JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Florian ITO SPRUNG

Chromatic Selmer groups and arithmetic invariants of elliptic curves

Tome 33, nº 3.2 (2021), p. 1103-1114.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2021__33_3.2_1103_0>

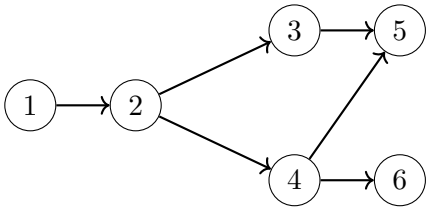
Journal de Théorie des Nombres
de Bordeaux **33** (2021), 1103–1114

Chromatic Selmer groups and arithmetic invariants of elliptic curves

par Florian ITO SPRUNG

Résumé. Les groupes de Selmer chromatiques sont des modifications des groupes de Selmer, qui contiennent des informations locales pour les nombres premiers p supersinguliers. Dans les sections 2–5, on esquisse leur rôle dans la démonstration de la partie p-primaire de la formule de Birch et Swinnerton-Dyer, et ensuite, dans la section 6, on étudie la croissance du rang de Mordell–Weil le long de la $\mathbb{Z}_p^2$-extension d'un corps quadratique imaginaire dans lequel p est décomposé.

Abstract. Chromatic Selmer groups are modified Selmer groups with local information for supersingular primes p. We sketch their role in establishing the p-primary part of the Birch–Swinnerton-Dyer formula in Sections 2–5, and then study the growth of the Mordell–Weil rank along the $\mathbb{Z}_p^2$-extension of a quadratic imaginary number field in which p splits in Section 6.



Guide

1. Motivation

Let E be an elliptic curve over the rational numbers, and $p > 2$ be a prime of good reduction. We denote by $\mathbb{Q}_n$ the nth layer of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. From the Mordell–Weil theorem, the $\mathbb{Q}_n$-rational points then have a structure of the form

$$E(\mathbb{Q}_n) \simeq \mathbb{Z}^{r(\mathbb{Q}_n)} \times (\text{finite}).$$

Manuscrit reçu le 12 décembre 2019, révisé le 9 juin 2020, accepté le 28 juillet 2020.
Mathematics Subject Classification. 11G40, 11R23, 14H52.
Mots-clefs. Elliptic curves, Selmer group, Mordell–Weil rank.
Supported by Simons Collaboration Grant 635320 and NSF Grant DMS 2001280.

For the growth of the rank, we know it stays bounded by the following theorem of Kato and Rohrlich:

Theorem 1.1 (Kato [14], Rohrlich [26])**.**

$$\lim_{n\to\infty} r(\mathbb{Q}_n) < \infty$$

We give the circle of ideas of the proof under the assumption $p \nmid a_p := p+1-\#E(\mathbf{F}_p)$, which we make until the end of this section. An important idea is the Main Conjecture:

The Main Conjecture is a bridge between algebra and analysis and states that

$$\operatorname{Char} \mathcal{X}_{\mathbb{Q}_\infty} = (L_p) \neq 0,$$

where $\mathcal{X}_{\mathbb{Q}_\infty} = \varprojlim_n \mathcal{X}_{\mathbb{Q}_n}$ with $\mathcal{X}_{\mathbb{Q}_n} = \operatorname{Hom}_{\mathrm{cont}}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n), \mathbb{Q}_p/\mathbb{Z}_p)$, and L_p is the p-adic L-function attached to E.

On the algebraic side, the Selmer group $\mathrm{Sel}(E/\mathbb{Q}_n)$ as well as its p-primary part $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n)$ encodes the interplay between the global points $E(\mathbb{Q}_n)$ and the local points $E(\mathbb{Q}_{n,v})$ for every place v.

On the analytic side, the p-adic L-function L_p encodes all special values $L(E, \chi_{p^n}, 1)$ of the Hasse–Weil L-function at the critical point twisted by p-power conductor Dirichlet characters. L_p is believed to be an element of the Iwasawa algebra $\Lambda = \mathbb{Z}_p[\![T]\!]$, but at present we only know $L_p \in \Lambda \otimes \mathbb{Q}$.

We are now ready to sketch the idea of the proof: Rohrlich showed that $L(E, \chi_{p^n}, 1)$ only vanishes for finitely many χ_{p^n}, so that $L_p \neq 0$. Kato proved (under small assumptions) that $L_p \in \operatorname{Char} \mathcal{X}_{\mathbb{Q}_\infty}$. Putting these together, one sees that $\mathrm{rk}_{\mathbb{Z}_p} \mathcal{X}_{\mathbb{Q}_\infty} \leqslant \lambda :=$ number of zeros of L_p. Now a consequence of a theorem of Mazur (the control theorem) is that for large enough n, we have $\mathrm{rk}_{\mathbb{Z}_p} \mathcal{X}_{\mathbb{Q}_n} \leqslant \lambda$. We can conclude from this that $r(\mathbb{Q}_n) \leqslant \lambda$ because of the injection $E(\mathbb{Q}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n)$.

This note is mainly concerned with the case of supersingular reduction, i.e. in which $p|a_p$. In Section 2, we give a description of the chromatic Iwasawa theory involving pairs of analogues of $\mathcal{X}$ and L_p for the extension $\mathbb{Q}_\infty$. In Sections 3 and 5, we then give a strategy for the proof of the main conjecture. In between in Section 4, we describe chromatic Iwasawa theory for imaginary quadratic fields. Section 5 is dedicated to the scrutiny of rank growth in the $\mathbb{Z}_p^2$-extension. Unlike the Kato–Rohrlich theorem, the rank does not stay bounded and we give an upper growth estimate. The reader who is only interested in this growth of ranks may only read the even sections.

2. Chromatic (♯/♭) Iwasawa Theory

When $p|a_p$, the objects appearing in the main conjecture encounter problems on both the algebraic and analytic sides. $\mathcal{X}_{\mathbb{Q}_\infty}$ is not Λ-torsion, while L_p is not a power series with bounded coefficients, so that one cannot even

formulate a main conjecture in the classical form. A solution is to compatibly divide the local points $E(\mathbb{Q}_{n,p})$ that appear in the Selmer group in half, giving rise to a pair of Selmer groups, and thus of a pair of objects $\mathcal{X}^\sharp_{\mathbb{Q}_\infty}$ and $\mathcal{X}^\flat_{\mathbb{Q}_\infty}$ which are torsion Λ-modules. Correspondingly, there is a construction of p-adic L-functions $L_p^\sharp$, $L_p^\flat$ which are elements of Λ, out of the badly behaved analogues of L_p.

One central idea in this construction is a pair of maps, the chromatic Coleman maps[1] $\mathrm{Col}_p^\sharp$ and $\mathrm{Col}_p^\flat$. For simplicity, let us describe the $\sharp$-Coleman map, since the $\flat$ case is analogous. This is a map

$$\mathrm{Col}_p^\sharp : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T_p) \to \Lambda,$$

where $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, \cdot) = \varprojlim_{\mathbb{Q}_{\infty,p} \supset L \supset \mathbb{Q}_p} H^1(L, \cdot)$, $\mathbb{Q}_p$ denotes the p-adic rationals, and T_p is the Tate module for E. From the kernel $\ker \mathrm{Col}_p^\sharp$ of the $\sharp$-Coleman map, one can define a Selmer group dual $\mathcal{X}^\sharp$ in an analogous way to $\mathcal{X}_{\mathbb{Q}_\infty}$. Thus, $\mathcal{X}^\sharp$ encodes the interplay between the global points $E(\mathbb{Q}_n)$ for the various n on one side, and the local points $E(\mathbb{Q}_{n,v})$ for $v \neq p$ and $(\ker \mathrm{Col}_p^\sharp)^\perp$ on the other side. The orthogonality here is with respect to the Tate pairing. (See [17, Section 8.5] and [29, Section 5] for details. For a general survey in the case $a_p = 0$, see also [11, Section 1].)

A crucial property is that the chromatic Coleman maps send the local image of Kato's zeta element to the chromatic p-adic L-functions.

Proposition 2.1. $\mathrm{Col}_p^\sharp(z_{Kato}) = L_p^\sharp$.

Proof. This proposition follows from noting that these two elements of Λ agree at infinitely many values, and then combining [29, Definition 6.1, Main Theorem 6.12] and [32, Theorem 2.14]. □

Analogously to the ordinary case, we can then formulate a main conjecture asking whether

$$\mathrm{Char}\, \mathcal{X}^\sharp = (L_p^\sharp).$$

The proposition above then shows that this main conjecture is equivalent to those of Kato's and Perrin-Riou's, which can be found in [14, Conjecture 12.10] and [23, Section 3.4], but see also [24]. Further, the work of Kato allows us to show that we have $L_p^\sharp \in \mathrm{Char}\, \mathcal{X}^\sharp$ [31, Theorem 7.16], much like in the ordinary case.

We shall discuss in the next section the proof of the other inclusion:

Theorem 2.2 (Wan when $a_p = 0$ [35], S. when $p|a_p$ [31])**.** *Let $p|a_p$. If E has square-free conductor, then the main conjecture holds.*

[1]The term "Coleman maps" has become the standard terminology since it was introduced in the work of Kobayashi [17], the idea being that they are analogues of Coleman's maps for cyclotomic units. However, the term "Perrin-Riou map" would be appropriate as well, and was used in the original version of [17].

3. Proof of the inclusion Char $\mathcal{X}^\sharp \subset (L_p^\sharp)$

While a formulation of the chromatic main conjecture is important for applications to the Birch and Swinnerton-Dyer formula, the proof of the other inclusion rests on Greenberg's formulation of main conjectures in terms of automorphic representations [8]. Let K be an imaginary quadratic field in which p splits, assume for simplicity that the class number h_K is coprime to p, and put $\Lambda_K = \mathcal{O}_K[\![X, Y]\!]$. Here, the variables X and Y correspond to generators of two different $\mathbb{Z}_p$-extensions of K. (They are the ray class fields of infinite powers of the two primes $\mathfrak{p}$ and $\mathfrak{q}$ above p. One reason we need $\mathfrak{p} \neq \mathfrak{q}$ is so that we can handle the variables X and Y separately.)

Greenberg's machinery associates to the input E and (a CM-form, call it f_K associated to) K a main conjecture

$$\operatorname{Char} \mathcal{X}^{Gr} = (L_p^{Gr}) \subset \Lambda_K \otimes \mathbb{Q}.$$

Although E has supersingular reduction at p, the CM-form f_K is ordinary[2], and this is what makes Greenberg's formulation possible: the Selmer group dual comes from a local condition that satisfies the so-called "Panchishkin condition", see [8, p. 211, Section 3].

Greenberg's formulation of the main conjecture is more amenable to proof:

Theorem 3.1 (Wan [35])**.** *Under mild technical assumptions and up to some easily controllable primes, we have* $\mathcal{X}^{Gr} \subset (L_p^{Gr})$.

The assumptions in the theorem hold when the elliptic curve has square-free conductor. The "easily controllable" primes by which the inclusion is off are primes which disappear when passing from the two-variable main conjecture to two one-variable main conjectures – the interested reader may read [31, Section 4.3] for a discussion of this.

The proof uses heavily that the CM-form f_K is ordinary, and it is this ordinarity that allows Wan to employ the methods of congruences of Eisenstein series for the group $U(3,1)$, heavily building on the methods of Hsieh for $U(2,1)$ [12].

To relate this to the chromatic main conjectures, we want to lift the objects in Section 2 from $\mathbb{Q}$ to K.

4. Interlude: Chromatic Coleman maps for imaginary quadratic fields

We let K be a quadratic imaginary field with class number coprime to p and so that $p = \mathfrak{pq}$ is split, with the class number h_K coprime to p. We know from class field theory that there is a unique $\mathbb{Z}_p^2$-extension of K, denoted

[2] it is in fact a Hida family

K_∞. Assume we have chosen K so that that there is a unique prime in K_∞ above $\mathfrak{p}$ and the same for $\mathfrak{q}$. We let K_n be the intermediate n-th layer, characterized by the fact that $\mathrm{Gal}(K_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z})^2$. We denote by Λ_K the Iwasawa algebra associated to $\mathrm{Gal}(K_\infty/K)$.

As in Section 2, we can analogously define $\mathcal{X}_{K_\infty}$, and encounter the problem that $\mathcal{X}_{K_\infty}$ is not Λ_K-torsion. To generalize the solution of Section 2, choose a prime $\varpi \in \{\mathfrak{p}, \mathfrak{q}\}$. This allows us to consider

$$H^1_{\mathrm{Iw}}(K_\varpi, \cdot\,) := \varprojlim_{(K_\infty)_\varpi \supset L \supset K_\varpi} H^1(L, \cdot\,),$$

and chromatic Coleman maps

$$\mathrm{Col}^\sharp_\varpi : H^1_{\mathrm{Iw}}(K_\varpi, T_p) \to \Lambda_K,$$

and $\mathrm{Col}^\flat_\varpi$.

The kernel of each $\mathrm{Col}^{\sharp/\flat}_\varpi$ then gives rise to a local condition at ϖ, allowing us to define four chromatic Selmer groups $\mathcal{X}^{\circ\bullet}$, where $\circ$ and $\bullet$ are each chosen from $\{\sharp, \flat\}$ and $\circ$ denotes the local condition at $\mathfrak{p}$ and $\bullet$ at $\mathfrak{q}$. For example, $\mathcal{X}^{\sharp\flat}$ encodes the interplay between the system of global points $E(K_n)$ as n varies and three types of local information: At places v not dividing p, this local information is the points $E(K_{n,v})$, at the place $\mathfrak{p}$ it is the condition $(\ker \mathrm{Col}^\sharp_\mathfrak{p})^\perp$, and finally at $\mathfrak{q}$, it is $(\ker \mathrm{Col}^\flat_\mathfrak{q})^\perp$.

In the case $a_p = 0$, the construction of the four chromatic Selmer groups is due to B.D Kim [15]. See also [11, Definition 1.3]. (For the general supersingular case, see [31].)

5. Proof of the inclusion $\mathrm{Char}\,\mathcal{X}^\sharp \subset (L_p^\sharp)$, continued

We would like to progress as in Section 2 and use the chromatic Coleman maps to relate Euler systems to p-adic L-functions.

There are compatible cohomology classes ("Euler systems") associated to E and (the CM-form f_K associated to) K due to Kings, Loeffler, and Zerbes [16]. There is in fact a pair of such classes, one for (the stabilization of the modular form corresponding to E associated to) each eigenvalue α and β of Frobenius. The resulting pair of objects Δ_α and Δ_β is in contrast to z_{Kato} not integral, so that it(s local image) does not land inside $H^1_{\mathrm{Iw}}(K_\mathfrak{q}, T_p)$.

The idea for the remedy is to factor[3] this pair as

$$(\Delta_\alpha, \Delta_\beta) = (\Delta_\sharp, \Delta_\flat)\mathcal{L}og$$

for an explicit 2×2 matrix $\mathcal{L}og$ and cohomology classes $\Delta_\sharp \in H^1_{\mathrm{Iw}}(K_\mathfrak{q}, T_p)$ and $\Delta_\flat \in H^1_{\mathrm{Iw}}(K_\mathfrak{q}, T_p)$.

One of the four analogues of Proposition 2.1 is then

[3]In the interest of sketching the main idea, we ignored some controllable denominators that appear in this factorization. See ([31, 35]) for details.

Proposition 5.1 ([31, Section 4.2]). $\mathrm{Col}_{\mathfrak{q}}^{\sharp}(\Delta_\flat) = L^{\flat\sharp} \in \Lambda_K$, *up to a controllable factor.*

The chromatic p-adic L-functions $L^{\flat\sharp}$ are two-variable generalizations, due to Lei [18], of the chromatic p-adic L-functions constructed in [29] for the one-variable case (i.e. for the case $\mathbb{Q}_\infty$). These chromatic p-adic L-functions in [29] generalize a construction of Pollack for the case $a_p = 0$ [25].

There are (up to [4]) four chromatic main conjectures of the form

Main Conjecture 5.2. *For* $\circ, \bullet \in \{\sharp, \flat\}$ *so that* $L^{\circ\bullet} \neq 0$, *we have*

$$\mathrm{Char}\, \mathcal{X}^{\circ\bullet} = (L^{\circ\bullet}).$$

Proposition 5.1 and its three analogues then allow us to show an equivalence of main conjectures

(Main Conjecture in terms of $\Delta_\sharp$ or $\Delta_\flat$) $\iff$ (Main Conjecture 5.2). The "Main Conjecture in terms of $\Delta_\sharp$ or $\Delta_\flat$" is a main conjecture in which the analytic side of the conjecture involves the quotient of a cohomology group by $\Delta_\sharp$ or $\Delta_\flat$. They[5] are thus analogues of Kato's main conjecture in terms of zeta elements. See e.g. [31, Introduction] for more details. However, we want to relate 5.2 to the Greenberg-type Main Conjecture. To do this, we construct a regulator map $\mathfrak{L}_{\mathfrak{p}}^{\sharp}$ so that $\mathfrak{L}_{\mathfrak{p}}^{\sharp}(\Delta_\sharp) = L_p^{Gr}$ (up to a controllable constant). This was done in the case $a_p = 0$ by Wan [35]. For the general supersingular case, see [31].

The regulator map $\mathfrak{L}_{\mathfrak{p}}^{\sharp}$ (resp. its twin $\mathfrak{L}_{\mathfrak{p}}^{\flat}$) allows us to connect the main conjectures in terms of Greenberg's objects to that in terms of $\Delta_\sharp$ (resp $\Delta_\flat$):

(Main Conjecture in terms of $\Delta_\sharp$ or $\Delta_\flat$) $\iff$ ($\mathrm{Char}\, \mathcal{X}^{Gr} = (L_p^{Gr})$). In fact, the two equivalences hold at the level of inclusions, so that we obtain

Corollary 5.3. *Choose* K *so that* $L^{\sharp\sharp} \neq 0$. *Then*

$$\mathrm{Char}\, \mathcal{X}^{\sharp\sharp} \subset (L^{\sharp\sharp}) \iff \mathrm{Char}\, \mathcal{X}^{Gr} \subset (L_p^{\mathrm{Gr}}).$$

The right-hand side is Theorem 3.1, proving half of the chromatic main conjecture 5.2. Recall that Kato's result gave us that $(L_p^{\sharp}) \subset \mathrm{Char}\, \mathcal{X}^{\sharp}$, i.e. the reverse inclusion in the case of one-variable chromatic main conjectures. Combining these facts together, one gets (see [31, Section 5] for the precise arguments) that

$$\mathrm{Char}\, \mathcal{X}^{\sharp} = (L_p^{\sharp}),$$

[4] as many as there are non-zero chromatic p-adic L-functions. We know at least one of them is non-zero. Thus, there is at least one conjectured equality in the Main Conjecture 5.2.

[5] We conjecture that both $\Delta_\sharp$ and $\Delta_\flat$ are non-zero, in which case there are indeed two main conjectures. However, we only know that at least one of the $\Delta's$ is non-zero, which we work with. Cf. previous footnote.

i.e. the main conjecture holds.

A corollary of the main conjecture is the p-part of the Birch and Swinnerton-Dyer formula.

Corollary 5.4. *Let $p > 2$ be a good supersingular prime. If E has square-free conductor and $r := \operatorname{ord}_{s=1} L(E,s) = 0$ or 1, then the p-part of the Birch and Swinnerton-Dyer formula holds, i.e.*

$$\operatorname{ord}_p\left(\frac{L^r(E,1)}{\Omega_E \operatorname{Reg}_E}\right) = \operatorname{ord}_p\left(\frac{\#Ш(E)\Pi c_l}{\#E_{\mathrm{tors}}(\mathbb{Q})^2}\right).$$

See [5] how to prove the corollary for ordinary primes. For $a_p = 0$, Wan easily modifies Greenberg's arguments, but for $a_p \neq 0$, one needs a more involved argument [31, Sections 5.1 and 5.2].

Combined with the p-part for ordinary p ([14, 28]) and multiplicative p ([27]), and most importantly, recent work of Cai–Li–Zhai [3] for $p = 2$, we can thus prove:

Corollary 5.5 ([31, Discussion after Corollary 1.4])**.** *For a prime p and an integer $a \in (-2\sqrt{p}, 2\sqrt{p})$, there are infinitely many elliptic curves E with $a_p(E) = a$ satisfying the full Birch and Swinnerton-Dyer conjecture.*

6. The growth of ranks along $\mathbb{Z}_p^2$-extensions (joint with A. Lei)

For a number field F, we denote by $r(F)$ the Mordell–Weil rank of $E(F)$.

6.1. Previously known results. The result of Kato and Rohrlich extends to cyclotomic $\mathbb{Z}_p$-extensions of any abelian extension of $\mathbb{Q}$, so we know that the rank is bounded inside the cyclotomic $\mathbb{Z}_p$-extension K_{cyc} of K. In fact, much more is conjectured:

Conjecture 6.1 (Mazur)**.** *The rank is bounded in any $\mathbb{Z}_p$-extension of K except the anticyclotomic one.*

The anticyclotomic $\mathbb{Z}_p$-extension has been scrutinized in various works. Denote by K_n^{ac} its n-th layer (so that $\operatorname{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$).

Theorem 6.2 (Agboola–Howard [1], Bertolini [2], Cornut [6], Greenberg [9], Longo–Vigni [22], Vatsal [34])**.** *We have the estimate*

$$r(K_n) \leqslant 2p^n + \mathcal{O}(1)$$

(and the coefficient 2 can be replaced by 1 or 0 in various cases.)

6.2. The main result. Recall that K_n was the n-th layer of the $\mathbb{Z}_p^2$-extension of K. We let $\Gamma_n := \operatorname{Gal}(K_\infty/K_n)$. In the main result below, we need to assume the following torsion hypothesis (tor) in the case $p|a_p$:

(tor) At least two of $\mathcal{X}^{\sharp\sharp}, \mathcal{X}^{\sharp\flat}, \mathcal{X}^{\flat\sharp}, \mathcal{X}^{\flat\flat}$ are Λ_K-torsion.

(The analogue of (tor) when $p \nmid a_p$ is Theorem 6.5 explained below.)

The main result is:

Theorem 6.3 (Lei–S. [20, Theorem 1.1])**.** *Assume that $p \nmid h_K$. When $p \nmid a_p$, we have $r(K_n) = \mathcal{O}(p^n)$. When $p|a_p$, then we also have $r(K_n) = \mathcal{O}(p^n)$ provided* (tor) *holds.*

6.3. Proof of Theorem 6.3 when $p \nmid a_p$. In the ordinary case, the proof of the theorem is an application of two theorems:

Theorem 6.4 (Greenberg [9])**.** *"$\mathcal{X}_{K_\infty}$ controls $\mathcal{X}_{K_n}$", i.e. we have short exact sequences*

$$0 \longrightarrow \ker \varphi_n \longrightarrow \mathrm{Sel}_{p^\infty}(E/K_n) \xrightarrow{\varphi_n} \mathrm{Sel}_{p^\infty}(E/K_\infty)^{\Gamma_n} \longrightarrow \operatorname{coker} \varphi_n \longrightarrow 0,$$

and the sizes of $\ker \varphi_n$ *and* $\operatorname{coker} \varphi_n$ *are bounded as n varies.*

Building on results of Hachimori–Venjakob [10, Theorem 2.8] and Coates–Schneider–Sujatha [4, Proposition 2.9], Van Order proved[6]:

Theorem 6.5 (Van Order [33, Theorem 3.8])**.** *$\mathcal{X}_{K_\infty}$ is a finitely generated torsion Λ_K-module.*

For a $\mathbb{Z}_p$-module M, let $M^* := \mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ be its Pontryagin dual.

The corollary of the two above theorems is the following:

Corollary 6.6. *We have that*

$$r(K_n) \leqslant \mathrm{rk}_{\mathbb{Z}_p} \mathcal{X}_{K_n} \leqslant \mathrm{rk}_{\mathbb{Z}_p} \left(\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\Gamma_n}\right)^* = \mathcal{O}(p^n)$$

Note that in the corresponding situation for $\mathbb{Q}_\infty$ (where one applies the original control theorem of Mazur and the finite generation theorem of Kato), the estimate on the right-hand side is $\mathcal{O}(1)$.

The toy example to keep in mind that illustrates why we should get $\mathcal{O}(p^n)$ is

$$\mathcal{X}_{K_\infty} = \mathrm{Sel}_{p^\infty}(E/K_\infty))^* \cong \mathbb{Z}_p[\![X, Y]\!]/(X).$$

6.4. Proof of Theorem 6.3 when $p|a_p$.

6.4.1. ***The case $a_p = 0$.*** When $a_p = 0$, which is automatic as soon as $p \geqslant 5$ because of the Hasse–Weil bound $|a_p| \leqslant 2\sqrt{p}$, Kim has proved an analogue of Greenberg's Control Theorem [15], generalizing ideas of Kobayashi in the case for $\mathbb{Q}_\infty$.

The idea is to write the local condition $(\ker \mathrm{Col}_{\varpi}^{\sharp/\flat})^\perp$ explicitly as a limit of local points $E^{\sharp/\flat}(K_{n,\varpi})$ using trace conditions. For example, $E^\flat(K_{n,\varpi}) = \{P \in E(K_{n,\varpi}) : \mathrm{Tr}_{n/m} P \in E(K_{m-1,\varpi}) \text{ if } m \equiv n \bmod 2\}$ ("the traces lie one level lower than you expect every other time"). This allows one to

[6]Van Order's theorem is in the context of non-CM curves, but her arguments work in the CM case as well.

almost decompose $E(K_{n,\varpi}) \cong E^\sharp(K_{n,\varpi}) \oplus E^\flat(K_{n,\varpi})$. (This is not quite true as there turns out to be a small intersection.)

Using ideas similar to those of the ordinary case, we conclude that the chromatic Selmer groups control the chromatic Selmer groups at finite level, e.g. $\mathcal{X}^{\sharp\sharp}$ controls $\mathcal{X}^{\sharp\sharp\sharp}_{K_n} = \left(\mathrm{Sel}_p^\infty(E/K_n)\right)^*$. In view of the almost decomposition from above, this allows us to then control the growth of the rank of the rational points.

6.4.2. ***The case $a_p \neq 0$.*** When $a_p \neq 0$, a new idea is needed: We first control an auxiliary object, the fine Selmer group, by means of techniques similar to those used in the ordinary case, and then we use the chromatic Coleman maps to study the discrepancy between the fine Selmer group and the Selmer group we are interested in.

We can control the fine Selmer groups $\mathrm{Sel}^0(E/K_n)$, which encode the relationship between $E(K_n)$ on the one hand, and the points $E(K_{n,v})$ for $v \nmid p$ and 0 for $v|p$ on the other hand. (We can control them via their inverse limit, which is Λ_K-torsion.) This gives us a short exact sequence

$$0 \longrightarrow \ker f_n \xrightarrow{f_n} \mathcal{X}_{K_n} \longrightarrow \mathcal{X}^0_{K_n} \longrightarrow 0,$$

where $\mathcal{X}^0_{K_n} = (\mathrm{Sel}_p^\infty(E/K_n)^0)^*$. Since the strategy for the ordinary case works for $\mathcal{X}^0_{K_n}$, we know that the $\mathbb{Z}_p$-rank of $\mathcal{X}^0_{K_n}$ is $\mathcal{O}(p^n)$. To say the same about $\mathcal{X}_{K_n}$, we must therefore show that $\mathcal{Y}_n := \ker(f_n)$ has $\mathbb{Z}_p$-rank $\mathcal{O}(p^n)$.

To prove that $\mathrm{rk}_{\mathbb{Z}_p} \mathcal{Y}_n = \mathcal{O}(p^n)$, the idea is to encode rank growth as zeroes of p-adic power series. In our proof, we do this for a slightly larger module $\mathcal{Y}'_n$. (See [20, Section 5.3] for the precise definitions. We have the inequality $\mathrm{rk}_{\mathbb{Z}_p} \mathcal{Y}_n \leqslant \mathrm{rk}_{\mathbb{Z}_p} \mathcal{Y}'_n$.)

By a theorem of Cuoco and Monsky [7], we have that

$$\mathrm{rk}_{\mathbb{Z}_p} \mathcal{Y}'_n - \mathrm{rk}_{\mathbb{Z}_p} \mathcal{Y}'_{n-1} = \sum_{\theta\text{: new characters in } \mathrm{Gal}(K_n/K)} \mathrm{rk}_{\mathbb{Z}_p} e_\theta \mathcal{Y}'_n,$$

where by "new" we mean characters of $\mathrm{Gal}(K_n/K)$ which do not factor through $\mathrm{Gal}(K_{n-1}/K)$.

One can then analyze the idempotent components and show that

$$\mathrm{rk}_{\mathbb{Z}_p} e_\theta \mathcal{Y}'_n = (p^n - p^{n-1}) \times \begin{cases} 0 \\ 1 \\ 2. \end{cases}$$

We are interested when $\mathrm{rk}_{\mathbb{Z}_p} e_\theta \mathcal{Y}'_n > 0$. The (kernel of) the Bloch-Kato exponential map detects rational points, and a p-adic version of this for quadratic imaginary fields was worked out in [21]. Using techniques from [30] and others that are similar to the ones that let us construct the chromatic

p-adic L-functions from the unbounded ones, we then show that

$$\mathrm{rk}_{\mathbb{Z}_p} e_\theta \mathcal{Y}'_n > 0 \text{ implies that } \det \left(\begin{smallmatrix} * & * \\ * & * \end{smallmatrix}\right) \text{ vanishes when evaluating at } \theta$$

for certain power series $*$ constructed in such a way that $\det \left(\begin{smallmatrix} * & * \\ * & * \end{smallmatrix}\right)$ is a sum of auxiliary power series[7]. Detecting the zeroes of this expression directly is hard, but we can give a criterion for the p-adic valuations of these auxiliary power series being different (so that their sum is not zero) that is often satisfied. (The criterion is that the conductor of θ has large $\mathfrak{p}$-power part or large $\mathfrak{q}$-power part, or that the difference between these parts is large.) Thus, the determinant doesn't vanish then.

We thus conclude that the determinant vanishing "happens rarely", say less than C_n times.

Thus, we have

$$\mathrm{rk}_{\mathbb{Z}_p} \mathcal{Y}'_n - \mathrm{rk}_{\mathbb{Z}_p} \mathcal{Y}'_{n-1} \leqslant 2C_n(p^n - p^{n-1}).$$

A calculation shows that C_n is independent of n, i.e.

$$C_n \leqslant C,$$

from which we conclude that

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathcal{Y}'_n) \leqslant 2Cp^n.$$

6.4.3. ***Recent developments.*** The work of Lei–Ponsinet [19] gives an analogue for abelian varieties of the last part of the proof, i.e. a formulation of a criterion for rank growth. In another development, the work of Hung and Lim [13] scrutinizes general p-adic Lie extensions. Reducing to our setup, they formulate a conjecture that is more precise than our result: Their conjecture says that when $a_p = 0$,

$$r(K_n) \leqslant 4p^n + r(K^{\mathrm{cyc}}).$$

Acknowledgments. We thank Antonio Lei, Joël Bellaïche, and the anonymous referee for valuable comments and suggestions.

References

[1] A. Agboola & B. Howard, "Anticyclotomic Iwasawa theory of CM elliptic curves. II", *Math. Res. Lett.* **12** (2005), no. 5-6, p. 611-621.

[2] M. Bertolini, "Selmer groups and Heegner points in anticyclotomic $\mathbf{Z}_p$-extensions", *Compos. Math.* **99** (1995), no. 2, p. 153-182.

[3] L. Cai, C. Li & S. Zhai, "On the 2-part of the Birch and Swinnerton-Dyer conjecture for quadratic twists of elliptic curves", *J. Lond. Math. Soc.* **101** (2020), no. 2, p. 714-734, https://arxiv.org/abs/https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/jlms.12284.

[4] J. Coates, P. Schneider & R. Sujatha, "Links between cyclotomic and GL_2 Iwasawa theory", *Doc. Math.* (2003), no. Extra Vol., p. 187-215, Kazuya Kato's fiftieth birthday.

[7] which depend on n. The sum involves four terms.

[5] J. H. Coates, K. A. Ribet, R. Greenberg & K. Rubin, *Arithmetic theory of elliptic curves*, Lecture Notes in Mathematics, vol. 1716, Springer, 1999, Lectures given at the 3rd Session of the Centro Internazionale Matematico Estivo (C.I.M.E.) held in Cetraro, Italy, July 12–19, 1997, viii+234 pages.

[6] C. Cornut, "Mazur's conjecture on higher Heegner points", *Invent. Math.* **148** (2002), no. 3, p. 495-523.

[7] A. A. Cuoco & P. Monsky, "Class numbers in $\mathbf{Z}_p^d$-extensions", *Math. Ann.* **255** (1981), no. 2, p. 235-258.

[8] R. Greenberg, "Iwasawa theory and p-adic deformations of motives", in *Motives (Seattle, WA, 1991)*, Proceedings of Symposia in Pure Mathematics, vol. 55, American Mathematical Society, 1994, p. 193-223.

[9] ———, "Galois theory for the Selmer group of an abelian variety", *Compos. Math.* **136** (2003), no. 3, p. 255-297.

[10] Y. Hachimori & O. Venjakob, "Completely faithful Selmer groups over Kummer extensions", *Doc. Math.* (2003), no. Extra Vol., p. 443-478, Kazuya Kato's fiftieth birthday.

[11] P. Hamidi & J. Ray, "Conjecture A and μ-invariant for Selmer groups of supersingular elliptic curves", *J. Théor. Nombres Bordeaux* **33** (2021), no. 3.1, p. 853-886.

[12] M.-L. Hsieh, "Eisenstein congruence on unitary groups and Iwasawa main conjectures for CM fields", *J. Am. Math. Soc.* **27** (2014), no. 3, p. 753-862.

[13] P.-C. Hung & M. F. Lim, "On the growth of Mordell-Weil ranks in p-adic Lie extensions", `https://arxiv.org/abs/1902.01068`, 2019.

[14] K. Kato, "p-adic Hodge theory and values of zeta functions of modular forms", in *Cohomologies p-adiques et applications arithmétiques. III*, Astérisque, vol. 295, Société Mathématique de France, 2004, p. 117-290.

[15] B. D. Kim, "Signed-Selmer groups over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field", *Can. J. Math.* **66** (2014), no. 4, p. 826-843.

[16] G. Kings, D. Loeffler & S. L. Zerbes, "Rankin-Eisenstein classes and explicit reciprocity laws", *Camb. J. Math.* **5** (2017), no. 1, p. 1-122.

[17] S.-i. Kobayashi, "Iwasawa theory for elliptic curves at supersingular primes", *Invent. Math.* **152** (2003), no. 1, p. 1-36.

[18] A. Lei, "Factorisation of two-variable p-adic L-functions", *Can. Math. Bull.* **57** (2014), no. 4, p. 845-852.

[19] A. Lei & G. Ponsinet, "On the Mordell–Weil ranks of supersingular abelian varieties in cyclotomic extensions", *Proc. Am. Math. Soc., Ser. B* **7** (2020), p. 1-16.

[20] A. Lei & F. Sprung, "Ranks of elliptic curves over $\mathbb{Z}_p^2$-extensions", *Isr. J. Math.* **236** (2020), no. 1, p. 183-206.

[21] D. Loeffler & S. L. Zerbes, "Iwasawa theory and p-adic L-functions over $\mathbb{Z}_p^2$-extensions", *Int. J. Number Theory* **10** (2014), no. 8, p. 2045-2095.

[22] M. Longo & S. Vigni, "Plus/minus Heegner points and Iwasawa theory of elliptic curves at supersingular primes", *Boll. Unione Mat. Ital.* **12** (2019), no. 3, p. 315-347.

[23] B. Perrin-Riou, "Fonctions L p-adiques d'une courbe elliptique et points rationnels", *Ann. Inst. Fourier* **43** (1993), no. 4, p. 945-995.

[24] ———, *Fonctions L p-adiques des représentations p-adiques*, Astérisque, vol. 229, Société Mathématique de France, 1995, 198 pages.

[25] R. Pollack, "On the p-adic L-function of a modular form at a supersingular prime", *Duke Math. J.* **118** (2003), no. 3, p. 523-558.

[26] D. E. Rohrlich, "On L-functions of elliptic curves and cyclotomic towers", *Invent. Math.* **75** (1984), no. 3, p. 409-423.

[27] C. Skinner, "Multiplicative reduction and the cyclotomic main conjecture for GL_2", *Pac. J. Math.* **283** (2016), no. 1, p. 171-200.

[28] C. Skinner & E. Urban, "The Iwasawa main conjectures for GL_2", *Invent. Math.* **195** (2014), no. 1, p. 1-277.

[29] F. Sprung, "Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures", *J. Number Theory* **132** (2012), no. 7, p. 1483-1506.

[30] ———, "The Šafarevič–Tate group in cyclotomic $\mathbb{Z}_p$-extensions at supersingular primes", *J. Reine Angew. Math.* **681** (2013), p. 199-218.
[31] ———, "The Iwasawa Main Conjecture for Elliptic Curves at odd supersingular primes", `https://arxiv.org/abs/1610.10017`, submitted, 2016.
[32] ———, "On pairs of p-adic L-functions for weight-two modular forms", *Algebra Number Theory* **11** (2017), no. 4, p. 885-928.
[33] J. Van Order, "Some remarks on the two-variable main conjecture of Iwasawa theory for elliptic curves without complex multiplication", *J. Algebra* **350** (2012), p. 273-299.
[34] V. Vatsal, "Special values of anticyclotomic L-functions", *Duke Math. J.* **116** (2003), no. 2, p. 219-261.
[35] X. Wan, "Iwasawa Main Conjecture and BSD Conjecture", `https://arxiv.org/abs/1411.6352`, submitted, 2014.

Florian Ito Sprung
School of Mathematical and Statistical Sciences
Arizona State University
Tempe, AZ 85287-1804, USA
E-mail: `ian.sprung@gmail.com`