On growth of arithmetic objects in tower of number fields

Meng Fai Lim
Central China Normal University

Iwasawa theory and p-adic L-functions
Sun Yat-sen University
Apr 6th, 2022

Introduction

Throughout the talk, p will always denote an odd prime. Let F_∞ be a $\mathbb{Z}_p$-extension of F with intermediate subfields F_n. Set e_n to be the p-exponent of the class group of F_n, i.e.,

$$e_n = \log_p \left| Cl(F_n)[p^\infty] \right|$$

Introduction

Throughout the talk, p will always denote an odd prime. Let F_∞ be a $\mathbb{Z}_p$-extension of F with intermediate subfields F_n. Set e_n to be the p-exponent of the class group of F_n, i.e.,

$$e_n = \log_p \left| Cl(F_n)[p^\infty] \right|$$

Theorem (Iwasawa 1959)

There exist integers $\mu = \mu(F_\infty/F)$, $\lambda = \lambda(F_\infty/F)$ and $\nu(F_\infty/F)$ (independent of n) such that

$$e_n = \mu p^n + \lambda n + \nu \quad \text{for } n \gg 0.$$

Basic philosophy

To illustrate the idea, we use the $\mathbb{Z}_p[\![\Gamma]\!]$-context, where $\Gamma \cong \mathbb{Z}_p$ and $\Gamma_n = \Gamma^{p^n}$.

Basic philosophy

To illustrate the idea, we use the $\mathbb{Z}_p[\![\Gamma]\!]$-context, where $\Gamma \cong \mathbb{Z}_p$ and $\Gamma_n = \Gamma^{p^n}$.

Let M_n be a sequence of $\mathbb{Z}_p[\![\Gamma]\!]$-modules (of interest) with transition maps $M_{n+1} \longrightarrow M_n$, where each M_n is finitely generated over $\mathbb{Z}_p$ and the action of $\mathbb{Z}_p[\![\Gamma]\!]$ on M_n factors through $\mathbb{Z}_p[\Gamma/\Gamma_n]$. In Iwasawa theoretical context, one is usually interested in the growth of $M_n[p^\infty]$.

Basic philosophy

To illustrate the idea, we use the $\mathbb{Z}_p[\![\Gamma]\!]$-context, where $\Gamma \cong \mathbb{Z}_p$ and $\Gamma_n = \Gamma^{p^n}$.

Let M_n be a sequence of $\mathbb{Z}_p[\![\Gamma]\!]$-modules (of interest) with transition maps $M_{n+1} \longrightarrow M_n$, where each M_n is finitely generated over $\mathbb{Z}_p$ and the action of $\mathbb{Z}_p[\![\Gamma]\!]$ on M_n factors through $\mathbb{Z}_p[\Gamma/\Gamma_n]$. In Iwasawa theoretical context, one is usually interested in the growth of $M_n[p^\infty]$.

One then considers the inverse limit $M_\infty := \varprojlim_n M_n$, which in most application can be shown to be a finitely generated $\mathbb{Z}_p[\![\Gamma]\!]$-module and, under certain favorable condition, even a torsion $\mathbb{Z}_p[\![\Gamma]\!]$-module.

Basic philosophy

Apply (appropriate) module theory to obtain growth formula for

$$(M_\infty)_{\Gamma_n}[p^\infty].$$

This is the "algebraic" aspect.

Basic philosophy

Apply (appropriate) module theory to obtain growth formula for

$$(M_\infty)_{\Gamma_n}[p^\infty].$$

This is the "algebraic" aspect.

The next is the "arithmetic" aspect. Namely, one needs to understand the difference between $(M_\infty)_{\Gamma_n}[p^\infty]$ and $M_n[p^\infty]$.

However, there are situations, where $M_n[p^\infty]$ has "nothing to do" with $(M_\infty)_{\Gamma_n}[p^\infty]$.

Content

- Algebraic Aspects

- Arithmetic Aspects

ALGEBRAIC

ASPECTS

Algebraic results for $\mathbb{Z}_p[[\Gamma]]$

This case is essentially well-known and goes back to Iwasawa. We will present the most recent development in this aspect.

Algebraic results for $\mathbb{Z}_p[\![\Gamma]\!]$

This case is essentially well-known and goes back to Iwasawa. We will present the most recent development in this aspect.

Theorem (Lee 2020)

Let M be a finitely generated $\mathbb{Z}_p[\![\Gamma]\!]$-module. Then there exist μ, λ, ν such that

$$\log_p \left| M_{\Gamma_n}[p^\infty] \right| = \mu p^n + \lambda n + \nu$$

for $n \gg 0$.

Algebraic results for $\mathbb{Z}_p[\![\Gamma]\!]$

This case is essentially well-known and goes back to Iwasawa. We will present the most recent development in this aspect.

Theorem (Lee 2020)

Let M be a finitely generated $\mathbb{Z}_p[\![\Gamma]\!]$-module. Then there exist μ, λ, ν such that

$$\log_p \left| M_{\Gamma_n}[p^\infty] \right| = \mu p^n + \lambda n + \nu$$

for $n \gg 0$.

Remark: In Jaehoon Lee's result, M needs not be torsion!

Algebraic results for $\mathbb{Z}_p[[G]]$, $G \cong \mathbb{Z}_p^d$

We now consider the case when $G \cong \mathbb{Z}_p^d$. We shall write $G_n = G^{p^n} \cong (p^n\mathbb{Z}_p)^d$.

Algebraic results for $\mathbb{Z}_p[[G]]$, $G \cong \mathbb{Z}_p^d$

We now consider the case when $G \cong \mathbb{Z}_p^d$. We shall write $G_n = G^{p^n} \cong (p^n\mathbb{Z}_p)^d$.

Theorem (Cocuo-Monsky 81)

Let M be a finitely generated torsion $\mathbb{Z}_p[[G]]$-module, where $G \cong \mathbb{Z}_p^d$ with $d \geq 2$. Suppose that $\mathrm{rank}_{\mathbb{Z}_p}(M_{G_n}) = O(p^{(d-2)n})$. Then there exist integers μ, l_0 such that

$$\log_p \left| M_{G_n}[p^\infty] \right| = \mu p^{dn} + l_0 n p^{(d-1)n} + O(p^{(d-1)n}).$$

Remark (Harris 79): The module M is torsion over $\mathbb{Z}_p[[G]]$ if and only if $\mathrm{rank}_{\mathbb{Z}_p}(M_{G_n}) = O(p^{(d-1)n})$.

Algebraic results for $\mathbb{Z}_p[[G]]$, $G \cong \mathbb{Z}_p^d$

The following can be thought as an attempt to generalize Lee's result, although we only obtain a partial result.

Algebraic results for $\mathbb{Z}_p[\![G]\!]$, $G \cong \mathbb{Z}_p^d$

The following can be thought as an attempt to generalize Lee's result, although we only obtain a partial result.

Theorem (Liang-L 19)

Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module, where $G \cong \mathbb{Z}_p^d$. Then there exist an integer μ such that

$$\log_p \left| M_{G_n}[p^\infty] \right| = \mu p^{dn} + O(np^{(d-1)n}).$$

Powerful pro-p groups

Let G be a pro-p group.

Let $G^{\{p\}} = \{g^p \mid g \in G\}$, that is, the set of all pth-powers of elements in G.

Set $G^p = \langle g^p \mid g \in G \rangle$, that is, the group generated by the pth-powers of elements in G.

The lower p-series of G is given by $P_1(G) = G$, and

$$P_{n+1}(G) = \overline{P_n(G)^p [P_n(G), G]}, \text{ for } n \geq 1.$$

Powerful pro-p groups

Let G be a pro-p group.

Let $G^{\{p\}} = \{g^p | \ g \in G\}$, that is, the set of all pth-powers of elements in G.

Set $G^p = \langle g^p | \ g \in G \rangle$, that is, the group generated by the pth-powers of elements in G.

The lower p-series of G is given by $P_1(G) = G$, and

$$P_{n+1}(G) = \overline{P_n(G)^p[P_n(G), G]}, \text{ for } n \geq 1.$$

The pro-p group G is said to be **powerful** if $G/\overline{G^p}$ is abelian.

Powerful pro-p groups

Let G be a pro-p group.

Let $G^{\{p\}} = \{g^p |\ g \in G\}$, that is, the set of all pth-powers of elements in G.

Set $G^p = \langle g^p |\ g \in G\rangle$, that is, the group generated by the pth-powers of elements in G.

The lower p-series of G is given by $P_1(G) = G$, and

$$P_{n+1}(G) = \overline{P_n(G)^p[P_n(G), G]}, \text{ for } n \geq 1.$$

The pro-p group G is said to be **powerful** if $G/\overline{G^p}$ is abelian.

Fact: If G is a powerful pro-p group, then

$$G^{\{p^n\}} = G^{p^n} = P_{n+1}(G).$$

Powerful pro-p groups

Let G be a pro-p group.

Let $G^{\{p\}} = \{g^p \mid g \in G\}$, that is, the set of all pth-powers of elements in G.

Set $G^p = \langle g^p \mid g \in G \rangle$, that is, the group generated by the pth-powers of elements in G.

The lower p-series of G is given by $P_1(G) = G$, and

$$P_{n+1}(G) = \overline{P_n(G)^p[P_n(G), G]}, \text{ for } n \geq 1.$$

The pro-p group G is said to be **powerful** if $G/\overline{G^p}$ is abelian.

Fact: If G is a powerful pro-p group, then

$$G^{\{p^n\}} = G^{p^n} = P_{n+1}(G).$$

Personal opinion: Think of it as "power-full".

Uniform pro-p groups

For a powerful pro-p group G, the p-power map induces a surjection on

$$P_n(G)/P_{n+1}(G) \xrightarrow{\cdot p} P_{n+1}(G)/P_{n+2}(G)$$

is surjective for each $n \geq 1$.

Uniform pro-p groups

For a powerful pro-p group G, the p-power map induces a surjection on

$$P_n(G)/P_{n+1}(G) \xrightarrow{\cdot p} P_{n+1}(G)/P_{n+2}(G)$$

is surjective for each $n \geq 1$.

If the p-power maps are isomorphisms for all $n \geq 1$, we say that G is **uniformly powerful** (abrev. **uniform**). Note that in this case, we have an equality $|G : P_2(G)| = |P_n(G) : P_{n+1}(G)|$ for every $n \geq 1$. In fact, it is not difficult to see that $|G : P_{n+1}(G)| = p^{nd}$, where $d = \dim G$ $(= \dim_{\mathbb{Z}/p} H_1(G, \mathbb{Z}/p))$.

Examples of uniform pro-p groups

(1) $G = \mathbb{Z}_p^d$. One has $G_n = p^n \mathbb{Z}_p^d$.

(2) $G = \{x \in \mathrm{GL}_m(\mathbb{Z}_p) : x \equiv 1 \bmod p\}$.
In this case, we have $G_n = \{x \in \mathrm{GL}_m(\mathbb{Z}_p) : x \equiv 1 \bmod p^n\}$

Examples of uniform pro-p groups

(1) $G = \mathbb{Z}_p^d$. One has $G_n = p^n\mathbb{Z}_p^d$.

(2) $G = \{x \in \mathrm{GL}_m(\mathbb{Z}_p) : x \equiv 1 \bmod p\}$.
In this case, we have $G_n = \{x \in \mathrm{GL}_m(\mathbb{Z}_p) : x \equiv 1 \bmod p^n\}$

(3) A theorem of Lazard asserts that a closed subgroup G of $GL_m(\mathbb{Z}_p)$ contains a open normal uniform pro-p subgroup of G.

Torsion module

Let G be a uniform pro-p group. Then a theorem of Lazard tells us that $\mathbb{Z}_p[\![G]\!]$ is Noetherian with no zero divisors. Hence the ring $\mathbb{Z}_p[\![G]\!]$ admits a skew field $Q(G)$ which is known to be flat over $\mathbb{Z}_p[\![G]\!]$. Thus, it makes sense to define

$$\mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = \dim_{Q(G)}\big(Q(G) \otimes_{\mathbb{Z}_p[\![G]\!]} M\big).$$

Torsion module

Let G be a uniform pro-p group. Then a theorem of Lazard tells us that $\mathbb{Z}_p[\![G]\!]$ is Noetherian with no zero divisors. Hence the ring $\mathbb{Z}_p[\![G]\!]$ admits a skew field $Q(G)$ which is known to be flat over $\mathbb{Z}_p[\![G]\!]$. Thus, it makes sense to define

$$\mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = \dim_{Q(G)} \left(Q(G) \otimes_{\mathbb{Z}_p[\![G]\!]} M\right).$$

The module M is said to be **torsion** if $\mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = 0$. It can be shown that M is torsion if and only if $\mathrm{Hom}_{\mathbb{Z}_p[\![G]\!]}(M, \mathbb{Z}_p[\![G]\!]) = 0$.

Torsion module

Let G be a uniform pro-p group. Then a theorem of Lazard tells us that $\mathbb{Z}_p[\![G]\!]$ is Noetherian with no zero divisors. Hence the ring $\mathbb{Z}_p[\![G]\!]$ admits a skew field $Q(G)$ which is known to be flat over $\mathbb{Z}_p[\![G]\!]$. Thus, it makes sense to define

$$\mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = \dim_{Q(G)}\left(Q(G) \otimes_{\mathbb{Z}_p[\![G]\!]} M\right).$$

The module M is said to be **torsion** if $\mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = 0$. It can be shown that M is torsion if and only if $\mathrm{Hom}_{\mathbb{Z}_p[\![G]\!]}(M, \mathbb{Z}_p[\![G]\!]) = 0$.

A torsion $\mathbb{Z}_p[\![G]\!]$-module is then said to be **pseudo-null** if

$$\mathrm{Ext}^1_{\mathbb{Z}_p[\![G]\!]}(M, \mathbb{Z}_p[\![G]\!]) = 0.$$

μ_G-invariant

Unfortunately, for a general non-commutative uniform pro-p group, we do not have a nice enough structure theorem. The best we have at present is the following.

Theorem (Howson 02, Venjakob 02)

Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module, where G is a uniform pro-p group. Then there is a $\mathbb{Z}_p[\![G]\!]$-homomorphism

$$M[p^\infty] \longrightarrow \bigoplus_{i=1}^{s} \mathbb{Z}_p[\![G]\!]/p^{\alpha_i}$$

with kernel and cokernel being pseudo-null $\mathbb{Z}_p[\![G]\!]$-modules.

μ_G-invariant

Unfortunately, for a general non-commutative uniform pro-p group, we do not have a nice enough structure theorem. The best we have at present is the following.

Theorem (Howson 02, Venjakob 02)

Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module, where G is a uniform pro-p group. Then there is a $\mathbb{Z}_p[\![G]\!]$-homomorphism

$$M[p^\infty] \longrightarrow \bigoplus_{i=1}^{s} \mathbb{Z}_p[\![G]\!]/p^{\alpha_i}$$

with kernel and cokernel being pseudo-null $\mathbb{Z}_p[\![G]\!]$-modules.

We define the μ_G-invariant of M to be

$$\mu_G(M) = \sum_i^s \alpha_i.$$

Perbet's estimate

Building on the structure theorems of Howson and Venjakob, Perbet established the following.

Theorem (Perbet 2011)

Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module, where G is a uniform pro-p group of dimension d. Then we have

$$\log_p \left| M_{G_n}/p^n \right| = \mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}(M) n p^{dn} + \mu_G(M) p^{dn} + O(n p^{(d-1)n}).$$

Perbet's estimate

Building on the structure theorems of Howson and Venjakob, Perbet established the following.

Theorem (Perbet 2011)

Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module, where G is a uniform pro-p group of dimension d. Then we have

$$\log_p \left| M_{G_n}/p^n \right| = \mathrm{rank}_{\mathbb{Z}_p[\![G]\!]}(M) np^{dn} + \mu_G(M)p^{dn} + O(np^{(d-1)n}).$$

Note that Perbet's result is only giving an estimate for M_{G_n}/p^n rather than $M_{G_n}[p^\infty]$.

An estimate for $\mathbb{Z}_p^{d-1} \rtimes \mathbb{Z}_p$

One case where one can obtain a somewhat precise estimate is the following

An estimate for $\mathbb{Z}_p^{d-1} \rtimes \mathbb{Z}_p$

One case where one can obtain a somewhat precise estimate is the following

Theorem (Lei 17, Liang-L 19)

Let G be a pro-p group which contains a closed normal subgroup H such that $H \cong \mathbb{Z}_p^{d-1}$ and $G/H \cong \mathbb{Z}_p$. Let M be a $\mathbb{Z}_p[\![G]\!]$-module, which is finitely generated over $\mathbb{Z}_p[\![H]\!]$ with M_{G_n} being finite for every n. Then we have

$$\log_p \left| M_{G_n} \right| = \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}(M) n p^{(d-1)n} + O(p^{(d-1)n}).$$

An estimate for $\mathbb{Z}_p^{d-1} \rtimes \mathbb{Z}_p$

One case where one can obtain a somewhat precise estimate is the following

Theorem (Lei 17, Liang-L 19)

Let G be a pro-p group which contains a closed normal subgroup H such that $H \cong \mathbb{Z}_p^{d-1}$ and $G/H \cong \mathbb{Z}_p$. Let M be a $\mathbb{Z}_p[\![G]\!]$-module, which is finitely generated over $\mathbb{Z}_p[\![H]\!]$ with M_{G_n} being finite for every n. Then we have

$$\log_p \left| M_{G_n} \right| = \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}(M) n p^{(d-1)n} + O(p^{(d-1)n}).$$

Remark: The $\mathbb{Z}_p^{d-1}$ estimate of Liang-Lim is used here.

An upper bound for $H \rtimes \mathbb{Z}_p$

If one replace $\mathbb{Z}_p^{d-1}$ with a general H, we have the following

An upper bound for $H \rtimes \mathbb{Z}_p$

If one replace $\mathbb{Z}_p^{d-1}$ with a general H, we have the following

Theorem (Lei 17, L. 19)

Let G be a pro-p group which contains a closed normal subgroup H such that $G/H \cong \mathbb{Z}_p$. Let M be a $\mathbb{Z}_p[\![G]\!]$-module, which is finitely generated over $\mathbb{Z}_p[\![H]\!]$. Then we have

$$\log_p \left| M_{G_n}/p^n \right| \leq \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}(M) n p^{(d-1)n} + \mu_H(M) p^{(d-1)n} + O(np^{(d-2)n}).$$

ARITHMETIC

ASPECTS

Class groups

Theorem (Iwasawa 1959)

Let F_n denote the intermediate subfield of a $\mathbb{Z}_p$-extension F_∞/F with $|F_n : F| = p^n$. Then there exist integers $\mu = \mu(F_\infty/F)$, $\lambda = \lambda(F_\infty/F)$ and $\nu(F_\infty/F)$ (independent of n) such that

$$\log_p \left| Cl(F_n)[p^\infty] \right| = \mu p^n + \lambda n + \nu \quad \text{for } n \gg 0.$$

Class groups

Theorem (Iwasawa 1959)

Let F_n denote the intermediate subfield of a $\mathbb{Z}_p$-extension F_∞/F with $|F_n : F| = p^n$. Then there exist integers $\mu = \mu(F_\infty/F)$, $\lambda = \lambda(F_\infty/F)$ and $\nu(F_\infty/F)$ (independent of n) such that

$$\log_p \left| Cl(F_n)[p^\infty] \right| = \mu p^n + \lambda n + \nu \quad \text{for } n \gg 0.$$

Theorem (Cuoco-Monsky 81)

Let F_n denote the intermediate subfield of a $\mathbb{Z}_p^d$-extension F_∞/F with $\mathrm{Gal}(F_n/F) \cong (\mathbb{Z}/p)^d$. Then there exist integers μ and l_0 (independent of n) such that

$$\log_p \left| Cl(F_n)[p^\infty] \right| = \mu p^{dn} + \lambda n p^{(d-1)n} + O(p^{(d-1)}) \quad \text{for } n \gg 0.$$

A question of Venjakob

Let $F_\infty = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{p})$, and $F_n = \mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{p})$.

Question (Venjakob 02)

Do one have

$$\log_p \left| Cl(F_n)[p^\infty] \right| = \lambda n p^n + O(p^n) \quad \text{for } n \gg 0$$

for some λ?

A question of Venjakob

Let $F_\infty = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{p})$, and $F_n = \mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{p})$.

Question (Venjakob 02)

Do one have

$$\log_p \left| Cl(F_n)[p^\infty] \right| = \lambda n p^n + O(p^n) \quad \text{for } n \gg 0$$

for some λ?

Remark : Venjakob has shown "$\mu(X_{F_\infty}) = 0$", where X_{F_∞} is the Galois group of the p-Hilbert class field of F_∞ over F_∞.

A question of Venjakob

Let $F_\infty = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{p})$, and $F_n = \mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{p})$.

Question (Venjakob 02)

Do one have

$$\log_p \left| Cl(F_n)[p^\infty] \right| = \lambda n p^n + O(p^n) \quad \text{for } n \gg 0$$

for some λ?

Remark : Venjakob has shown "$\mu(X_{F_\infty}) = 0$", where X_{F_∞} is the Galois group of the p-Hilbert class field of F_∞ over F_∞.

Remark : Venjakob's question has been resolved by Antonio Lei.

A result of Lei

Theorem (Lei 17)

Let F_∞ be a $H \rtimes \mathbb{Z}_p$-extension of F with $H \cong \mathbb{Z}_p$. Suppose that the following statements hold.

1. F contains only one prime above p, and this prime is totally ramified in F_∞/F.
2. X_{F_∞} is finitely generated over $\mathbb{Z}_p[\![H]\!]$.

Then one has

$$\log_p \left|Cl(F_n)[p^\infty]\right| = \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}(X)np^n + O(p^n).$$

A result of Lei

Theorem (Lei 17)

Let F_∞ be a $H \rtimes \mathbb{Z}_p$-extension of F with $H \cong \mathbb{Z}_p$. Suppose that the following statements hold.

1. F contains only one prime above p, and this prime is totally ramified in F_∞/F.
2. X_{F_∞} is finitely generated over $\mathbb{Z}_p[\![H]\!]$.

Then one has

$$\log_p \left| Cl(F_n)[p^\infty] \right| = \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}(X) np^n + O(p^n).$$

Remark : Lei's result has been extended to the case $\mathbb{Z}_p^{d-1} \rtimes \mathbb{Z}_p$ by Liang-L. in 2019.

A result of Perbet

Theorem (Perbet 11)

Let F_∞ be an extension of F with $G = \mathrm{Gal}(F_\infty/F)$ being a uniform pro-p group of dimension n. Let F_n be the fixed field of G_n. Then one has

$$\log_p \left| Cl(F_n)[p^n] \right| = \mathrm{rank}_{\mathbb{Z}_p[[H]]}(X_{F_\infty}) n p^{dn} + \mu_H(X_{F_\infty}) p^{dn} + O(np^{(d-1)n}).$$

A result of Perbet

Theorem (Perbet 11)

Let F_∞ be an extension of F with $G = \mathrm{Gal}(F_\infty/F)$ being a uniform pro-p group of dimension n. Let F_n be the fixed field of G_n. Then one has

$$\log_p \left| Cl(F_n)[p^n] \right| = \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}(X_{F_\infty}) np^{dn} + \mu_H(X_{F_\infty}) p^{dn} + O(np^{(d-1)n}).$$

Remark : Perbet's result is concerned with $Cl(F_n)[p^n]$ rather than $Cl(F_n)[p^\infty]$.

An upper bound for $H \rtimes \mathbb{Z}_p$

If one replace $\mathbb{Z}_p^{d-1}$ with a general H, we have the following

An upper bound for $H \rtimes \mathbb{Z}_p$

If one replace $\mathbb{Z}_p^{d-1}$ with a general H, we have the following

Theorem (Lei 17, L. 19)

Let F_∞ be an extension of F such that $G = \mathrm{Gal}(F_\infty/F)$ is a uniform pro-p group which contains a closed normal subgroup H such that $G/H \cong \mathbb{Z}_p$. Suppose that X_{F_∞} is finitely generated over $\mathbb{Z}_p[\![H]\!]$. Then we have

$$\log_p \left| Cl(F_n)[p^n] \right| \leq \mathrm{rank}_{\mathbb{Z}_p[\![H]\!]}(X_{F_\infty}) np^{(d-1)n} + \mu_H(X_{F_\infty}) p^{(d-1)n} + O(np^{(d-2)n}).$$

K-groups

Let R be a ring with identity. Define $\mathrm{GL}(R) = \varinjlim_j \mathrm{GL}_j(R)$, where the transition map $\mathrm{GL}_j(R) \longrightarrow \mathrm{GL}_{j+1}(R)$ is given by

$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}.$$

K-groups

Let R be a ring with identity. Define $\mathrm{GL}(R) = \varinjlim_j \mathrm{GL}_j(R)$, where the transition map $\mathrm{GL}_j(R) \longrightarrow \mathrm{GL}_{j+1}(R)$ is given by

$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}.$$

The classifying space $B\mathrm{GL}(R)$ of the group $\mathrm{GL}(R)$ is a connected topological space whose fundamental group is $\mathrm{GL}(R)$ and the higher homotopy groups are zero. In other words,

$$\pi_i(B\mathrm{GL}(R)) = \begin{cases} \mathrm{GL}(R) & \text{if } i = 1, \\ 0, & \text{if } i \neq 1. \end{cases}$$

$K_i(R)$

$K_i(R)$

From $B\mathrm{GL}(R)$, there is a prescribed way (known as the $+$-construction) to obtain another space (more precisely, a certain CW-complex) $B\mathrm{GL}(R)^+$. Following Quillen, the K_i-groups are then defined to be

$$K_i(R) = \pi_i\big(B\mathrm{GL}(R)^+\big).$$

$K_i(R)$

From $B\mathrm{GL}(R)$, there is a prescribed way (known as the $+$-construction) to obtain another space (more precisely, a certain CW-complex) $B\mathrm{GL}(R)^+$. Following Quillen, the K_i-groups are then defined to be

$$K_i(R) = \pi_i\big(B\mathrm{GL}(R)^+\big).$$

Theorem (Quillen 73, Borel 1974)

Let $\mathcal{O}_F$ be the ring of integers of a number field F. For $i \geq 2$, the groups $K_{2i-2}(\mathcal{O}_F)$ are finite and

$$\operatorname{rank}_{\mathbb{Z}} K_{2i-1}(\mathcal{O}_F) = \begin{cases} r_1(F) + r_2(F), & \text{if } i \text{ is odd}, \\ r_2(F), & \text{if } i \text{ is even}. \end{cases}$$

Here $r_1(F)$ (resp., $r_2(F)$) is the number of real embeddings (resp., number of pairs of complex embeddings) of F.

Lichtenbaum's conjecture

Conjecture (Lichtenbaum 1972)

Let F be a number field and ζ_F the Dedekind zeta function of F. Then for $i \geq 2$, we have an equality (up to a power of 2)

$$\zeta_F^*(1-i) = \pm \frac{|K_{2i-2}(\mathcal{O}_F)|}{|K_{2i-1}(\mathcal{O}_F)_{\mathrm{tor}}|} R_i^B(F),$$

where $R_i^B(F)$ is the Borel regulator.

If F is an abelian totally real field, the conjecture is known thanks to a collective effort of Birch-Tate, Coates, Iwasawa, Quillen-Lichtenbaum, Soulé, Bayer-Neukirch, Mazur-Wiles, Quillen, Wiles, Kolster-Nguyen Quang Do-Fleckinger, Rost-Voevodsky and many others.

Analogue of Iwasawa asymptotic formula for K-groups

Theorem (Coates 1972, Ji-Qin 2013)

Let $i \geq 2$. Suppose that the number field F contains a primitive pth root of unity and F^{cyc} is the cyclotomic $\mathbb{Z}_p$-extension of F. Then one has that

$$\log_p \left| K_{2i-2}(\mathcal{O}_{F_n})[p^\infty] \right| = \mu(F^{\mathrm{cyc}}/F)p^n + \lambda(F^{\mathrm{cyc}}/F)n + O(1),$$

where $\mu(F^{\mathrm{cyc}}/F)$ and $\lambda(F^{\mathrm{cyc}}/F)$ are the quantities that appear in Iwasawa's formula.

Analogue of Iwasawa asymptotic formula for K-groups

Theorem (Coates 1972, Ji-Qin 2013)

Let $i \geq 2$. Suppose that the number field F contains a primitive pth root of unity and F^{cyc} is the cyclotomic $\mathbb{Z}_p$-extension of F. Then one has that

$$\log_p \left| K_{2i-2}(\mathcal{O}_{F_n})[p^\infty] \right| = \mu(F^{\mathrm{cyc}}/F)p^n + \lambda(F^{\mathrm{cyc}}/F)n + O(1),$$

where $\mu(F^{\mathrm{cyc}}/F)$ and $\lambda(F^{\mathrm{cyc}}/F)$ are the quantities that appear in Iwasawa's formula.

We like to extend the result of Coates and Ji-Qin to more general p-adic Lie extensions which do not contain the cyclotomic $\mathbb{Z}_p$-extension.

Quillen-Lichtenbaum conjecture

There is a connection between the higher K-groups with Galois/étale cohomology via the p-adic Chern class maps of Soulé

$$\mathrm{ch}_{i,k}^{(p)} : K_{2i-k}(\mathcal{O}_F) \otimes \mathbb{Z}_p \longrightarrow H^k\left(G_{S_p}(F), \mathbb{Z}_p(i)\right)$$

for $i \geq 2$ and $k = 1, 2$. (The existence of such a map was previously conjectured by Quillen.) The famed Quillen-Lichtenbaum Conjecture predicts that these maps are isomorphisms which **we now know is a theorem** by the works of Rost-Voevodsky.

Consequently, we have

$$K_{2i-2}(\mathcal{O}_F)[p^\infty] \cong H^2\left(G_{S_p}(F), \mathbb{Z}_p(i)\right).$$

In fact, one even has

$$K_{2i-2}(\mathcal{O}_{F,S})[p^\infty] \cong H^2\left(G_S(F), \mathbb{Z}_p(i)\right),$$

where S is a finite set of primes of F containing S_p.

Iwasawa cohomology groups

Let F_∞ be a uniform p-adic Lie extension of F contained in F_S. One can define the Iwasawa cohomology groups

$$H^2_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p(i)) := \varprojlim_L H^2(G_S(L), \mathbb{Z}_p(i)),$$

where L runs through all finite extension of F contained in F_∞ and the transition maps are given by the corestriction maps.

Iwasawa cohomology groups

Let F_∞ be a uniform p-adic Lie extension of F contained in F_S. One can define the Iwasawa cohomology groups

$$H^2_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p(i)) := \varprojlim_L H^2(G_S(L), \mathbb{Z}_p(i)),$$

where L runs through all finite extension of F contained in F_∞ and the transition maps are given by the corestriction maps.

Theorem (L. $\geq$ 22)

For $i \geq 2$, $H^2_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p(i))$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module, where $G = \mathrm{Gal}(F_\infty/F)$.

Descent of Iwasawa cohomology groups

Theorem (Nekovar 05, Fukaya-Kato 05, L-Sharifi 13)

Let L be a finite Galois extension of F contained in F_∞ and write $G_L = \mathrm{Gal}(F_\infty/L)$. Then we have a homological spectral sequence

$$H_r\left(G_L, H^{-s}_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p(i))\right) \Longrightarrow H^{-r-s}_{\mathrm{Iw},S}\left(L_\infty/F, \mathbb{Z}_p(i)\right).$$

By considering the initial $(0,-2)$-term, we have an isomorphism

$$H^2_{\mathrm{Iw},S}\left(F_\infty/F, \mathbb{Z}_p(i)\right)_{G_L} \cong H^2_{\mathrm{Iw},S}\left(G_S(L), \mathbb{Z}_p(i)\right).$$

The above is an Iwasawa-theoretical version of the Tate spectral sequence which is proven by Nekovar (for commutative G), Fukaya-Kato and Lim-Sharifi (for noncommutative G).

Even K-groups

Therefore, the algebraic results apply quite seamlessly for the even K-groups. We just require some slight further argument.

Even K-groups

Therefore, the algebraic results apply quite seamlessly for the even K-groups. We just require some slight further argument.

Suppose that $S \supseteq S_p$. The localization sequence of Soulé gives

$$0 \longrightarrow K_{2i-2}(\mathcal{O}_F)[p^\infty] \longrightarrow K_{2i-2}(\mathcal{O}_{F,S})[p^\infty] \longrightarrow \bigoplus_{v \in S - S_p} K_{2i-1}(k_v)[p^\infty] \longrightarrow 0,$$

where k_v is the residue field of F_v.

It remains to estimate the local term $K_{2i-1}(k_v)[p^\infty]$.

Even K-groups

Theorem (Quillen 1972)

Let $\mathbb{F}$ be a finite field. Then one has

$$K_{2i-1}(\mathbb{F}) = \mathbb{Z}/(|\mathbb{F}|^i - 1)\mathbb{Z}.$$

Even K-groups

Theorem (Quillen 1972)

Let $\mathbb{F}$ be a finite field. Then one has

$$K_{2i-1}(\mathbb{F}) = \mathbb{Z}/(|\mathbb{F}|^i - 1)\mathbb{Z}.$$

Now, if k_∞ is a $\mathbb{Z}_p$-extension of a finite field k, we have

$$\mathrm{ord}_p(|k_n|^i - 1) = O(n),$$

where k_n is the intermediate subfield of k_∞/k with $|k_n : k| = p^n$.

A combination of the above analysis will yield asymptotic formula for $K_{2i-2}(\mathcal{O}_{F_n})[p^\infty]$.

One may also obtain similar asymptotic formula for $K_{2i-2}(\mathcal{O}_{F_n,S})[p^\infty]$.

p-primary Selmer groups

Let A be an abelian variety defined over F. The classical p-primary Selmer group is defined by

$$\mathrm{Sel}(A/F) := \mathrm{Sel}_{p^\infty}(E/F) := \mathrm{Sel}(A[p^\infty]/\mathbb{Q})$$

$$= \ker\left(H^1(\mathrm{Gal}(\bar{F}/F), A[p^\infty]) \longrightarrow \prod_v H^1(\mathrm{Gal}(\bar{F}_v/F_v), A)[p^\infty]\right)$$

p-primary Selmer groups

Let A be an abelian variety defined over F. The classical p-primary Selmer group is defined by

$$\mathrm{Sel}(A/F) := \mathrm{Sel}_{p^\infty}(E/F) := \mathrm{Sel}(A[p^\infty]/\mathbb{Q})$$

$$= \ker\left(H^1(\mathrm{Gal}(\bar{F}/F), A[p^\infty]) \longrightarrow \prod_v H^1(\mathrm{Gal}(\bar{F}_v/F_v), A)[p^\infty]\right)$$

This fits into the following short exact sequence

$$0 \longrightarrow E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_{p^\infty}(A/F) \longrightarrow Ш(A/F)[p^\infty] \longrightarrow 0.$$

Morally, one expects $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/F) = \mathrm{rank}_{\mathbb{Z}} A(F)$ in view of the conjectural finiteness of Ш.

Ш growth in $\mathbb{Z}_p$-extension: p-ordinary case

Theorem (Mazur 72, Greenberg 99, Lee 20)

Let F_∞ be a $\mathbb{Z}_p$-extension of F. Suppose that A is an abelian variety defined over F with good ordinary reduction at all primes above p. Assume that $Ш(A/F_n)[p^\infty]$ is finite for every n. Then one has

$$\log_p \left| Ш(A/F_n)[p^\infty] \right| = \mu p^n + \lambda n + O(1)$$

for some μ, λ.

Remark: The torsionness of $\mathrm{Sel}(A/F_\infty)^\vee$ is not required in the above theorem. In particular, the above theorem also applies in the "indefinite" anticyclotomic $\mathbb{Z}_p$-extension context.

Mazur Control Theorem

Theorem (Mazur 72)

Let F_∞ be a $\mathbb{Z}_p$-extension of F. Suppose that A is an abelian variety defined over F with good ordinary reduction at all primes above p. Then the restriction maps

$$\mathrm{Sel}(A/F_n) \longrightarrow \mathrm{Sel}(A/F_\infty)^{\Gamma_n}$$

are finite with bounded kernel and cokernel.

Mazur Control Theorem

Theorem (Mazur 72)

Let F_∞ be a $\mathbb{Z}_p$-extension of F. Suppose that A is an abelian variety defined over F with good ordinary reduction at all primes above p. Then the restriction maps

$$\mathrm{Sel}(A/F_n) \longrightarrow \mathrm{Sel}(A/F_\infty)^{\Gamma_n}$$

are finite with bounded kernel and cokernel.

Remark: However, we do not have a control theorem for $\text{Ш}(A/F_n)$!

Idea of proof: p-ordinary case

Write $X(A/F_n) = \mathrm{Sel}(A/F_n)^\vee$ for $0 \leq n \leq \infty$.

Module theoretical result ("algebraic aspect") tells us that

$$\log_p \left| X(A/F_\infty)_{\Gamma_n}[p^\infty] \right| = \mu p^n + \lambda n + O(1).$$

Idea of proof: p-ordinary case

Write $X(A/F_n) = \mathrm{Sel}(A/F_n)^\vee$ for $0 \le n \le \infty$.

Module theoretical result ("algebraic aspect") tells us that

$$\log_p \left| X(A/F_\infty)_{\Gamma_n}[p^\infty] \right| = \mu p^n + \lambda n + O(1).$$

Mazur Control Theorem then in turn tells us that

$$\log_p \left| X(A/F_n)[p^\infty] \right| = \mu p^n + \lambda n + O(1).$$

Idea of proof: p-ordinary case

Write $X(A/F_n) = \mathrm{Sel}(A/F_n)^\vee$ for $0 \le n \le \infty$.

Module theoretical result ("algebraic aspect") tells us that

$$\log_p \left| X(A/F_\infty)_{\Gamma_n}[p^\infty] \right| = \mu p^n + \lambda n + O(1).$$

Mazur Control Theorem then in turn tells us that

$$\log_p \left| X(A/F_n)[p^\infty] \right| = \mu p^n + \lambda n + O(1).$$

The latter then yields the conclusion for Ш in view of the following short exact sequence

$$0 \longrightarrow Ш(A/F_n)^\vee \longrightarrow X(A/F_n) \longrightarrow \left(A(F_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee \longrightarrow 0.$$

Sha in p-adic Lie extension

At present, we do not have asymptotic formula for Ш in p-adic Lie extension.

But we should note that Delbourgo-Lei have obtained asymptotic upper bound for certain class of p-adic Lie extensions under a so-called $\mathfrak{M}_H(G)$-conjecture.

Even for $\mathbb{Z}_p^d$-extension, this is an issue because Cocuo-Monsky's result requires $\mathrm{rank}_{\mathbb{Z}_p} M_{G_n} = O(p^{(d-2)n})$.

Fine Selmer groups

The fine Selmer group is defined by

$$R(A/F) := R_{p^\infty}(A/F)$$

$$= \ker\left(H^1(\mathrm{Gal}(\bar{F}/F), A[p^\infty]) \longrightarrow \prod_v H^1(\mathrm{Gal}(\bar{F}_v/F_v), A[p^\infty])\right)$$

The fine Mordell-Weil group $\mathcal{M}(A/L)$ is defined by

$$\mathcal{M}(A/F) = \ker\left(A(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \bigoplus_{v|p} A(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)$$

Fine Tate-Sha groups

These fit into the following commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathcal{M}(A/F) & \longrightarrow & A(F)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & \bigoplus_{v|p} A(F_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \\
 & & \downarrow & & \downarrow & & \| \\
0 & \longrightarrow & R(A/F) & \longrightarrow & \mathrm{Sel}(A/F) & \longrightarrow & \bigoplus_{v|p} A(F_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p
\end{array}$$

Fine Tate-Sha groups

These fit into the following commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathcal{M}(A/F) & \longrightarrow & A(F)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & \bigoplus_{v|p} A(F_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \\
 & & \downarrow & & \downarrow & & \| \\
0 & \longrightarrow & R(A/F) & \longrightarrow & \mathrm{Sel}(A/F) & \longrightarrow & \bigoplus_{v|p} A(F_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p
\end{array}$$

The fine Tate-Shafarevich group $Ж(A/F)$ is then defined to be

$$Ж(A/F) = \mathrm{coker}\Big(\mathcal{M}(A/F) \longrightarrow R(A/F)\Big).$$

Applying the snake lemma, we obtain a short exact sequence

$$0 \longrightarrow \mathcal{M}(A/F) \longrightarrow R(A/F) \longrightarrow Ж(A/F) \longrightarrow 0$$

with $Ж(A/F)$ injecting into $Ш(A/F)[p^\infty]$.

Control Theorem for fine Selmer groups

Theorem (L. 20)

Let F_∞ be a $\mathbb{Z}_p$-extension of F. Suppose that A is an abelian variety defined over F. Then the restriction maps

$$R(A/F_n) \longrightarrow R(A/F_\infty)^{\Gamma_n}$$

are finite with bounded kernel and cokernel.

Control Theorem for fine Selmer groups

Theorem (L. 20)

Let F_∞ be a $\mathbb{Z}_p$-extension of F. Suppose that A is an abelian variety defined over F. Then the restriction maps

$$R(A/F_n) \longrightarrow R(A/F_\infty)^{\Gamma_n}$$

are finite with bounded kernel and cokernel.

Remark: The above control theorem does not require any reduction type assumption of A.

Some side remarks

Corollary (L. 20)

Let F_∞ be a $\mathbb{Z}_p$-extension of F. Suppose that A is an abelian variety defined over F. Assume that $Ш(A/F_n)$ is finite for all n. Then $Ш(A/F_\infty)^\vee$ is a torsion $\mathbb{Z}_p[\![\Gamma]\!]$-module.

Some side remarks

Corollary (L. 20)

Let F_∞ be a $\mathbb{Z}_p$-extension of F. Suppose that A is an abelian variety defined over F. Assume that $\text{Ж}(A/F_n)$ is finite for all n. Then $\text{Ж}(A/F_\infty)^\vee$ is a torsion $\mathbb{Z}_p[\![\Gamma]\!]$-module.

Remark: (1) We have no control theorem for Ж.

(2) The analogue statement for Ш is of course false in general! For instance, $\text{Ш}(E/\mathbb{Q}^{\mathrm{cyc}})[p^\infty]^\vee$ is not torsion if E has good supersingular reduction.

Towards an asymptotic formula for fine Tate-Sha

Write $Y(A/F_n) = R(A/F_n)^\vee$ for $0 \leq n \leq \infty$.

Module theoretical result ("algebraic aspect") tells us that

$$\log_p \left| Y(A/F_\infty)_{\Gamma_n}[p^\infty] \right| = \mu p^n + \lambda n + O(1).$$

Towards an asymptotic formula for fine Tate-Sha

Write $Y(A/F_n) = R(A/F_n)^\vee$ for $0 \le n \le \infty$.

Module theoretical result ("algebraic aspect") tells us that

$$\log_p \left| Y(A/F_\infty)_{\Gamma_n}[p^\infty] \right| = \mu p^n + \lambda n + O(1).$$

Control Theorem of fine Selmer groups then in turn tells us that

$$\log_p \left| Y(A/F_n)[p^\infty] \right| = \mu p^n + \lambda n + O(1).$$

Towards an asymptotic formula for fine Tate-Sha

Write $Y(A/F_n) = R(A/F_n)^\vee$ for $0 \leq n \leq \infty$.

Module theoretical result ("algebraic aspect") tells us that

$$\log_p \left| Y(A/F_\infty)_{\Gamma_n}[p^\infty] \right| = \mu p^n + \lambda n + O(1).$$

Control Theorem of fine Selmer groups then in turn tells us that

$$\log_p \left| Y(A/F_n)[p^\infty] \right| = \mu p^n + \lambda n + O(1).$$

But in the following short exact sequence

$$0 \longrightarrow Ш(A/F_n)^\vee \longrightarrow Y(A/F_n) \longrightarrow \left(\mathcal{M}(A/F_n)\right)^\vee \longrightarrow 0,$$

the fine Mordell-Weil group $\left(\mathcal{M}(A/F_n)\right)^\vee$ may have p-torsion. (Wuthrich has given examples of these.)

Growth for fine Tate-Sha

Theorem (L. 20)

Let F_∞ be a $\mathbb{Z}_p$-extension of F. Suppose that A is an abelian variety defined over F. Assume that either of the following statement holds.

(a) $A(F_\infty)$ is a finitely generated abelian group and $Ш\!\!К(A/F_n)$ is finite for all n.

(b) A has potentially good ordinary reduction at all primes above p and $Ш(A/F_n)[p^\infty]$ is finite for all n.

Then we have

$$\log_p \left| Ш\!\!К(A/F_n) \right| = \mu p^n + \lambda n + O(1).$$

Remark: Under assumption (b), we show that the fine Mordell-Weil group $\mathcal{M}(A/F_n)$ has control theorem.

Fine Selmer groups over p-adic Lie extensions

It is natural to ask if one can study growth formula for $\text{Ж}(A/F_n)$ in p-adic Lie extension.

Fine Selmer groups over p-adic Lie extensions

It is natural to ask if one can study growth formula for $Ж(A/F_n)$ in p-adic Lie extension.

In a recent work of Debanjana Kundu and myself, we prove control theorems for fine Selmer groups over certain classes of p-adic Lie extension. Our results can be thought as "effective" version of Greenberg.

We are not able to obtain results for $Ж$. The reason is because the "nice" structure of $\mathbb{Z}_p[[\Gamma]]$ is crucially used in the derivation of the $Ж$ in the previous slide.

Growth for Tate-Sha: p-supersingular case

Growth for Tate-Sha: p-supersingular case

Theorem (Kurihara 02, Kobayashi 03)

Let E be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at $p \geq 5$. Assume that $\text{Ш}(E/\mathbb{Q}_n)[p^\infty]$ is finite for all n, where $\mathbb{Q}_n$ is the intermediate subextension of $\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}$ with $|\mathbb{Q}_n : \mathbb{Q}| = p^n$. Then one has

$$\log_p \left|\text{Ш}(E/\mathbb{Q}_n)[p^\infty]\right| = \sum_{k=0}^{\lfloor \frac{n-2}{2} \rfloor} p^{n-1-2k} - \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor \lambda_E^+ + \left\lfloor \frac{n+1}{2} \right\rfloor \lambda_E^-$$

$$-nr_\infty + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \phi(p^{2k})\mu_E^+ + \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} \phi(p^{2k-1})\mu_E^- + \nu_E,$$

where ϕ is the Euler totient function and r_∞ is given by the quantity

$$\lim_{m\to\infty} \operatorname{rank} E(\mathbb{Q}_m).$$

Growth for Tate-Sha: p-supersingular case

Remark: The invariants $\mu_E^{\pm}$ and $\lambda_E^{\pm}$ come from the signed Selmer groups $\mathrm{Sel}^{\pm}(E/\mathbb{Q}^{\mathrm{cyc}})$. Conjecturally, one expects $\mu_E^{\pm} = 0$.

An important algebraic tool is the notion of Kobayashi rank.

Iovita-Pollack (06) have extended Kobayashi's result to a general ramified $\mathbb{Z}_p$-extension F_∞ with $\mathrm{rank}_{\mathbb{Z}}\left(E(F_n)\right)$ bounded.

However, their approach does not apply to the "indefinite" anticyclotomic setting.

Growth for Tate-Sha: indefinite anti-cyclotomic context

Theorem (Lei-L-Müller, preprint 2022)

Let E be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at $p \geq 5$. Let K be an imaginary quadratic field at which p split completely in $K/\mathbb{Q}$. Suppose the conductor of E is given by MD, where D is a square-free product of an even number of primes. Assume that all primes dividing pM split in K, whereas those dividing D are inert in K. Assume that $Ш(E/K_n)[p^\infty]$ is finite for all n, where K_n is the intermediate subextension of $K^{\mathrm{anti-cyc}}/K$ with $|K_n : K| = p^n$. Then one has

$$\log_p \left| Ш(E/K_n)[p^\infty] \right| = \sum_{k \leq m, k \text{ even}} \mu^+_{E,K} \phi(p^k) + \sum_{k \leq m, k \text{ odd}} \mu^-_{E,K} \phi(p^k) + \left\lfloor \frac{m}{2} \right\rfloor \lambda^+_{E,K} + \left\lfloor \frac{m+1}{2} \right\rfloor \lambda^-_{E,K} + \nu_{E,K}$$

Final remark on the invariants

The invariants appearing have the following form

$$\mu^{\pm}_{E,K} = \mu^{\mathrm{BDP}} - 2\mu^{\pm}, \quad \lambda^{\pm}_{E,K} = \lambda^{\mathrm{BDP}} - \lambda' - 2\lambda^{\pm}.$$

Here μ^{BDP} and λ^{BDP} are the Iwasawa invariants of $\mathrm{Sel}^{\mathrm{BDP}}(E/K_\infty)$.

(Remark: One expects $\mu^{\mathrm{BDP}} = 0$ in view of analytical results of Hsieh 14 and Burungale 17.)

$\lambda' = \lim_{n\to\infty} \mathrm{rank}_{\mathbb{Z}_p} \mathrm{Sel}^{\mathrm{BDP}}(E/K_n)^\vee$.

$\mu^{\pm}$ and $\lambda^{\pm}$ comes from "plus" and "minus" parts of $\ker \psi_n$, where

$$\psi_n : E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow E(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

Here v is a prime of K above p.

THE END

THANK YOU!