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*

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

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).*