Bulletin

de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

INVARIANCE OF THE PARITY CONJECTURE

Thomas de La Rochefoucauld

Tome 139
Fascicule 4

2011

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Publié avec le concours du Centre national de la recherche scientifique

pages 571-592

Bull. Soc. math. France
139 (4), 2011, p. 571–592

INVARIANCE OF THE PARITY CONJECTURE FOR p-SELMER GROUPS OF ELLIPTIC CURVES IN A D_{2p^n}-EXTENSION

by Thomas de La Rochefoucauld

Abstract. — We show a p-parity result in a D_{2p^n}-extension of number fields L/K ($p \geq 5$) for the twist $1 \oplus \eta \oplus \tau$: $W(E/K, 1 \oplus \eta \oplus \tau) = (-1)^{\langle 1\oplus\eta\oplus\tau, X_p(E/L)\rangle}$, where E is an elliptic curve over K, η and τ are respectively the quadratic character and an irreductible representation of degree 2 of $\mathrm{Gal}(L/K) = D_{2p^n}$, and $X_p(E/L)$ is the p-Selmer group. The main novelty is that we use a congruence result between ε_0-factors (due to Deligne) for the determination of local root numbers in bad cases (places of additive reduction above 2 and 3). We also give applications to the p-parity conjecture (using the machinery of the Dokchitser brothers).

Résumé (*Invariance de la conjecture de parité des p-groupes de Selmer de courbes elliptiques dans une D_{2p^n}-extension*)

On démontre un résultat de p-parité, dans une extension galoisienne de corps de nombre de groupe D_{2p^n}, pour le twist $1 \oplus \eta \oplus \tau$:
$$W(E/K, 1 \oplus \eta \oplus \tau) = (-1)^{\langle 1\oplus\eta\oplus\tau, X_p(E/L)\rangle},$$
où E est une courbe elliptique définie sur K, η et τ sont respectivement le caractère quadratique et une représentation irréductible de degré 2 de $\mathrm{Gal}(L/K) = D_{2p^n}$, et $X_p(E/L)$ est le p-groupe de Selmer. La principale nouveauté est le fait que l'on utilise un résultat de congruence (dû à Deligne) pour déterminer les « root numbers » locaux dans les mauvais cas (les places additives au-dessus de 2 et 3). On donne aussi, en utilisant la machinerie des frères Dokchitser, deux applications à la conjecture de p-parité.

Texte reçu le 18 février 2010, révisé et accepté le 21 février 2011.

Thomas de La Rochefoucauld, 4 place Jussieu, 75005 Paris •
E-mail : `thomas@math.jussieu.fr` • *Url :* `http://people.math.jussieu.fr/~thomas/`

2000 Mathematics Subject Classification. — 11G05, 11G07, 11G40.

Key words and phrases. — Elliptic curves, Birch and Swinnerton-Dyer conjecture, parity conjecture, regulator constants, epsilon factors, root numbers.

1. Introduction

1.1. The conjecture of Birch and Swinnerton-Dyer and the parity conjecture. — Let K be a number field and E an elliptic curve defined over K. Denote by K_v the completion of K at a place v.

We recall a few definitions:

Definition 1.1 (Tate Module). — *The l-adic Tate module of E is the inverse limit of the system of multiplication by l maps $E[l^{n+1}] \longrightarrow E[l^n]$, where $E[m]$ denotes the kernel of multiplication by m on E. Set*

$$T_l(E) = \varprojlim E[l^n], V_l(E) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(E)$$

and

$$\sigma'_{E/K_v,l} : \mathrm{Gal}(\overline{K}_v/K_v) \longrightarrow \mathrm{GL}(V_l(E)^*).$$

Fix an embedding, $\iota : \mathbb{Q}_l \hookrightarrow \mathbb{C}$; we can then associate to $\sigma'_{E/K_v,l}$ a complex representation $\sigma'_{E/K_v,l,\iota}$ of the Weil-Deligne group (see [9] *§13).*

Remark 1.2. — *One can show that the isomorphism class of $\sigma'_{E/K_v} := \sigma'_{E/K_v,l,\iota}$ is independent of the choice of l and ι (see* [9] *§13, §14, §15).*

Denote by $L(E/K, s)$ the global L-function, product of local L-functions:

$$L(E/K,s) = \prod_{v \text{ finite}} L(E/K_v, s) \left(= \prod_{v \text{ finite}} L(\sigma'_{E/K_v}, s)\right)$$

defined for $\mathrm{Re}(s) > \frac{3}{2}$ (see [9] §17 for the correspondence between the classical definition of $L(E/K_v, s)$ and the one using σ'_{E/K_v}) and by

$$\Lambda(E/K, s) = A(E/K)^{s/2} L(E/K, s)(2(2\pi)^{-s}\Gamma(s))^{[K:\mathbb{Q}]},$$

the "complete" L-function where $A(E/K)$ is a constant depending on the disciminant and the conductor of E/K (see [9] §21).

Recall the following classical conjectures:

Conjecture 1.3 (Birch and Swinnerton-Dyer: BSD). — *We have*

$$\mathrm{ord}_{s=1}\Lambda(E/K, s) = rk(E/K).$$

Conjecture 1.4 (Functional equation of Λ : FE). — *$L(E/K, s)$ has a holomorphic continuation to $\mathbb{C}$ and there is a number*

$$W(E/K) = \prod_v W(E/K_v) \in \{\pm 1\}$$

such that:

$$\Lambda(E/K, s) = W(E/K)\Lambda(E/K, 2 - s)$$

(see [9] §12 and §19 for the definition of $W(E/K_v) := W(\sigma'_{E/K_v})$ and [9] §21 p. 157 for the functional equation of Λ).

This conjecture is known in a few cases:

- For elliptic curves over $\mathbb{Q}$ thanks to modularity results on elliptic curves due to Wiles, Taylor, Breuil, Diamond and Conrad.
- For elliptic curves over a totally real field K, we only know a meromorphic continuation and the functional equation of Λ thanks to a potential modularity result of Wintenberger (see [16]) together with an argument of Taylor.

In general, Conjecture 1.4 is not known.

The conjecture of Birch and Swinnerton-Dyer implies the following weaker conjecture:

Conjecture 1.5 (BSD (mod 2)). — *We have*

$$\mathrm{rk}(E/K) \equiv \mathrm{ord}_{s=1}\Lambda(E/K,s) \pmod 2 .$$

Combining it with the conjectural functional equation we get:

Conjecture 1.6 (Parity conjecture). — *We have*

$$(-1)^{\mathrm{rk}(E/K)} = W(E/K).$$

Tim and Vladimir Dokchitser showed that this conjecture is true assuming that the 6^∞-part of the Tate-Shafarevich group of E over $K(E[2])$ is finite (see [5] Th 7.1 p. 20).

Definition 1.7 (Selmer group). — *Let*

$$X_p(E/K) := \mathrm{Hom}_{\mathbb{Z}_p}(S(E/K,p^\infty),\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

where $S(E/K,p^\infty) := \varinjlim_n S(E/K,p^n)$ is the p^∞-Selmer group, sitting in an exact sequence:

$$0 \longrightarrow E(K)\otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow S(E/K,p^\infty) \longrightarrow Ш_{E/K}[p^\infty] \longrightarrow 0.$$

If we let $\mathrm{rk}_p(E/K) := \dim_{\mathbb{Q}_p} X_p(E/K) = \mathrm{rk}(E/K) + \mathrm{cork}_{\mathbb{Z}_p} Ш_{E/K}[p^\infty]$, a more accessible form of the Conjecture 1.6 is the following:

Conjecture 1.8 (p-parity conjecture). — *We have*

$$(-1)^{\mathrm{rk}_p(E/K)} = W(E/K).$$

If L/K is a finite Galois extension and τ is a self-dual $\overline{\mathbb{Q}}_p$-representation of $\mathrm{Gal}(L/K)$ then there is an equivariant form of Conjecture 1.8:

Conjecture 1.9 (p-parity conjecture for (self-dual) twists)

We have

$$(-1)^{\langle \tau, X_p(E/L)\rangle} = W(E/K,\tau),$$

where $W(E/K,\tau) = \prod_v W(\sigma'_{E/K_v} \otimes \mathrm{Res}_{D_v} \tau)$, $D_v \subset \mathrm{Gal}(L/K)$ *is the decomposition group at* v *and* $\langle \tau, * \rangle$ *is the usual representation-theoretic inner product of* τ *and the complexification of* $*$.

It is this last conjecture in a particular setting that will interest us for the rest of the paper.

1.2. Statement of the main theorem and applications to the p-parity conjecture. — Let K be a number field, E/K an elliptic curve and L/K a finite Galois extension such that $\mathrm{Gal}(L/K) \simeq D_{2p^n}$, with $p \geq 5$ a prime number.

D_{2p^n} admits the following irreducible representations over $\overline{\mathbb{Q}}_p$:

- 1 the trivial representation
- η the quadratic character
- $\frac{p^n-1}{2}$ irreducible representations of degree 2; they are of the form,

$$I(\chi) := \mathrm{Ind}_{C_{p^n}}^{D_{2p^n}}(\chi) = I(\chi^{-1}),$$

  where χ is a non-trivial character of C_{p^n} ($I(1) = 1 \oplus \eta$ is reducible). See for example [12] for the description of irreducible representations of D_{2p^n}.

Let $\tau = I(\chi)$ be such an irreducible representation of degree 2.

Theorem 1.10. — *With the notation above and* $p \geq 5$, *we have the following equality:*

$$\frac{W(E/K,\tau)}{W(E/K,1\oplus\eta)} = \frac{(-1)^{\langle \tau, X_p(E/L)\rangle}}{(-1)^{\langle 1\oplus\eta, X_p(E/L)\rangle}}$$

In other words, the p-parity conjecture for E/K *tensored by* $1\oplus\eta\oplus\tau$ *holds:*

$$W(E/K, 1\oplus\eta\oplus\tau) = (-1)^{\langle 1\oplus\eta\oplus\tau, X_p(E/L)\rangle}$$

Remark 1.11. — *The Dokchitser brothers have shown that this equality holds in two different cases:*

- *In the case when p is any prime number but the extension* L/K *has a cyclic decomposition group at all places of additive reduction of* E/K *above* 2 *and* 3 *(see* [3] *Th.4.2 (1) p. 65).*
- *In the case when* $p \equiv 3 \pmod 4$ *(without any additional assumption) using a strong global p-parity result over totally real fields due to Nekovář* [8] *(see* [5] *Prop. 6.12 p. 18).*

REMARK 1.12. — *The statement of Thm.1.10 holds for $p = 3$ (see previous remark). This case can be proved without using the "painful calculation" ([3] p. 53) in the case of additive reduction (see the appendix below).*

Here we prove the equality for all $p \geq 5$ (without any additional assumption).

COROLLARY 1.13. — $\frac{W(E/K, I(\chi))}{(-1)^{\langle I(\chi), X_p(E/L)\rangle}}$ *does not depend on* $\chi : C_{p^n} \longrightarrow \mathbb{C}^*$.

Theorem 1.10 is equivalent to the fact that Hypothesis 4.1 of [3] holds for any elliptic curve and any $p > 3$ (using a result of the Dokchitser brothers it is also true for $p = 3$, see Remark 1.11 above). Now using the machinery of the Dokchitser brothers (see Th.4.3 and Th.4.5 in [3]) we have the following theorems:

THEOREM 1.14. — *Let K be a number field, $p \neq 2$, and E/K an elliptic curve. Suppose F is a p-extension of a Galois extension M/K, Galois over K. If the p-parity conjecture $(-1)^{\mathrm{rk}_p E/L} = W(E/L)$ holds for all subfields $K \subset L \subset M$, then it holds for all subfields $K \subset L \subset F$.*

THEOREM 1.15. — *Let K be a number field, $p \neq 2$, E/K an elliptic curve and F/K a Galois extension. Assume that the p-Sylow subgroup P of $G = \mathrm{Gal}(F/K)$ is normal and G/P is abelian. If the p-parity conjecture holds for E over K and its quadratic extensions in F, then it holds for all twists of E by orthogonal representations of G.*

2. Invariance of the parity conjecture in a D_{2p^n}-extension

2.1. Reduction to the case of a D_{2p}-extension. — Here we reduce the demonstration of Theorem 1.10 by an induction argument together with the Galois invariance of root numbers due to Rohrlich (see [11] Theorem 2), to the following statement:

PROPOSITION 2.1. — *It is sufficient to prove Theorem 1.10 in the case when $n = 1$ (i.e. $\mathrm{Gal}(L/K) \simeq D_{2p}$).*

Proof. — Suppose Theorem 1.10 is true for $n = N - 1$. We will show that theorem is true for $n = N$.

Consider L/K a finite Galois extension such that $\mathrm{Gal}(L/K) \simeq D_{2p^N}$ and $\tau = I(\chi)$ an irreducible representation of degree 2 of D_{2p^N}.

- If χ is not injective, then the statement is known by the induction hypothesis.
- If χ is injective:

  Let $\sigma = \mathrm{res}(I(\chi)) := \mathrm{res}^{D_{2p^N}}_{D_{2p^{N-1}}}(I(\chi))$.

Then $\sigma = I(\chi')$, where $\chi' := \chi_{|C_{p^{N-1}}} : C_{p^{N-1}} \to \overline{\mathbb{Q}}_p$ is injective.

We have: $\mathrm{Ind}_{D_{2p^{N-1}}}^{D_{2p^N}}(\sigma) = \bigoplus_{\chi_0} I(\chi_0)$, where the sum is taken over the χ_0 such that $\chi_{0|C_{p^{N-1}}} = \chi_{|C_{p^{N-1}}}$.

For each such χ_0 there is an element of $Aut(\mathbb{C})$ sending χ into χ_0 and $I(\chi)$ into $I(\chi_0)$.

By inductivity of root numbers in Galois extension:

$$W(E/K, \sigma) = W(E/K, \mathrm{Ind}_{D_{2p^{N-1}}}^{D_{2p^N}}(\sigma)).$$

By Galois invariance of root numbers:

$$W(E/K, I(\chi')) = W(E/K, I(\chi_0)),\ \forall \chi_0 \text{ such that } \chi_{0|C_{p^{N-1}}} = \chi_{|C_{p^{N-1}}}.$$

So $W(E/K, \sigma) = W(E/K, \mathrm{Ind}_{D_{2p^{N-1}}}^{D_{2p^N}}(\sigma)) = W(E/K, \tau)^p = W(E/K, \tau)$.

On the other hand,

$$\langle \sigma, X_p(E/L)\rangle = \left\langle \mathrm{Ind}_{D_{2p^{N-1}}}^{D_{2p^N}}(\sigma), X_p(E/L)\right\rangle = p.\langle \tau, X_p(E/L)\rangle,$$

because $X_p(E/L)$ is a $\mathbb{Q}_p$-representation. So $(-1)^{\langle 1\oplus\eta\oplus\sigma, X_p(E/L)\rangle} = (-1)^{\langle 1\oplus\eta\oplus\tau, X_p(E/L)\rangle}$. By the induction hypothesis, $(-1)^{\langle 1\oplus\eta\oplus\sigma, X_p(E/L)\rangle} = W(E/K, \sigma)$. As a result, $W(E/K, 1\oplus\eta\oplus\tau) = (-1)^{\langle 1\oplus\eta\oplus\tau, X_p(E/L)\rangle}$. □

2.2. The case of a D_{2p}-extension. — We first restate Theorem 1.10 in the case of a D_{2p}-extension.

Let K be a number field, E/K an elliptic curve and L/K a Galois extension such that $\mathrm{Gal}(L/K) \simeq D_{2p} \simeq C_p \rtimes C_2$, with $p \geq 5$ a prime number. We are going to use the notation D_2 instead of C_2 to avoid confusion with the local Tamagawa factors C_v defined below.

Recall the irreducible representations of D_{2p} over $\overline{\mathbb{Q}}_p$:

- 1 the trivial representation
- η the quadratic character
- $I(\chi) = \mathrm{Ind}_{C_p}^{G}(\chi)$ irreducible representations of degree 2, where χ is a non-trivial character of C_p.

THEOREM 2.2. — *With the notation above and $p \geq 5$, we have the following equality:*

$$\frac{W(E/K, \tau)}{W(E/K, 1\oplus\eta)} = \frac{(-1)^{\langle \tau, X_p(E/L)\rangle}}{(-1)^{\langle 1\oplus\eta, X_p(E/L)\rangle}}.$$

In other words, the p-parity conjecture for E/K tensored by $1\oplus\eta\oplus\tau$ holds: $W(E/K, 1\oplus\eta\oplus\tau) = (-1)^{\langle 1\oplus\eta\oplus\tau, X_p(E/L)\rangle}$.

The proof of Theorem 2.2 will occupy the rest of section 2.

We use the following notations:

- v a finite place of K
- K_v the completion of K at v
- $q = l_v^r$ the cardinality of the residue field of K_v
- $z \mid v$ a finite place of L
- $w \mid v$ a finite place of L^H (where H is a subgroup of $\mathrm{Gal}(L/K) = D_{2p}$)
- $\delta = \mathrm{ord}_v$ (the minimal discriminant of E/K_v)
- $\delta_H = \mathrm{ord}_w\left(\text{the minimal discriminant of } E/\left(L^H\right)_w\right)$
- e_H the ramification index of $\left(L^H\right)_w/K_v$
- f_H the residue degree of $\left(L^H\right)_w/K_v$
- ω^0_{E/K_v} = a minimal invariant differential of E/K_v
- $C_w(E/L^H) = c_w(E/L^H)\omega(H)$,

$$\text{where}\begin{cases} c_w(E/L^H) = \text{ local Tamagawa factor of } E/\left(L^H\right)_w \\ \omega(H) = \left|\dfrac{\omega^0_{E/K_v}}{\omega^0_{E/(L^H)_w}}\right|_{(L^H)_w} \end{cases}.$$

A minimal invariant differential of E/K_v and one of $E/\left(L^H\right)_w$ differ by an element of $\left(L^H\right)_w$. If we choose ω'^0_{E/K_v} (resp $\omega'^0_{E/(L^H)_w}$) a different minimal invariant differential of E/K_v (resp $E/\left(L^H\right)_w$), we have $\frac{\omega'^0_{E/K_v}}{\omega'^0_{E/(L^H)_w}} = \alpha\frac{\omega^0_{E/K_v}}{\omega^0_{E/(L^H)_w}}$, where α is a unit in $\left(L^H\right)_w$ (see [14] p. 172). Therefore $\omega(H)$ is well defined.

Furthermore, if $l_v > 3$ then (see [3] p. 53):

$$\left|\frac{\omega^0_{E/K_v}}{\omega^0_{E/(L^H)_w}}\right|_{(L^H)_w} = q^{\frac{\delta.e_H-\delta_H}{12}f_H}$$

$$\left(= q^{\left\lfloor\frac{\delta.e_H}{12}\right\rfloor f_H} \text{ in the case of potentially good reduction}\right).$$

For D_{2p}, there is the following equality:

$$\mathrm{Ind}^{D_{2p}}_{\{1\}}1 - 2.\mathrm{Ind}^{D_{2p}}_{D_2}1 - \mathrm{Ind}^{D_{2p}}_{C_p}1 + 2.1 = 0$$

of virtual representations of G, this gives the G-relation $\Theta : \{1\} - 2D_2 - C_p + 2G$ in the sense of [3] (Def 2.1 p. 34).

We recall two definitions in our setting (i.e. with $\Theta : \{1\} - 2D_2 - C_p + 2D_{2p}$), for general definitions see [3].

Definition 2.3 ([3], Def. 2.13 p. 36). — *Let ρ be a self-dual $\mathbb{Q}_p[G]$-representation.*

Pick a G-invariant non-degenerate $\mathbb{Q}_p$-linear pairing $\langle , \rangle$ on ρ and set

$$C_\Theta(\rho) = \det(\langle , \rangle \left| \rho^{\{1\}} \right.) \det(\tfrac{1}{2} \langle , \rangle \left| \rho^{D_2} \right.)^{-2} \det(\tfrac{1}{p} \langle , \rangle \left| \rho^{C_p} \right.)^{-1} \det(\tfrac{1}{2p} \langle , \rangle \left| \rho^{D_{2p}} \right.)^{2}$$

as an element of $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$, where $\det(\langle , \rangle \left| \rho^A \right.)$ is $\det((\langle e_i, e_j \rangle_{i,j})$ in any $\mathbb{Q}_p$-basis $\{e_i\}$ of ρ^A.

Remark 2.4. — *$C_\Theta(\rho)$ is well defined and does not depend on the choice of the pairing (see [3] Theorem 2.17 p. 37).*

Definition 2.5 ([3], Def. 2.50 p. 46). — *We define:*

$$T_{\Theta,p} = \left\{ \begin{array}{l|l} \sigma \text{ a self-dual } \overline{\mathbb{Q}}_p[G]\text{-} & \langle \sigma, \rho \rangle \equiv \mathrm{ord}_p C_\Theta(\rho) \pmod 2 \\ \text{representation} & \forall \rho \text{ a self-dual } \mathbb{Q}_p[G]\text{-representation.} \end{array} \right\}$$

Following the approach of the Dokchitser brothers, we have the following theorem

Theorem 2.6 (Theorem 1.14 of [3]). — *Let L/K be a Galois extension of number fields with Galois group $G = D_{2p}$, where $p > 2$ is a prime number. Let $\Theta : \{1\} - 2D_2 - C_p + 2D_{2p}$. For every elliptic curve E/K, the $\mathbb{Q}_p[G]$-represention $X_p(E/L)$ is self-dual, and*

$$\forall \sigma \in T_{\Theta,p}, \quad (-1)^{\langle \sigma, X_p(E/L) \rangle} = (-1)^{\mathrm{ord}_p(C)},$$

where $C = \prod_{v \nmid \infty} C_v$ with $C_v = C_v(\{1\}) C_v(D_2)^{-2} C_v(C_p)^{-1} C_v(G)^2$ and

$$C_v(H) = \prod_{\substack{w | v \\ w \text{ places of } L^H}} C_w(E/L^H).$$

Now, since $1 \oplus \eta \oplus \tau \in T_{\Theta,p}$ (see [3], example 2.53 p. 46), we only need to prove that :

$$\frac{W(E/K, \tau)}{W(E/K, 1 \oplus \eta)} = (-1)^{\mathrm{ord}_p C}. \tag{1}$$

Furthermore, since we are only interested in the parity of $\mathrm{ord}_p(C)$, we do not have to determine $C_v(D_2)$ and $C_v(G)$, because these terms only bring an even contribution (since they appear with an even exponent).

Both sides of (1) are of local nature.

As $W(E/K, \tau) = \prod_v W(E/K_v, \tau_v)$, where $\sigma_v := \mathrm{res}_{\mathrm{Gal}(L_z/K_v)} \sigma$, all we need to do is to prove the following local equality:

$$\frac{W(E/K_v, \tau_v)}{W(E/K_v, (1 \oplus \eta)_v)} = (-1)^{\mathrm{ord}_p(C_v)}, \tag{2}$$

for each finite place v of K ($v \mid \infty$ do not contribute, since $p \neq 2$).

Denote by $G_v := \mathrm{Gal}(L_z/K_v)$ the decomposition group of v. The proof of Theorem 2.2 splits in several cases:

- $G_v = \{1\}$ (there are $2p$ places above v in L) see section 2.2.2
- $G_v = D_2$ (there are p places above v in L) see section 2.2.3
- $G_v = C_p$ (there are 2 places above v in L) see section 2.2.2
- $G_v = D_{2p}$ (there is a unique place above v in L) see section 2.2.4

The case where G_v is cyclic is treated in Dokchitser's work but the proof given here is slightly different and specific to our particular choices of G and Θ.

We first recall a few facts about the local Tamagawa factors of elliptic curves.

2.2.1. *Local Tamagawa factors of elliptic curves.* — The assumptions and notation from above are in force.

The local Tamagawa factor at v, $c(E/K_v) = \#\big(E(K_v)/E^0(K_v)\big)$, $\big($where $E^0(K_v) = \{\text{Points of non-singular reduction}\}\big)$ is determined by Tate's algorithm (see [13] IV §9):

$$c(E/K_v) = \begin{cases} 1 & \text{if } E \text{ has good reduction at } v \\ 1,\ 2,\ 3 \text{ or } 4 & \text{if } E \text{ has additive reduction at } v \\ n & \begin{array}{l}\text{if } E \text{ has split multiplicative reduction} \\ \text{of type } I_n \text{ at } v\end{array} \\ 1 \text{ or } 2 & \begin{array}{l}\text{if } E \text{ has non-split multiplicative reduction} \\ \text{of type } I_n \text{ at } v\end{array} \end{cases}$$

If E acquires semi-stable reduction over L_z, then:

1. If E has split multiplicative reduction of type I_n over K_v, then:
$$c(E/\left(L^H\right)_w) = n.e_H.$$
2. If E has non-split multiplicative reduction of type I_n over K_v, then:
$$c(E/\left(L^H\right)_w) = \begin{cases} n.e_H & \begin{array}{l}\text{if } E \text{ has split multiplicative reduction} \\ \text{over } \left(L^H\right)_w\end{array} \\ 1 \text{ or } 2 & \text{otherwise.}\end{cases}$$
3. If E has potentially good reduction, then $c(E/\left(L^H\right)_w) = 1, 2, 3$ or 4.
4. If E has additive and potentially multiplicative reduction then:
$$c(E/\left(L^H\right)_w) = \begin{cases} n.e_H & \begin{array}{l}\text{if } E \text{ has split multiplicative reduction} \\ \text{of type } I_n \text{ over } \left(L^H\right)_w \text{ and } l_v \neq 2.\end{array} \\ 1, 2, 3 \text{ or } 4 & \text{otherwise.}\end{cases}$$

The following proposition will be used in the subsequent computations.

Proposition 2.7. — 1. *If w_1 and w_2 are two places of L above the same v, then: $c_{w_1}(E/L) = c_{w_2}(E/L)$. In particular:*

$$\begin{cases} C_v(\{1\}) = C_w(E/L)^r \\ C_v(C_p) = C_{w'}(E/L^{C_p})^{r'}, \end{cases}$$

where r =the number of places w of L such that $w \mid v$ and r' =the number of places w' of L^{C_p} such that $w' \mid v$.

2. *If E/K has potentially good reduction at v, then:$\forall w$ (resp. w') place of L (of L^{C_p}), $c_w(E/L)$ $(c_{w'}(E/L^{C_p})) \in \{1,..,4\}$, and therefore* $\mathrm{ord}_p(c_v) = 0$ *and* $(-1)^{\mathrm{ord}_p(C_v)} = (-1)^{\mathrm{ord}_p\left(\frac{\omega(\{1\})}{\omega(C_p)}\right)}$.
3. *If the reduction of E/K at v is semi-stable, then $\forall H$ subgroup of D_{2p}, $\delta_H = \delta.e_H$ and therefore $\omega(H) = 1$ and $(-1)^{\mathrm{ord}_p(C_v)} = (-1)^{\mathrm{ord}_p(c_v)}$.*
4. *If $v \nmid p$ (i.e. $p \neq l_v$, p is fixed, l_v is variable), then* $\mathrm{ord}_p(\omega(H)) = 0$ *and* $(-1)^{\mathrm{ord}_p(C_v)} = (-1)^{\mathrm{ord}_p(c_v)}$.

Remark 2.8. — *By points 3 and 4 of the proposition, if E/K has good reduction at v, then: $(-1)^{\mathrm{ord}_p(C_v)} = 1$. As $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = \frac{\det \tau_v(-1)}{\det(1\oplus\eta)_v(-1)} = 1$ in the case of good reduction, we have the desired equality* (2) *in the case of good reduction at v.*

Remark 2.9. — *From 2 and 4 we deduce that the only case that needs the calculation of both $\omega(H)$ and $c_w(E/L^H)$ is the case of additive potentially multiplicative reduction at $v \mid p$.*

2.2.2. *The cases $G_v = \{1\}$ and $G_v = C_p$.* — In these cases, $C_v(\{1\})$ and $C_v(C_p)$ are squares, so $\mathrm{ord}_p(C_v) \equiv 0 \pmod 2$.

- If $G_v = \{1\}$, $\mathrm{res}_{\mathrm{Gal}(L_z/K_v)}\tau = 1\oplus 1 = (1\oplus\eta)_v$, hence $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1$.
- If $G_v = C_p$, $(1\oplus\eta)_v = 1\oplus 1$ and $\tau_v = \chi \oplus \chi^*$, so

$$W(E/K_v,\tau_v) = 1 = W(E/K_v,(1\oplus\eta)_v) \text{ (see [3] lemma A.1 p. 69).}$$

As a result, in both cases we have: $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1 = (-1)^{\mathrm{ord}_p(C_v)}$.

2.2.3. *The case $G_v = D_2$.* — We have $\tau_v = (1\oplus\eta)_v$, so $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1$.

On the other hand, in this case, $\forall w' \mid v$ place of L^{C_p} and $\forall w \mid w'$ place of L, $[\left(L^{C_p}\right)_{w'} : K_v] = 2$ and $\left(L^{C_p}\right)_{w'} = L_w$. In particular, $C_v(\{1\}) = C_v(C_p)^p$, therefore $C_v = C_v(C_p)^{p-1}$ and $\mathrm{ord}_p(C_v) = 0$.

Finally, we get: $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1 = (-1)^{\mathrm{ord}_p(C_v)}$.

2.2.4. *The case $G_v = D_{2p}$.* — Denote by w (resp z) the unique place of L^{C_p} (resp L) above v.

In this case, there are two possibilities for the inertia group of G_v, $I_v = C_p$ or D_{2p} (because I_v is a normal subgroup of $G_v = D_{2p}$ and G_v/I_v is cyclic).

Furthermore, if $l_v \neq p$ then $I_v = C_p$:

– For $l_v \neq 2$ because the inertia group of a tamely ramified extension is cyclic.

– For $l_v = 2$ because the case $I_v = D_{2p}$, $I_v^{\text{wild}} = D_2$ (the wild inertia group) is impossible since I_v^{wild} is normal in I_v.

2.2.4.1. *Computation of* $(-1)^{\operatorname{ord}_p(C_v)}$

1. If E/K_v has potentially multiplicative reduction:
   (a) If E/K_v acquires split multiplicative reduction of type I_n over L_z (and therefore over $\left(L^{C_p}\right)_w$), then:

$$\begin{aligned} C_v(\{1\}) = c_w(E/L_z) &= e_{L_z/\left(L^{C_p}\right)_w} \times c_{w'}(E/\left(L^{C_p}\right)_w) \\ &= \frac{e_{\{1\}}}{e_{C_p}} \times c_v(E/K)C_v(C_p) \\ &= \frac{e_{\{1\}}}{e_{C_p}} \times C_v(C_p) \end{aligned}$$

$$\text{but } \begin{cases} \text{if } I_v = C_p \text{ then } e_{\{1\}} = p \text{ and } e_{C_p} = 1 \\ \text{if } I_v = D_{2p} \text{ then } e_{\{1\}} = 2p \text{ and } e_{C_p} = 2. \end{cases}$$

   In both cases we get: $C_v = p$ and $(-1)^{\operatorname{ord}_p(C_v)} = -1$.
   (b) If E/K_v does not acquire split multiplicative reduction of type I_n over L_z (and therefore nor over $\left(L^{C_p}\right)_w$), then:

$$c_v(\{1\}), c_v(C_p) \in \{1,2,3,4\} \text{ and } \operatorname{ord}_p\left(\frac{\omega\left(\{1\}\right)}{\omega\left(C_p\right)}\right) \equiv 0 \pmod 2 .$$

   The second claim is a consequence of Proposition 2.7.4 in the case $l_v \neq p$.
   In the case $l_v = p$, we have to distinguish two cases:
      (i) If E/K_v acquires non-split multiplicative reduction of type I_n over L_z (and therefore over $\left(L^{C_p}\right)_w$), then $\delta_{\{1\}} = \delta_{C_p}$. Furthermore, $f_{C_p} = f_{\{1\}} = 1$ or 2 and $\frac{\omega(\{1\})}{\omega(C_p)} = q^{\delta f(e_{\{1\}} - e_{C_p})}$, so $\operatorname{ord}_p\left(\frac{\omega(\{1\})}{\omega(C_p)}\right) \equiv 0 \pmod 2$ (because $p-1 \mid \left(e_{\{1\}} - e_{C_p}\right)$).
      (ii) If $E/K_v, E/\left(L^{C_p}\right)_w$ and E/L_z have additive reduction (of type I_n^*):
         - If $I_v = C_p$, then $f_{C_p} = f_{\{1\}} = 2$ and the result follows.

- if $I_v = D_{2p}$, since $p \geq 5$, E becomes of type I_{2n}^* over $\left(L^{C_p}\right)_w$ and I_{2pn}^* over L_z and we get: $\mathrm{ord}_p\left(\omega\left(\{1\}\right)\right) = \mathrm{ord}_p\left(\omega\left(C_p\right)\right) \equiv 0 \pmod 2$.

To sum up, in the case of potentially multiplicative reduction:

$$(-1)^{\mathrm{ord}_p(C_v)} = \begin{cases} -1 & \text{if } E/(L^{C_p}) \text{ has split multiplicative reduction} \\ 1 & \text{otherwise.} \end{cases}$$

2. If E/K_v has potentially good reduction, then:
   (a) If $I_v = C_p$ (i.e. $e_{\{1\}} = p$ and $e_{C_p} = 1$), we get: $f_{\{1\}} = f_{C_p} = 2$ so $\mathrm{ord}_p(\omega(C_p)) \equiv \mathrm{ord}_p(\omega(\{1\})) \equiv 0 \pmod 2$ and therefore $(-1)^{\mathrm{ord}_p(C_v)} = 1$ (see Proposition 2.7.2).
   (b) If $I_v = D_{2p}$ (i.e. $e_{\{1\}} = 2p$, $e_{C_p} = 2$ and $l_v = p$), we get:

$$\frac{C_v(\{1\})}{C_v(C_p)} = \frac{\omega(\{1\})}{\omega(C_p)} = q^{\left\lfloor \frac{\delta . e_{\{1\}}}{12} \right\rfloor - \left\lfloor \frac{\delta . e_{C_p}}{12} \right\rfloor} = q^{\left\lfloor \frac{\delta . 2p}{12} \right\rfloor - \left\lfloor \frac{\delta . 2}{12} \right\rfloor}.$$

   (i) If q is an even power of p, then

$$(-1)^{\mathrm{ord}_p(C_v)} = (-1)^{\mathrm{ord}_p\left(\frac{\omega(\{1\})}{\omega(C_p)}\right)} = 1.$$

   (ii) If q is an odd power of p :
   A computation of $\left\lfloor \frac{\delta . 2p}{12} \right\rfloor$ and $\left\lfloor \frac{\delta . 2}{12} \right\rfloor$ depending on p modulo 12 gives the following table:

   Table of values of $(-1)^{\mathrm{ord}_p(C_v)}$ depending on the Kodaira symbol of the curve (and the value of $\mathfrak{e} = \frac{12}{\mathrm{pgcd}(\delta, 12)}$) and p mod 12:

p mod 12	1	5	7	11
II, II^* ($\mathfrak{e} = 6$)	1	-1	1	-1
III, III^* ($\mathfrak{e} = 4$)	1	1	-1	-1
IV, IV^* ($\mathfrak{e} = 3$)	1	-1	1	-1
I_o^* ($\mathfrak{e} = 2$)	1	1	1	1

   In relation to the above table it may be useful to recall the following fact: if the residue characteristic of K_v is > 3, then we have the following correspondence between $\mathfrak{e} = \frac{12}{\mathrm{pgcd}(\delta, 12)}$, the valuation of the minimal discriminant δ and the Kodaira symbols:

$$\begin{array}{lll}\mathfrak{e}=1 & \Leftrightarrow \delta=0 & \Leftrightarrow E \text{ is of type } I_0\\ \mathfrak{e}=2 & \Leftrightarrow \delta=6 & \Leftrightarrow E \text{ is of type } I_0^*\\ \mathfrak{e}=3 & \Leftrightarrow \delta=4 \text{ or } 8 & \Leftrightarrow E \text{ is of type } IV \text{ or } IV^*\\ \mathfrak{e}=4 & \Leftrightarrow \delta=3 \text{ or } 9 & \Leftrightarrow E \text{ is of type } III \text{ or } III^*\\ \mathfrak{e}=6 & \Leftrightarrow \delta=2 \text{ or } 10 & \Leftrightarrow E \text{ is of type } II \text{ or } II^*.\end{array}$$

For the meaning of the Kodaira symbols see [13] p. 354.

2.2.4.2. *Computation of* $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}$

1. The case of potentially multiplicative reduction:

We have an explicit formula of Rohrlich (see [10] Th.2 (ii) p. 329):

$$W(E/K_v,\sigma)=\det\sigma(-1)\chi(-1)^{\dim\sigma}(-1)^{\langle\chi,\sigma\rangle},$$

where χ is the character of K_v^* associated to the extension $K_v(\sqrt{-c_6})$ of K_v (c_6 is the classical factor, see [14] p. 46).

Since $\dim\tau_v=\dim 1\oplus\eta=2$, $\det(\tau_v)=\det(1\oplus\eta)$ and $\langle\chi,\tau_v\rangle=0$, we get:

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}=\frac{(-1)^{\langle\chi,\tau_v\rangle}}{(-1)^{\left\langle\chi,(1\oplus\eta)_v\right\rangle}}=\frac{1}{(-1)^{\left\langle\chi,(1\oplus\eta)_v\right\rangle}}=(-1)^{\left\langle\chi,(1\oplus\eta)_v\right\rangle}.$$

(a) If the reduction of E/K_v is split multiplicative (i.e. $\chi=1$): Then $(-1)^{\left\langle\chi,(1\oplus\eta)_v\right\rangle}=-1$.

(b) If the reduction of E/K_v is non-split multiplicative (i.e. χ is an unramified quadratic character):

  (i) If E acquires split multipl. reduction over L_z (and therefore over $\left(L^{C_p}\right)_w$), then $\eta_v=\chi$, hence $(-1)^{\left\langle\chi,(1\oplus\eta)_v\right\rangle}=-1$.

  (ii) If E acquires non-split multiplicative reduction over L_z (and therefore over $\left(L^{C_p}\right)_w$), then $\eta_v\neq\chi$, hence $(-1)^{\left\langle\chi,(1\oplus\eta)_v\right\rangle}=1$.

(c) If the reduction of E/K_v is additive (i.e. χ is a ramified quadratic character)

  (i) If E acquires split multipl. reduction over L_z (and therefore over $\left(L^{C_p}\right)_w$), then $\eta_v=\chi$, hence $(-1)^{\left\langle\chi,(1\oplus\eta)_v\right\rangle}=-1$.

  (ii) If E acquires non-split multiplicative reduction over L_z (and therefore over $\left(L^{C_p}\right)_w$), then $\eta_v\neq\chi$, hence $(-1)^{\left\langle\chi,(1\oplus\eta)_v\right\rangle}=1$.

To sum up, in the case of potentially multiplicative reduction:

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = \begin{cases} -1 & \text{if } E/(L^{C_p}) \text{ has split multiplicative reduction} \\ 1 & \text{otherwise.} \end{cases}$$
$$= (-1)^{\mathrm{ord}_p(C_v)}, \text{ by } 2.2.4.1.1$$

2. The case of potentially good reduction:
   Here we have to distinguish the cases $l_v = p$ and $l_v \neq p$.
   (a) The case $l_v = p$.
   We have again an explicit formula of Rohrlich, since $p \geq 5$ (see [10], Th.2 (iii) p. 329). We use the following notation:
   - $q = p^r$ the cardinality of the residue field residue degree of K_v
   - $\mathfrak{e} = \frac{12}{\mathrm{pgcd}(\delta,12)}$
   - $\epsilon = \begin{cases} 1 & \text{if } r \text{ is even or } \mathfrak{e} = 1 \\ \left(\frac{-1}{p}\right) & \text{if } r \text{ is odd and } \mathfrak{e} = 2 \text{ or } 6 \\ \left(\frac{-3}{p}\right) & \text{if } r \text{ is odd and } \mathfrak{e} = 3 \\ \left(\frac{-2}{p}\right) & \text{if } r \text{ is odd and } \mathfrak{e} = 4. \end{cases}$

   Then $\forall\sigma$ a self-dual representation of $\mathrm{Gal}(\overline{K}_v/K_v)$ with finite image:

$$W(E/K_v,\sigma) = \begin{cases} \alpha(\sigma,\epsilon) & \text{if } q \equiv 1[\mathfrak{e}] \\ \alpha(\sigma,\epsilon)(-1)^{\langle 1+\eta_{nr}+\hat{\sigma}_e,\sigma\rangle} & \text{if } q \equiv -1[\mathfrak{e}] \\ & \text{and } \mathfrak{e} = 3,4,6, \end{cases}$$

   where η_{nr} is the unramified quadratic character, $\hat{\sigma}_e$ is an irreductible representation of degree 2 of $D_{2\mathfrak{e}}$ and $\alpha(\sigma,\epsilon) := (\det\sigma)(-1)\epsilon^{\dim\sigma}$.
   Since $\dim\tau_v = \dim\,(1\oplus\eta)_v = 2$ and $\det\tau_v = \det\,(1\oplus\eta)_v$, $\alpha((1\oplus\eta)_v\,,\epsilon) = \alpha(\tau_v,\epsilon)$ and we get:

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = \begin{cases} 1 & \text{if } q \equiv 1[\mathfrak{e}] \\ (-1)^{\langle 1+\eta_{nr}+\hat{\sigma}_e,1+\eta_v+\tau_v\rangle} & \text{if } q \equiv -1[\mathfrak{e}] \text{and } \mathfrak{e} = 3,4,6, \end{cases}$$
$$= \begin{cases} 1 & \text{if } q \equiv 1[\mathfrak{e}] \\ (-1)^{\langle 1+\eta_{nr},1+\eta_v\rangle} & \text{if } q \equiv -1[\mathfrak{e}] \text{and } \mathfrak{e} = 3,4,6, \end{cases}$$
$$(\langle\hat{\sigma}_e,\tau_v\rangle = 0 \text{ since } \mathfrak{e} = 3,4,6 \text{ and } p \geq 5).$$

   (i) If r is even, then $q \equiv 1[\mathfrak{e}]$ $\forall\mathfrak{e} \in \{2,3,4,6\}$ and therefore

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1 = (-1)^{\mathrm{ord}_p(C_v)},$$

by 2.b.i (in section 2.3.4.1).

(ii) If r is odd, then $q \equiv 1[\mathfrak{e}] \iff p \equiv 1[\mathfrak{e}]$ and:

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = \begin{cases} 1 & \text{if } q \equiv 1[\mathfrak{e}] \\ (-1)^{\langle 1+\eta_{nr},1+\eta_v\rangle} & \text{if } q \equiv -1[\mathfrak{e}] \text{ and} \mathfrak{e} = 3,4,6. \end{cases}$$

(A) If $I_v = C_p$, then $\eta_{nr} = \eta_v$ and $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1$.

(B) If $I_v = D_{2p}$, then $\eta_{nr} \neq \eta_v$ and:

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = \begin{cases} 1 & \text{if } q \equiv 1[\mathfrak{e}] \\ -1 & \text{if } q \equiv -1[\mathfrak{e}] \text{ and } \mathfrak{e} = 3,4,6. \end{cases}$$

In both cases, we obtain for the values of $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}$ exactly the same table as for the values of $(-1)^{\mathrm{ord}_p(C_v)}$, depending on p modulo 12. Here is the table of values of $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}$ depending on the Kodaira symbol of the curve (and the value of $\mathfrak{e} = \frac{12}{\mathrm{pgcd}(\delta,12)}$) and $p \bmod 12$:

$p \bmod 12$	1	5	7	11
II, II^* ($\mathfrak{e} = 6$)	1	-1	1	-1
III, III^* ($\mathfrak{e} = 4$)	1	1	-1	-1
IV, IV^* ($\mathfrak{e} = 3$)	1	-1	1	-1
I_o^* ($\mathfrak{e} = 2$)	1	1	1	1

(b) The case $l_v \neq p$:

In this case, the explicit formula of Rohrlich cannot be used, since l_v can be 2 or 3.

Let σ be a representation $\sigma : \mathrm{Gal}(\overline{K}_v/K_v) \to \mathrm{GL}(V_\sigma)$ with finite image; let $\sigma'_{E/K_v} : WD(\overline{K}_v/K_v) \to \mathrm{GL}(V)$ be the representation of the Weil-Deligne group associated to the elliptic curve given by $\big(\sigma_{E/K_v}, N\big) = \big(\sigma_{E/K_v}, 0\big)$ (because the reduction is potentially good). This is simply a representation of the Weil group $W(\bar{K}_v/K_v)$ (because $N = 0$) and

$$\sigma'_{E/K_v} \otimes \sigma = \sigma_{E/K_v} \otimes \sigma : W(\overline{K}_v/K_v) \to \mathrm{GL}(W),$$

where $W = V \otimes V_\sigma$, is also a representation of the Weil group.

We first recall the definition of root numbers via ε-factors (see [9] §11 and §12):

$$W(E/K_v,\sigma) = \frac{\varepsilon(\sigma_{E/K_v} \otimes \sigma, \psi, dx)}{\big|\varepsilon(\sigma_{E/K_v} \otimes \sigma, \psi, dx)\big|} = \varepsilon(\sigma'_{E/K_v} \otimes \sigma, \psi, dx_\psi),$$

where dx is any Haar measure, ψ is any additive character of K_v and dx_ψ the self-dual Haar measure with respect to ψ on K_v.

Here, we choose an additive character ψ for which the Haar measure dx_ψ takes values (on open compact subsets of K_v) in $\mathbb{Z}_p[\zeta_p]$, where ζ_p is a primitive p-th root of unity. For example, if the conductor of ψ is trivial, then the values of dx_ψ lie in $l_v^{\mathbb{Z}} \cup \{0\} \subset \mathbb{Z}_p[\zeta_p]$.
In one of his articles ([2] p. 548), Deligne gives a description of the ε-factors in terms of ε_0-factors; in our settings this gives:

$$\varepsilon(\sigma_{E/K_v} \otimes \sigma, \psi, dx_\psi) = \varepsilon_0(\sigma_{E/K_v} \otimes \sigma, \psi, dx_\psi) \det(-\nu(\phi) \mid W^{I(v)}),$$

where ϕ is the geometric Frobenius at v and $I(v) = \mathrm{Gal}(\bar{K}_v/K_v^{ur})$.
Recall that, since $l_v \neq p$, the inertia group of D_{2p} is $I_v = C_p$.

(i) If E has additive reduction, denote by F the smallest Galois extension of K_v^{ur} such that E has good reduction over F and set $\Phi = \mathrm{Gal}(F/K_v^{ur})$; then the restiction of σ_{E/K_v} to $I(v)$ factors through Φ.
It is known that:
- For $l_v \geq 5$, Φ is cyclic of order $\mathfrak{e} = \frac{12}{\mathrm{pgcd}(\delta,12)}$.
- For $l_v = 3$, $|\Phi| \in \{2, 3, 4, 6, 12\}$.
- For $l_v = 2$, $|\Phi| \in \{2, 3, 4, 6, 8, 24\}$.

For a more precise description of Φ, see, for example, [1] or [6].
The representation $\sigma_{E/K} \otimes \sigma$ ($\sigma = \tau_v$ or $(1 \oplus \eta)_v$) restricted to $I(v)$ factors through a quotient H of $I(v)$ which admits Φ and C_p as quotients.
We have:

$$(V \otimes V_\sigma)^{I(v)} = (V \otimes V_\sigma)^H = \mathrm{Hom}_H(V^*, V_\sigma) = \mathrm{Hom}((V^\Phi)^*, V_\sigma^{C_p})$$

because H acts on V (resp. on V_σ) through its quotient Φ (resp. C_p) and $|\Phi|$ is prime to p.
Futhermore, $V^H = V^\Phi = \{0\}$ since E has additive reduction, hence

$$(V \otimes V_\sigma)^{I(v)} = 0, \quad \det\left(-\left(\sigma'_{E/K_v} \otimes \sigma\right)(\phi) \mid (V \otimes V_\sigma)^{I(v)}\right) = 1$$

and

$$W(E/K_v, \sigma) = \varepsilon_0(\sigma_{E/K_v} \otimes \sigma, \psi, dx_\psi) \qquad (\sigma = \tau_v, (1 \oplus \eta)_v). \tag{3}$$

Deligne also gives congruence results for these ε_0 ([2] p. 556-557). Since $\chi \equiv 1 \bmod (1 - \zeta_p)$, we deduce
$I(\chi) \equiv I(1) \bmod (1 - \zeta_p)$ and $\sigma'_{E/K_v} \otimes \tau_v \equiv \sigma'_{E/K_v} \otimes (1 \oplus \eta)_v$ $\bmod (1 - \zeta_p)$. So according to Deligne, $\varepsilon_0(\sigma'_{E/K_v} \otimes \tau_v, \psi, dx_\psi)$ and $\varepsilon_0(\sigma'_{E/K_v} \otimes (1 \oplus \eta)_v, \psi, dx_\psi)$ are two elements of $\{\pm 1\}$

(by (3)), which are congruent modulo $(1-\zeta_p)$, hence they are equal. As a result,

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}=1.$$

(ii) If E has good reduction, then σ_{E/K_v} is unramified. Then we have:

$$\varepsilon(\sigma_{E/K_v}\otimes\tau_v,\psi,dx)=\varepsilon(\tau_v,\psi,dx)^{\dim\sigma_{E/K_v}}\det\sigma_{E/K_v}(\Phi^{m(\tau_v,\psi)}),$$

where $m(\tau_v,\psi)\in\mathbb{N}$ depends on conductors of both τ_v and ψ, and the dimension of τ_v (see [15] 3.4.6 p. 15), therefore:

$$W(E/K_v,\tau_v)=W(\sigma_{E/K_v}\otimes\tau_v)=\frac{\varepsilon(\sigma_{E/K_v}\otimes\tau_v,\psi,dx)}{\left|\varepsilon(\sigma_{E/K_v}\otimes\tau_v,\psi,dx)\right|}=1,$$

since $\det\sigma_{E/K_v}=1$, $W(\tau_v)=\frac{\varepsilon(\tau_v,\psi,dx)}{|\varepsilon(\tau_v,\psi,dx)|}=\pm1$ (because $\det\tau_v=1$, see Proposition p. 145 [9]) and $\dim\sigma_{E/K_v}=2$. Similarly, $W(E/K_v,(1\oplus\eta)_v)=1$, so $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}=1$.

In both cases i) and ii) we also have $(-1)^{\mathrm{ord}_p(C_v)}=1$ by 2.a. (in section 2.3.4.1).

To sum up, we have, for each finite prime v of K,

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}=(-1)^{\mathrm{ord}_p(C_v)}.$$

This completes the proof of Theorem 2.2. □

REMARK 2.10. — *This proof can be adjusted to work in the case* $\mathrm{Gal}(L/K)\simeq D_{2p^n}$*, the computations are almost the same. The idea to reduce the proof to the case of a* D_{2p}*-extension, using Galois invariance of Rohrlich* [11]*, was suggested to me by Tim Dokchitser.*

3. Appendix

The purpose of this appendix is to make a small improvement on Theorem 6.7 of [5]. The interest of this improvement is that Proposition 6.12 of [5] (which is the same statement as Theorem 1.10 for $p\equiv 3 \bmod 4$) will no longer rely on the "truly painful case of additive reduction" anymore (see [3] p. 53). In fact, we use the passage to the global case to avoid all places of additive reduction, not just those above 2 and 3. Since we have proved the result for $p\geq 5$ (Theorem 1.10) without using any global parity results at all, for us this is of interest essentially in the case $p=3$.

We start by recalling the definition of an elliptic curve being *close to* another one:

PROPOSITION 3.1. — *Let* $\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ *be an elliptic curve over a non archimedean local field* $\mathcal{K}$ *(with valuation* v *and residue characteristic* p*) and* $\mathcal{F}/\mathcal{K}$ *a finite Galois extension.*

There exists $\varepsilon > 0$ *such that every elliptic curve* $\mathcal{E}' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$ *over* $\mathcal{K}$ *satisfying* $\forall i\, |a_i' - a_i|_v < \varepsilon$*, has the following properties:*

Over all intermediate fields $\mathcal{F}'$ *of* $\mathcal{F}/\mathcal{K}$*,* $\mathcal{E}$ *and* $\mathcal{E}'$ *have the same:*

- *conductor*
- *valuation of the minimal discriminant*
- *local Tamagawa factors,* $C(E/\mathcal{F}', \frac{dx}{2y+a_1x+a_3})$
- *root numbers*
- *the Tate module as a* $\mathrm{Gal}(\bar{\mathcal{K}}/\mathcal{K})$*-module (for each* $l \neq p$*).*

We will say that $\mathcal{E}'$ *is close to* $\mathcal{E}/\mathcal{K}$*.*

Proof. — This is Proposition 3.3 of [5]. □

We now state the minor improvement of Theorem 6.7 of [5]:

THEOREM 3.2. — *Let* $\mathcal{K}$ *a local non archimedean field of characteristic* 0 *and* $\mathcal{F}/\mathcal{K}$ *a finite Galois extension. Let* F/K *be a Galois extension of totally real fields and* v_0 *a place of* K *such that:*

- v_0 *admits a unique place* $\bar{v}_0$ *of* F *above it*
- $K_{v_0} \simeq \mathcal{K}$ *and* $F_{\bar{v}_0} \simeq \mathcal{F}$*.*

Such an extension exists (see Lemma 3.1 of [5]*).*

Let $\mathcal{E}/\mathcal{K}$ *be an elliptic curve with additive reduction.*

Then there exists an elliptic curve E/K *such that:*

- E *has semi-stable reduction for all* $w \neq v_0$
- $j(E)$ *is not an integer (i.e.* $j(E) \notin \mathcal{O}_K$*)*
- E/K_{v_0} *is close to* $\mathcal{E}/\mathcal{K}$*.*

Proof. — We first choose an elliptic curve E/K such that E/K_{v_0} is *close to* $\mathcal{E}/\mathcal{K}$ (this is possible, by Proposition 3.1).

Now the goal is to remove all places of additive reduction by changing E/K to an elliptic curve satisfying the three conditions of the theorem.

Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with $a_i \in \mathcal{O}_K$.

If we want a place w not to be of additive reduction we have to impose one of the two following conditions:

- The valuation $w(\Delta)$ is zero (in this case w is of good reduction).

- The valuation $w(c_4)$ is zero (in this case w is of good or multiplicative reduction depending on $w(\Delta) = 0$ or > 0).

Let $v \neq v_0$ be a place of K not above 2.

To get the condition "$j(E)$ is not an integer" it is sufficient to make v a multiplicative place (v is multiplicative $\Leftrightarrow v(j(E)) < 0$). We will do this in Step 2 below. But before doing this, we will show in Step 1 how to make semistable all places above 2.

Step 1: Make semi-stable all places $w \neq v_0$ above 2.

Denote by $v_{2,1}, \ldots, v_{2,r}$ these places.

In this case: $\left[v_{2,i}(a_1) = 0 \Rightarrow v_{2,i}(c_4) = 0\ (c_4 = (a_1^2 + 4a_2)^2 - 24a_1a_3 - 48a_4)\right]$.

Let $\mathfrak{p}_0$ and $\mathfrak{p}_{2,i}$ be the primes ideals associated to v_0 and $v_{2,i}$.

By the Chinese remainder theorem, there exists $d_1 \in \mathcal{O}_K$ such that:

- $d_1 \equiv 0 \bmod \mathfrak{p}_0^n$ (i.e. $v_0(d_1) \geq n$).
- $d_1 \equiv 1 - a_1 \bmod \mathfrak{p}_{2,i}$ $\forall i \in \{1, .., r\}$ (i.e. $v_{2,i}(a_1 + d_1) = 0$).
- $d_1 \equiv -a_1 \bmod \mathfrak{p}$ ($\mathfrak{p}$ associated to $v \neq v_0$).

So, if we let $a_1' = a_1 + d_1$ for n big enough we get the curve $y^2 + a_1'xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ which is *close to* $\mathcal{E}/\mathcal{K}$, $v_{2,i}(a_1') = v_{2,i}(a_1 + d_1) = 0$ $\forall i \in \{1, .., r\}$ and $v(a_1') > 0$.

Step 2: Make v semi-stable.

By the Chinese remainder theorem, there exist $d_2, d_3, d_4 \in \mathcal{O}_K$ such that:

- $d_2 \equiv 0 \bmod \mathfrak{p}_0^n$ (i.e. $v_0(d_2) \geq n$) $d_2 \equiv 1 - a_2 \bmod \mathfrak{p}$ (so $v(a_2 + d_2) = 0$).
- $d_3 \equiv 0 \bmod \mathfrak{p}_0^n$ (i.e. $v_0(d_3) \geq n$) $d_3 \equiv -a_3 \bmod \mathfrak{p}$ (so $v(a_3 + d_3) > 0$).
- $d_4 \equiv 0 \bmod \mathfrak{p}_0^n$ (i.e. $v_0(d_4) \geq n$) $d_4 \equiv -a_4 \bmod \mathfrak{p}$ (so $v(a_4 + d_4) > 0$).

So, if we let $a_i' = a_i + d_i$, $i \in \{2, 3, 4\}$, for n big enough we get:

$E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6$ is *close to* $\mathcal{E}/\mathcal{K}$ (Proposition 3.1).

Futhermore :
- $c_4' = (a_1'^2 + 4a_2')^2 - 24a_1'a_3' - 48a_4'$
- $v(a_1') > 0$
- $v(a_3') > 0$
- $v(a_4') > 0$
- $v(a_2') = 0$,

so $v(c_4') = 0$.

The curve $E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6$ is *close to* $\mathcal{E}/\mathcal{K}$; $\forall w \neq v_0$ above 2, $w(c_4') > 0$, and $v(c_4') = 0$. Since c_4' does not depend on a_6, we can modify a_6 to allow places $w \neq v_0$ such that $w(c_4') > 0$ to become places of good reduction (since c_4' will be unchanged, some places of good reduction can become of multiplicative reduction but not of additive reduction) and such that v is of multiplicative reduction ($v(j(E)) < 0$). We will do this in the next step.

Step 3: Turn additive reduction places into good reduction ones and make v multiplicative.

Let $v_1, ..., v_r, v_{r+1}, ..., v_t$ be the places where $v_i(c_4') > 0$, $v_i \neq v_0$ ($\neq v$ and not above 2).

Above, $v_1, ..., v_r$ are places of good reduction and $v_{r+1}, ..., v_t$ places of additive reduction of the curve E' constructed in step 2.

Let b_2, b_4, b_6, b_8 and Δ be the following classical quantities associatied to E':

$$\begin{aligned} b_2 &= a_1'^2 + 4a_2' \\ b_4 &= 2a_4' + a_1'a_3' \\ b_6 &= a_3'^2 + 4a_6 \\ b_8 &= a_1'^2 a_6 + 4a_2'a_6 - a_1'a_3'a_4' + a_2'a_3'^2 - a_4'^2 \end{aligned}$$

$$\begin{aligned} \text{and } \Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ &= \alpha + \beta a_6 + 16a_6^2, \\ &\text{where } \alpha = [-b_2^2(-a_1'a_3'a_4' + a_2'a_3'^2 - a_4'^2) - 8b_4^3 - 27a_3'^4 + 9b_2b_4a_3'^2] \\ &\text{and } \beta = [-b_2^3 - 216a_3'^2 + 36b_2b_4] \end{aligned}$$

Let $\gamma = \beta + 32a_6$; we know that 16 is invertible mod $\mathfrak{p}_i$ $\forall i \in \{1, .., t\}$ (because $\mathfrak{p}_i$ is not above 2).

By the Chinese remainder theorem, there exists c such that:

- $c \equiv 0 \bmod \mathfrak{p}_0^n$ (i.e. $v_0(c) \geq n$)
- $c \equiv 0 \bmod \mathfrak{p}_i$ $\forall i \in \{1, .., r\}$ (i.e. $v_i(c) > 0$)
- $16c \equiv \alpha_i - \gamma \bmod \mathfrak{p}_i$ $\forall i \in \{r+1, .., t\}$ (where $\alpha_i \neq 0, \gamma \bmod \mathfrak{p}_i$) (i.e. $\forall i \in \{r+1, .., t\}$, $v_i(\gamma + 16c) = 0$ and $v_i(c) = 0$)
- $c \equiv -a_6 \bmod \mathfrak{p}$ (i.e. $v(a_6') > 0$).

Finally, if we let $a_6' = a_6 + c$ for n big enough, we get:

$E'' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$

and we see that with this choice:

- $v_1, ..., v_t$ are all places of good reduction for E''.
- v is a place of multiplicative reduction for E''.

This completes the proof. □

Acknowledgements. — First of all, I would like to thank my advisor Jan Nekovář, for suggesting to me this topic, for his guidance along the work and his careful reading of the different versions of this paper. I would also like to thank Vladimir and Tim Dokchitser, the first one for his responses to my questions about their articles, the second one for his advice. Finally, I am grateful to the referee for making several corrections and suggesting improvements of the exposition.

BIBLIOGRAPHY

[1] N. Billerey – "Semi-stabilité des courbes elliptiques", *Dissertationes Math. (Rozprawy Mat.)* **468** (2009).

[2] P. Deligne – "Les constantes des équations fonctionnelles des fonctions L", in *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math., vol. 349, Springer, 1973, p. 501–597.

[3] T. Dokchitser & V. Dokchitser – "Regulator constants and the parity conjecture", *Invent. Math.* **178** (2009), p. 23–71.

[4] ———, "Self-duality of Selmer groups", *Math. Proc. Cambridge Philos. Soc.* **146** (2009), p. 257–267.

[5] ———, "Roots numbers and parity of ranks of elliptics curves", *J. reine angew. Math.* **658** (2011), p. 39–64.

[6] A. Kraus – "Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive", *Manuscripta Math.* **69** (1990), p. 353–385.

[7] J. Nekovář – "On the parity of ranks of Selmer groups. III", *Doc. Math.* **12** (2007), p. 243–274.

[8] ———, "On the parity of ranks of Selmer groups. IV", *Compos. Math.* **145** (2009), p. 1351–1359.

[9] D. E. Rohrlich – "Elliptic curves and the Weil-Deligne group", in *Elliptic curves and related topics*, CRM Proc. Lecture Notes, vol. 4, Amer. Math. Soc., 1994, p. 125–157.

[10] ———, "Galois theory, elliptic curves, and root numbers", *Compositio Math.* **100** (1996), p. 311–349.

[11] ———, "Galois invariance of local root numbers", *Mathematische Annalen* **351** (2011), p. 979–1003.

[12] J-P. Serre – *Représentations linéaires des groupes finis*, Hermann, 1998.

[13] J. H. Silverman – *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Math., vol. 151, Springer, 1994.

[14] ———, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer, 1994.

[15] J. Tate – "Number theoretic background", in *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., 1979, p. 3–26.

[16] J. P. Wintenberger – "Potential modularity of elliptic curves over totally real fields", appendix to [8].