm{End}_{F_0}(A')$ and $\dim(A') = [L : \mathbf{Q}]$ (A' arises as a simple quotient of the Jacobian of a suitable modular (respectively, Shimura) curve).

Combining (5.10.2) with (5.10.1) and its analogue for g, we deduce from the Čebotarev density theorem that

$$\forall g \in G_{F_0}, \quad \mathrm{Tr}(g \mid V_p(E_0)) \equiv \mathrm{Tr}(g \mid V_{\mathfrak{p}}(A')) \pmod{\mathfrak{p}}. \tag{5.10.3}$$

The representations $V = V_p(E_0) \otimes_{\mathbf{Q}_p} L_{\mathfrak{p}}$ and $V' = V_{\mathfrak{p}}(A')$ of G_{F_0} are two-dimensional over $\mathcal{K} = L_{\mathfrak{p}}$ and self-dual in the sense of 2.3. After rescaling the corresponding pairings $\langle\,,\rangle : V \times V \longrightarrow \mathcal{K}(1)$ and $\langle\,,\rangle' : V' \times V' \longrightarrow \mathcal{K}(1)$, we can assume that there exist G_{F_0}-stable self-dual lattices $T \subset V$ and $T' \subset V'$ (cf. 2.5).

The congruence (5.10.3) implies that the $k[G_{F_0}]$-modules (where $k = \mathcal{O}_L/\mathfrak{p}$) $\overline{T} = T/\mathfrak{p}T$ and $\overline{T}' = T'/\mathfrak{p}T'$ have isomorphic semi-simplifications. However, $\overline{T}^{\mathrm{ss}} \simeq E_0[p]^{\mathrm{ss}} \otimes k = E_0[p] \otimes k$ is an absolutely irreducible $k[G_{F_0}]$-module. It follows that $\overline{T} \simeq \overline{T}' \simeq E_0[p] \otimes k$ and that T (respectively,

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press

T') is unique up to a scalar multiple, hence is homothetic to $T_p(E_0) \otimes_{\mathbf{Z}_p} \mathcal{O}_{L,\mathfrak{p}}$ (respectively, to $T_{\mathfrak{p}}(A')$).

Consequently, the abelian varieties $A = E_0 \otimes \mathcal{O}_L$ and A' defined over the field F_0 satisfy (4.11.1)–(4.11.2). Moreover, the isomorphism $\overline{T} \simeq \overline{T}'$ is compatible with the reductions modulo $\mathfrak{p}$ of the pairings $\langle\,,\rangle$ and $\langle\,,\rangle'$, possibly after multiplying one of them by a suitable element of $\mathcal{O}^\times = \mathcal{O}_{L,\mathfrak{p}}^\times$, since the space of $k[G_{F_0}]$-equivariant skew-symmetric isomorphisms $\overline{T} \simeq \overline{T}^*(1)$ is one-dimensional over k. Thus (4.11.3) is also satisfied. Finally, $p \nmid D_K$ is unramified in $F_0/\mathbf{Q}$ and both A and A' have good reduction at all primes of F_0 above p, since the levels of both g_0 and g are prime to p. As a result, (4.11.4)–(4.11.5) also hold.

The form g is new at v_0, which implies that the abelian variety A' has totally toric reduction at v_0. It follows that the assumptions of Theorem 4.14 are satisfied for A and A' (with F/F_0 replacing the extension F'/F from 4.13). The statement of Theorem 4.14 then becomes ($\star$), since

$$L(\iota A \otimes \alpha/F, s) = L(E/F, s), \quad h^1_f(F, V_{\mathfrak{p}}(A) \otimes \alpha) = s_p(E/F). \qquad \square$$

5.11 The argument in the proof of Theorem 5.10 also works for $K = \mathbf{Q}(i)$ (respectively, $K = \mathbf{Q}(\sqrt{-3})$), provided that $p \neq 2$ (respectively, $p > 3$) and that there exists an elliptic curve E_0 over $\mathbf{Q}$ with good reduction at p such that E is a quadratic twist of $E_0 \otimes_{\mathbf{Q}} F$.

5.12 Putting together 5.9–5.11, we see that the conjecture ($\star$) for totally real number fields F has been established in all non-CM cases and in at least $(1 - 2/65 \times 1/4) > 99\%$ of CM cases, namely, in all cases except the following two:

(5.12.1) $p \neq 2$, E has complex multiplication by $K = \mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-3})$, p is inert in $K/\mathbf{Q}$, $2 \,|\, [F : \mathbf{Q}]$, E acquires good reduction everywhere over a cyclic extension of F, and no quadratic twist of E descends to an elliptic curve defined over $\mathbf{Q}$ which has good reduction at p;

(5.12.2) $p = 2$, E has complex multiplication by K, 2 is inert in $K/\mathbf{Q}$, $2 \,|\, [F : \mathbf{Q}]$, and E does not descend to any subfield $F_1 \subset F$ such that $[F : F_1] = 2$.

5.13 Note that if ($\star$) holds for E and all its quadratic twists over F, then

$$r_{an}(E/F') \equiv s_p(E/F') \pmod 2$$

holds for any tower of finite extensions $F \subset F_1 \subset F'$, where F_1/F is abelian and F'/F_1 is a Galois extension of odd degree [Nek06, 12.11.7–8].

References

BLGGT14 T. Barnet-Lamb, T. Gee, D. Geraghty and R. Taylor, *Potential automorphy and change of weight*, Ann. of Math. (2) **179** (2014), 501–609.

BK90 S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, in *The Grothendieck Festschrift I*, Progress in Mathematics, vol. 86 (Birkhäuser, Boston, 1990), 333–400.

Čes14 K. Česnavičius, *The p-parity conjecture for elliptic curves with a p-isogeny*, J. Reine Angew. Math., doi:10.1515/crelle-2014-0040.

Che10 S. Chetty, *Comparing local constants of elliptic curves in dihedral extensions*, Preprint (2010), arXiv:1002.2671.

CFKS10 J. Coates, T. Fukaya, K. Kato and R. Sujatha, *Root numbers, Selmer groups and non-commutative Iwasawa theory*, J. Algebraic Geom. **19** (2010), 19–97.

Del73 P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, in *Modular functions of one variable II (Antwerp, 1972)*, Lecture Notes in Mathematics, vol. 349 (Springer, Berlin, 1973), 501–597.

DS74 P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. Éc. Norm. Supér. (4) **7** (1974), 507–530.

DD09 T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), 23–71.

DD11 T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39–64.

Fla90 M. Flach, *A generalization of the Cassels–Tate pairing*, J. reine angew. Math. **412** (1990), 113–127.

Fon94 J.-M. Fontaine, *Représentations ℓ-adiques potentiellement semi-stables*, in *Périodes p-adiques (Bures-sur-Yvette, 1988)*, Astérisque, vol. 223 (Société Mathématique de France, Paris, 1994), 321–347.

FM95 J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, in *Elliptic curves, modular forms and Fermat's last theorem (Hong Kong, 1993)*, Series on Number Theory, vol. I (International Press, Cambridge, MA, 1995), 41–78.

FPR94 J.-M. Fontaine and B. Perrin-Riou, *Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L*, in *Motives (Seattle, 1991)*, Proceedings of Symposia in Pure Mathematics, vol. 55/I (American Mathematical Society, Providence, RI, 1994), 599–706.

FT93 A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27 (Cambridge University Press, Cambridge, 1993).

Gro80 B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics, vol. 776 (Springer, Berlin, 1980).

KMR13 Z. Klagsbrun, B. Mazur and K. Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), 287–320.

Maz72 B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

MR04 B. Mazur and K. Rubin, *Kolyvagin systems*, in *Memoirs of the American Mathematical Society,* no. 799, vol. 168 (American Mathematical Society, Providence, RI, 2004).

MR07 B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), 581–614.

MR08 B. Mazur and K. Rubin, *Growth of Selmer rank in nonabelian extensions of number fields*, Duke Math. J. **143** (2008), 437–461.

Nak04 T. Nakamura, *A classification of* **Q***-curves with complex multiplication*, J. Math. Soc. Japan **56** (2004), 635–648.

Nek06 J. Nekovář, *Selmer complexes*, Astérisque, vol. 310 (Société Mathématique de France, Paris, 2006).

Nek07 J. Nekovář, *On the parity of ranks of Selmer groups III*, Doc. Math. **12** (2007), 243–274; Erratum: Doc. Math. **14** (2009), 191–194.

Nek09 J. Nekovář, *On the parity of ranks of Selmer groups IV*, Compositio Math. **145** (2009), 1351–1359.

Nek12 J. Nekovář, *Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight two*, Canad. J. Math. **64** (2012), 588–668.

Nek13 J. Nekovář, *Some consequences of a formula of Mazur and Rubin for arithmetic local constants*, Algebra Number Theory **7** (2013), 1101–1120.

Ray74 M. Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.

Rib90 K. Ribet, *Raising the levels of modular representations*, in *Séminaire de Théorie des Nombres, Paris 1987–88*, Progress in Mathematics, vol. 81 (Birkhäuser, Boston, 1990), 259–271.

Roh82 D. Rohrlich, *Elliptic curves with good reduction everywhere*, J. Lond. Math. Soc. (2) **25** (1982), 216–222.

Shi71 G. Shimura, *On the zeta-function of an abelian variety with complex multiplication*, Ann. of Math. (2) **94** (1971), 504–533.

Tay89 R. Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), 265–280.

Wei73 P.J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. **22** (1973), 117–124.

Win09 J.-P. Wintenberger, *Potential modularity of elliptic curves over totally real fields*, appendix to [Nek09].

Jan Nekovář jan.nekovar@imj-prg.fr
Université Pierre et Marie Curie (Paris 6), Institut de Mathématiques de Jussieu,
Théorie des Nombres, Case 247, 4 place Jussieu, F-75252, Paris cedex 05, France

https://doi.org/10.1112/S0010437X14008069 Published online by Cambridge University Press