Mathematical Proceedings of the Cambridge Philosophical Society

VOL. 142 JANUARY 2007 PART 1

Math. Proc. Camb. Phil. Soc. (2007), **142**, 1 © 2007 *Cambridge Philosophical Society*
doi:10.1017/S0305004106009662 *Printed in the United Kingdom*

The fine Tate–Shafarevich group

BY CHRISTIAN WUTHRICH

Séction de mathématiques, CSAG, École Polytechnique Fédérale,
1015 *Lausanne, Switzerland.*

(*Received* 3 *June* 2005; *revised* 20 *October* 2005)

Abstract

Within the Tate–Shafarevich group of an elliptic curve E defined over a number field K, there is a canonical subgroup defined by imposing stronger conditions at the places above a given prime p. This group appears naturally in the Iwasawa theory for E. We propose a study of what one can say about the relation to the full Tate–Shafarevich group. Some numerical examples are included, as well as a few conjectures.

1. *Introduction*

Let E be an elliptic curve defined over a number field K. We fix a prime number p. Everything will depend on p, but we will omit it from our notations. For an abelian group A, the p-primary part of A will be denoted by $A(p)$. The p-primary part of the Tate–Shafarevich group $Ш(E/K)(p)$ is defined to be the kernel of the localisation map

$$0 \longrightarrow Ш(E/K)(p) \longrightarrow H^1(K, E)(p) \longrightarrow \oplus_v H^1(K_v, E)(p).$$

We will define in Section 2 a certain canonical subgroup of $Ш(E/K)(p)$ by imposing stronger conditions at the places above p. It will be called the fine Tate–Shafarevich group, denoted by another Russian letter $Ш(E/K)$. It is actually defined as the union of a sequence of subgroups $Ш^k(E/K)$ in $Ш(E/K)[p^k]$ and it represents the "Tate–Shafarevich part" of the fine Selmer group $\mathcal{R}(E/K)$ as defined in [**CS05**]. See Section 2 for the details.

The motivation for studying this group comes from the Iwasawa theory of E. Its behaviour is closely linked to Euler systems for the Tate-module $T_pE = \varprojlim E[p^k]$, like the one by Kato [**Kat04**]. Suppose E is defined over $\mathbb{Q}$. If the L-series of E does not vanish at 1, then Kato's Euler system $\mathbf{c}$ is such that $\mathbf{c}_{\mathbb{Q}} \in H^1(\mathbb{Q}, T_pE)$ is not torsion. By [**Rub00**, theorem 2·2·3], the fine Selmer group $\mathcal{R}(E/\mathbb{Q})$, which is then equal to $Ш(E/\mathbb{Q})$, is

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

finite. Moreover the divisibility of $\mathbf{c}_{\mathbb{Q}}$ by p may be used to give an upper bound on the size of $Ш(E/\mathbb{Q})$.

For more details on the Iwasawa theory of the fine Selmer group, we refer the reader to [**Wut04**], [**Wut05**] and [**PR95**].

This paper focuses on the analysis of the fine Tate–Shafarevich group over the number field K. The first part concerns its relation to the full Tate–Shafarevich group. For $K = \mathbb{Q}$, we prove in Theorem 3·4 that $Ш(E/\mathbb{Q})$ is non-trivial exactly if $Ш(E/\mathbb{Q})$ is non-trivial, and that they are equal if the rank of the curve is positive (see Theorem 3·5). Numerical examples are given in Section 4 for curves of rank 0 and $p = 2$. We find three examples of curves E defined over $\mathbb{Q}$ with $Ш(E/\mathbb{Q})(2) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ which show that all possible orders (namely 1, 2 or 4) can occur for $Ш^1(E/\mathbb{Q})$. The fine Tate–Shafarevich groups $Ш(E/\mathbb{Q})$ have order 2, for the first two curves, and 4 for the last example.

We present a version of the Cassels–Tate pairing due to Flach [**Fla90**] for our subgroup $Ш(E/K)$ in Section 6. Then the fine version of the Mordell–Weil group $E(K)$, also obtained by imposing conditions at the places above p, is considered. We end the article with some conjectures on the fine Tate–Shafarevich group $Ш(E/K)$. In contrast to the situation over $\mathbb{Q}$, it is not true for larger fields that the fine subgroup of the Tate–Shafarevich group is often relatively big. In fact, for $\mathbb{Z}_p$-extensions it is conjectured that the growth of the fine Tate–Shafarevich group is significantly smaller.

2. *Definitions*

For any $k \geqslant 1$, we have a short exact sequence coming from the p^k-descent

$$0 \longrightarrow E(K)/p^k E(K) \xrightarrow{\kappa} S^k(E/K) \longrightarrow Ш(E/K)[p^k] \longrightarrow 0 \qquad (2\cdot1)$$

where $S^k(E/K)$ is the Selmer group defined as the kernel of the map

$$H^1(K, E[p^k]) \longrightarrow \bigoplus_{\upsilon} H^1(K_\upsilon, E)[p^k]$$

with the sum running over all places υ in K. This Selmer group contains a subgroup $R^k(E/K)$, which we will call the *fine Selmer group*, obtained by imposing stronger conditions at the places above p, i.e. the sequence

$$0 \longrightarrow R^k(E/K) \longrightarrow S^k(E/K) \longrightarrow \bigoplus_{\upsilon|p} H^1(K_\upsilon, E[p^k])$$

is exact. The subgroup $R^k(E/K)$ is sometimes called the "strict" or "restricted" Selmer group, but in order to avoid possible confusions with different definitions, we prefer the terminology in [**CS05**]. Similarly we can define a fine subgroup of the Mordell–Weil group. Namely the following kernel

$$0 \longrightarrow M^k(E/K) \longrightarrow E(K)/p^k E(K) \longrightarrow \bigoplus_{\upsilon|p} E(K_\upsilon)/p^k E(K_\upsilon), \qquad (2\cdot2)$$

which can also be written as the intersection of $R^k(E/K)$ with the image of the Kummer map κ in (2·1) inside $S^k(E/K)$.

Now, we can proceed to define the group $Ш^k(E/K)$ as the quotient of $R^k(E/K)$ by $M^k(E/K)$. We call it the *fine Tate–Shafarevich group*. So we have an exact sequence

$$0 \longrightarrow M^k(E/K) \xrightarrow{\kappa} R^k(E/K) \longrightarrow Ш^k(E/K) \longrightarrow 0 \qquad (2\cdot3)$$

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

similar to the Kummer sequence (2·1). In order to prove that it is really a subgroup of the Tate–Shafarevich group, we consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/p^kE(K) & \longrightarrow & S^k(E/K) & \longrightarrow & Ш(E/K)[p^k] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow 0 & & \\ 0 & \longrightarrow & \oplus E(K_\upsilon)/p^kE(K_\upsilon) & \longrightarrow & \oplus H^1(K_\upsilon, E[p^k]) & \longrightarrow & \oplus H^1(K_\upsilon, E)[p^k] & \longrightarrow & 0 \end{array}$$

(the $\oplus$ stands for the sum over all places υ above p). We can extract an exact sequence

$$0 \longrightarrow M^k(E/K) \longrightarrow R^k(E/K) \longrightarrow Ш(E/K)[p^k] \xrightarrow{\delta^k} C^k \tag{2·4}$$

where C^k is the cokernel of the left vertical map in the above diagram. As a consequence, one can view $Ш^k(E/K)$ as a subgroup of $Ш(E/K)[p^k]$ with quotient inside C^k.

Limits

As usual, it is interesting to consider the limits as k tends to infinity. We write $\mathcal{S}(E/K)$ for the inductive limit $\varinjlim S^k(E/K)$ obtained from the inclusion $E[p^k] \hookrightarrow E[p^{k+1}]$. We denote the projective limit $\varprojlim S^k(E/K)$ induced from the map $[p]\colon E[p^{k+1}] \twoheadrightarrow E[p^k]$ by $\mathcal{S}(E/K)$. The same limits can be used for the subgroups $R^k(E/K)$ and $M^k(E/K)$.

$$\begin{aligned} \mathcal{S}(E/K) &= \varinjlim S^k(E/K) & \mathcal{S}(E/K) &= \varprojlim S^k(E/K) \\ \mathcal{R}(E/K) &= \varinjlim R^k(E/K) & \mathcal{R}(E/K) &= \varprojlim R^k(E/K) \\ \mathcal{M}(E/K) &= \varinjlim M^k(E/K) & \mathcal{M}(E/K) &= \varprojlim M^k(E/K). \end{aligned}$$

For the fine Tate–Shafarevich group, we will denote the limit $\varinjlim Ш^k(E/K)$ simply by $Ш(E/K)$. It is a subgroup of the p-primary part $Ш(E/K)(p)$ of the Tate–Shafarevich group. We have two exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{M}(E/K) & \longrightarrow & \mathcal{R}(E/K) & \longrightarrow & Ш(E/K) & \longrightarrow & 0 \\ 0 & \longrightarrow & \mathcal{M}(E/K) & \longrightarrow & \mathcal{R}(E/K) & \longrightarrow & \varprojlim Ш^k(E/K) & \longrightarrow & 0 \end{array}$$

since all terms in (2·3) are finite. Both $\varprojlim Ш^k(E/K)$ and $T_pШ(E/K) = \varprojlim Ш[p^k]$ are subgroups of $T_pШ(E/K)$, where, for an abelian group A, we write T_pA for the projective limit $\varprojlim A[p^k]$. Of course, it is widely believed that these three groups are trivial. One can show that.

LEMMA 2·1. *The group* $\varprojlim Ш^k(E/K)$ *has finite index in* $T_pШ(E/K)$.

A proof can be found in [**Wut04**, lemma II·1].

LEMMA 2·2. *The maps*

$$Ш^1(E/K) \longrightarrow Ш^2(E/K) \longrightarrow \cdots$$

are injective.

Proof. This is obvious from the following diagram. Here C^k is as in (2·4).

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Ш^k(E/K) & \longrightarrow & Ш(E/K)[p^k] & \xrightarrow{\delta^k} & C^k \\ & & \downarrow & & \downarrow \cap & & \downarrow \\ 0 & \longrightarrow & Ш^{k+1}(E/K) & \longrightarrow & Ш(E/K)[p^{k+1}] & \xrightarrow{\delta^{k+1}} & C^{k+1} \end{array} \tag{2·5}$$

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

where the map on the right-hand side is induced by the maps

$$[p]\colon E(K_\upsilon)/p^kE(K_\upsilon) \longrightarrow E(K_\upsilon)/p^{k+1}E(K_\upsilon).$$

The following lemma tells us in some cases when the above sequence stabilises.

LEMMA 2·3. *Let E be an elliptic curve over $\mathbb{Q}$ of rank 0 with $E(\mathbb{Q}_p)[p] = 0$. If p^k kills all elements in $Ш(E/\mathbb{Q})(p)$, then*

$$\text{Ж}^k(E/\mathbb{Q}) = \text{Ж}(E/\mathbb{Q}).$$

Proof. Under the hypothesis on k, the map in the middle of (2·5) becomes an isomorphism. Because $E(\mathbb{Q})/p^kE(\mathbb{Q}) = 0$, the group C^k is equal to $E(\mathbb{Q}_p)/p^kE(\mathbb{Q}_p)$. Hence the map induced by $[p]$ on $C^k \to C^{k+1}$ is injective if $E(\mathbb{Q}_p)[p] = 0$.

Even with weaker assumptions, it is usually easy to verify for which k the sequence of $\text{Ж}^k(E/K)$ stabilises.

Remark. Instead of imposing stronger conditions only at places above p, we could more generally consider a finite set Σ of places in K, containing the places above p, and then demand that elements in $S^k(E/K)$ have trivial localisation in the group $H^1(K_\upsilon, E[p^k])$ for all places in Σ. We would obtain even smaller subgroups $R^k_\Sigma(E/K)$ and $\text{Ж}^k_\Sigma(E/K)$. Note that $\mathcal{R}_\Sigma(E/K) = \varinjlim R^k_\Sigma(E/K)$ does not differ from $\mathcal{R}(E/K)$ because the groups $E(K_\upsilon) \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}$ are trivial for all places $\upsilon \nmid p$.

3. *Comparison*

LEMMA 3·1. *Let K_υ be a finite extension of $\mathbb{Q}_p$ of degree n_υ. Then*

$$\#\left(E(K_\upsilon)/p^kE(K_\upsilon)\right) = p^{n_\upsilon \cdot k} \cdot \#\left(E(K_\upsilon)[p^k]\right).$$

Proof. Note that, if A is a subgroup of an abelian group B of finite index, then

$$\frac{\#A/p^kA}{\#A[p^k]} = \frac{\#B/p^kB}{\#B[p^k]},$$

provided all terms are well-defined. Denote by $E^\circ(K_\upsilon)$ the K_υ-rational points on the connected component of the Néron-model of E and by $\widehat{E}$ the formal group associated to E (see [**Sil96**]). Since $E(K_\upsilon)$ has finite index in $E^\circ(K_\upsilon)$ and in $\widehat{E}(\mathfrak{m}_\upsilon^a)$, for any power of the maximal ideal $\mathfrak{m}_\upsilon$ in the ring of integers in K_υ, we obtain that

$$\begin{aligned}\frac{\#E(K_\upsilon)/p^kE(K_\upsilon)}{\#E(K_\upsilon)[p^k]} &= \frac{\#E^\circ(K_\upsilon)/p^kE(K_\upsilon)}{\#E^\circ(K_\upsilon)[p^k]} = \frac{\#\widehat{E}(\mathfrak{m}_\upsilon)/p^k\widehat{E}(\mathfrak{m}_\upsilon)}{\#\widehat{E}(\mathfrak{m}_\upsilon)[p^k]} \\ &= \frac{\#\widehat{E}(\mathfrak{m}_\upsilon^a)/p^k\widehat{E}(\mathfrak{m}_\upsilon^a)}{\#\widehat{E}(\mathfrak{m}_\upsilon^a)[p^k]}.\end{aligned}$$

Now, if a is large enough, the formal logarithm gives an isomorphism from $\widehat{E}(\mathfrak{m}_\upsilon^a)$ to $\mathfrak{m}_\upsilon^a$ and we have $\widehat{E}(\mathfrak{m}_\upsilon^a)[p^k] = 0$ and $\#\widehat{E}(\mathfrak{m}_\upsilon^a)/p^k\widehat{E}(\mathfrak{m}_\upsilon^a) = p^{kn_\upsilon}$.

PROPOSITION 3·2. *The index of $\text{Ж}^k(E/K)$ inside $Ш(E/K)[p^k]$ is bounded by*

$$[Ш(E/K)[p^k] : \text{Ж}^k(E/K)] \leqslant p^{[K:\mathbb{Q}]\cdot k} \cdot \prod_{\upsilon|p} \#E(K_\upsilon)[p^k].$$

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

Proof. We saw that the quotient of the two groups in question is contained in the cokernel C^k of the map from $E(K)/p^kE(K)$ to $\oplus E(K_v)/p^kE(K_v)$. The previous lemma proves that the target of this map has size bounded by the right-hand side of the formula in the proposition.

COROLLARY 3·3. *If E is defined over $\mathbb{Q}$ and $E(\mathbb{Q}_p)[p] = 0$, then*

$$\left[Ш(E/\mathbb{Q})[p] \,:\, \text{Ж}^1(E/\mathbb{Q})\right] \leqslant p.$$

THEOREM 3·4. *Let E be an elliptic curve defined over $\mathbb{Q}$. Suppose $Ш(E/\mathbb{Q})(p)$ is finite, then $\text{Ж}(E/\mathbb{Q})$ is non-trivial if and only if $Ш(E/\mathbb{Q})(p)$ is non-trivial.*

Proof. The injection of $\text{Ж}(E/\mathbb{Q})$ into $Ш(E/\mathbb{Q})(p)$ has cokernel in $C = \varinjlim C^k$ which is a quotient of $E(\mathbb{Q}_p) \otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$. But this last group is isomorphic to ${}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$. If $Ш(E/\mathbb{Q})(p)$ is finite and non-trivial, then it is of the form $A \oplus A$ for some abelian p-group A by the Cassels–Tate pairing. So $Ш(E/\mathbb{Q})(p)$ can not be embedded into ${}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$.

THEOREM 3·5. *Let E be an elliptic curve defined over $\mathbb{Q}$ of positive rank, then we have $\text{Ж}(E/\mathbb{Q}) = Ш(E/\mathbb{Q})(p)$.*

Proof. The group C in the proof of the previous theorem is the cokernel of the localisation map $E(\mathbb{Q}) \otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p} \twoheadrightarrow E(\mathbb{Q}_p) \otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$. The target of this map equals $\widehat{E}(p^2\mathbb{Z}_p) \otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$, which is isomorphic to ${}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$ via the p-adic elliptic logarithm map. If the rank of E is positive, the localisation map is non-trivial: a sufficiently large multiple of any point of infinite order in $E(\mathbb{Q})$ will belong to $\widehat{E}(p^2\mathbb{Z}_p)$ and has non-zero logarithm. Since $E(\mathbb{Q}_p) \otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$ is divisible the map has to be surjective and so $C = 0$.

If the rank is zero, $\text{Ж}(E/\mathbb{Q})$ may be strictly smaller than $Ш(E/\mathbb{Q})(p)$ as we will see in the numerical examples in the next section.

We see here that the fine Tate–Shafarevich group for an elliptic curve over $\mathbb{Q}$ tends to be rather large in comparison with the whole Tate–Shafarevich group. This is likely to be specific to $\mathbb{Q}$ as we will announce a conjecture for certain larger fields in Section 8.

4. *Numerical examples*

In this section we give four numerical examples of fine Tate–Shafarevich groups for $p = 2$. The four curves E are all defined over $\mathbb{Q}$. They all have rank 0, as can be verified using Kolyvagin's result or a 3-descent; in fact for each curve we have $E(\mathbb{Q}) = {}^{\mathbb{Z}}/_{2\mathbb{Z}} \oplus {}^{\mathbb{Z}}/_{2\mathbb{Z}}$. Then we perform a complete 2-descent on E as explained in [**Sil96**, proposition X·1·4].

The complete 2-descent proves for the first three examples that $Ш(E/\mathbb{Q})[2] = {}^{\mathbb{Z}}/_{2\mathbb{Z}} \oplus {}^{\mathbb{Z}}/_{2\mathbb{Z}}$. Hence the fine Tate–Shafarevich group $\text{Ж}^1(E/\mathbb{Q})$ can have 1, 2 or 4 elements. The examples are chosen as to show that all three cases can occur. Furthermore we can prove that the 2-primary part $Ш(E/\mathbb{Q})(2)$ has order 4 using a 4-descent or the Cassels-Tate pairing implemented in `magma`. So the fine Tate–Shafarevich group $\text{Ж}(E/\mathbb{Q})$ can have either 2 or 4 elements by Corollary 3·3.

The details of the computations are only included for the first example.

An example with a trivial $\text{Ж}^1(E/\mathbb{Q})$

Let $E/\mathbb{Q}$ be the elliptic curve O3 of conductor 930 in Cremona's table [**Cre97**]

$$E: \quad y^2 + xy = x^3 - 19'220\,x - 1'027'200.$$

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

The Mordell–Weil group $E(\mathbb{Q})$ is generated by two points $T_1 = (-80, 40)$ and $T_2 = (-321/4, 321/8)$ of order 2. The analytic order of $Ш(E/\mathbb{Q})$ is 4.

Let us change the equation to the non-minimal equation

$$y^2 = (x + 320) \cdot (x + 321) \cdot (x - 640)$$

in which T_1 has coordinates $(-320, 0)$ and T_2 is equal to $(-321, 0)$. Let Σ be the set $\{2, 3, 5, 31\}$ which includes all primes of bad reduction for E. The group $\mathbb{Q}(\Sigma, 2)$ is defined to be the group of non-zero integers only divisible by elements in Σ modulo squares; which in our case is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^5$. The above choice of a basis of $E(\mathbb{Q})[2]$ allows us to identify the Selmer group $S^1(E/\mathbb{Q})$ with a subgroup of the square of $\mathbb{Q}(\Sigma, 2)$. In fact, the image of T_1 is represented by $(-15, 1)$ while T_2 is sent to $(-1, 1)$ in $\mathbb{Q}(\Sigma, 2)^2$. One sees immediately that T_1 belongs to the fine Mordell-Weil group $M^1(E/\mathbb{Q})$ since both -15 and 1 are squares in $\mathbb{Q}_2^\times$, in other words there is a 4-torsion point

$$S_1 = (2^3 + 2^7 + 2^8 + \mathbf{O}(2^{10}), 2^3 + 2^8 + 2^9 + \mathbf{O}(2^{10}))$$

defined over $\mathbb{Q}_2$ such that $2 \cdot S_1 = T_1$.

Now the first Selmer group $S^1(E/\mathbb{Q})$ is generated by the image of T_1 and T_2 and the elements $(5, 1)$ and $(2, 1)$ in $\mathbb{Q}(\Sigma, 2)^2$. We can conclude that $R^1(E/\mathbb{Q})$ is equal to $(-15, 1) \cdot \mathbb{Z}/2\mathbb{Z} = M^1(E/\mathbb{Q})$, and hence that $Ш^1(E/\mathbb{Q})$ is trivial.

We now use the diagram (2·5) to compute the whole of $Ш(E/\mathbb{Q})$. We need to compute C^k first. Denote by $\Phi(E)(\mathbb{Q}_2)$ the group of connected components of the Néron-model over $\mathbb{Q}_2$. For our example $\Phi(E)(\mathbb{Q}_2)$ is a cyclic group of order 4; the reduction type is I_4. The torsion group of $E(\mathbb{Q}_2)$ is $\mathbb{Z}/4\mathbb{Z}\, S_1 \oplus \mathbb{Z}/2\mathbb{Z}\, T_2$. Since S_1 maps to the generator of $\Phi(E)(\mathbb{Q}_2)$, we know that $E(\mathbb{Q}_2) = E^\circ(\mathbb{Q}_2) \oplus \mathbb{Z}/4\mathbb{Z}\, S_1$ with E° being the connected component of the identity of the Néron model. The torsion point T_2 lies in the first layer of the formal group in the minimal model, and so we have $E(\mathbb{Q}_2) = \mathbb{Z}_2 \oplus \mathbb{Z}/4\mathbb{Z}\, S_1 \oplus \mathbb{Z}/2\mathbb{Z}\, T_2$. We conclude that C^k is isomorphic to $\mathbb{Z}/2^k\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\, S_1$. The map induced by [2] is the injection $\mathbb{Z}/2^k\mathbb{Z} \hookrightarrow \mathbb{Z}/2^{k+1}\mathbb{Z}$ on the first factor and the trivial map on the second:

$$\begin{array}{ccc} C^k & \longrightarrow & C^{k+1} \\ \mathbb{Z}/2^k\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} S_1 & \xrightarrow[(1,0)]{} & \mathbb{Z}/2^{k+1}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} S_1. \end{array}$$

The element $(5, 1)$ in $Ш(E/\mathbb{Q})[2]$ is mapped to the element $\delta^1(5, 1)$ in C^1 represented by

$$Q_1 = (2^{-2} + 1 + 2^6 + 2^7 + 2^9 + \mathbf{O}(2^{10}), 2^{-3} + 2 + 2^2 + 2^3 + 2^6 + 2^7 + 2^9 + \mathbf{O}(2^{10}))$$

which belongs to the first factor of $C^1 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\, S_1$. The image of the other generator $(2, 1)$ can be represented by S_1. Hence the first element of $Ш(E/\mathbb{Q})[2]$ always maps to a non-trivial element in C^k and does therefore not belong to $Ш^k(E/\mathbb{Q})$ for any k, while the latter element has trivial image in C^2 and thus belongs to $Ш^2(E/\mathbb{Q})$.

We can conclude the following:

$$Ш^1(E/\mathbb{Q}) = 0 \quad \text{and} \quad Ш^2(E/\mathbb{Q}) = Ш(E/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}.$$

A $Ш^1(E/\mathbb{Q})$ with 2 elements

Let E be the curve E5 of conductor 210

$$E: \quad y^2 + xy = x^3 - 120'050\, x - 16'020'000.$$

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

The Mordell–Weil group $E(\mathbb{Q})$ is generated by two points $T_1 = (400, -200)$ and $T_2 = (-801/4, 801/8)$ of order 2. A computation like for the first example shows that $M^1(E/\mathbb{Q}) = 0$ and that $R^1(E/\mathbb{Q}) = \text{Ш}^1(E/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. Using that $\text{Ш}(E/\mathbb{Q})(2)$ has 4 elements one shows that $\text{Ш}^k(E/\mathbb{Q}) = \text{Ш}(E/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ for all $k \geqslant 1$.

An example where $\text{Ш}^1(E/\mathbb{Q})$ has 4 elements

Let E be the elliptic curve

$$E: \quad y^2 + xy = x^3 - x^2 - 3'861\,x - 91'368.$$

It is labelled 1287E2 in the tables of Cremona. For this curve we have that $M^1(E/\mathbb{Q}) = 0$ and $R^1(E/\mathbb{Q}) = \text{Ш}^1(E/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} = \text{Ш}(E/\mathbb{Q})[2]$. Here we get $\text{Ш}(E/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

A bigger example

Finally, we include an example[1] of a larger Tate–Shafarevich group. The curve E

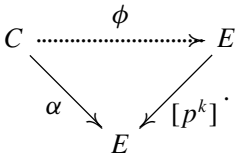
$$E: \quad y^2 + x\,y = x^3 - x^2 - 213'230'796\,x + 1'183'712'688'107$$

of conductor $3^2 \cdot 13^2 \cdot 17 \cdot 157^2$ is a twist of the curve $17A2$. The Mordell–Weil group has rank 0 and it has 4 rational 2-torsion points. The Birch and Swinnerton–Dyer conjecture predicts the order of $\text{Ш}(E/\mathbb{Q})$ to be 16.

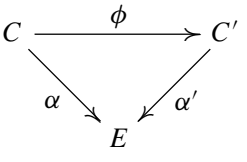
This time, we find that $S^1(E/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^6$ and so $\text{Ш}(E/\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^4$. It can be verified as before that the 2-primary part of $\text{Ш}(E/\mathbb{Q})$ consists of these 16 elements. The computation of the fine Selmer group shows that $R^1(E/\mathbb{Q}) = \text{Ш}^1(E/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^3$. The fine Tate–Shafarevich is equal to $\text{Ш}(E/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^3$.

5. *Geometric interpretation*

As usual, an element in the Selmer group and in the Tate–Shafarevich group may be interpreted geometrically in terms of torsors of E. Let F be an extension of K. An p^k-covering over F is a morphism of curves $\alpha: C \to E$ defined over F such that there is an isomorphism ϕ over $\bar{F}$ having the property that the following diagram commutes.



Note that C is a torsor of E. Two p^k-coverings α and α' are isomorphic if there is a ϕ defined over F such that



commutes. In particular, a p^k-covering α is isomorphic to the trivial p^k-covering given by $[p^k]: E \to E$ if and only if there is a point defined over F in the fibre of α above $O \in E(F)$.

[1] I am grateful to Christophe Delaunay for helping me to find this example.

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

It is well known that the elements of $H^1(F, E[p^k])$ can be represented in a unique way as isomorphism classes of p^k-coverings.

PROPOSITION 5·1. *The fine Selmer group $R^k(E/K)$ is in bijection with the pointed set of isomorphism classes of p^k-covering $\alpha: C \to E$ over K such that.*

(i) *$C(K_\upsilon)$ is non empty for all places υ in K, and,*
(ii) *for all places υ above p, there is a K_υ-rational point P_υ in the fibre $\alpha^{-1}(O)$ above $O \in E(K)$.*

The point P_υ is only defined up to addition by a K_υ-rational p^k-torsion point. For the fine Tate–Shafarevich group, we have the following description.

PROPOSITION 5·2. *The fine Tate–Shafarevich group $Ш^k(E/K)$ can be viewed as the pointed set of isomorphism classes of principal homogeneous spaces C under E defined over K such that*:

(i) *$C(K_\upsilon)$ is non empty for all places*;
(ii) *there is a K-rational effective divisor D of degree p^k on C; and*
(iii) *for all places υ above p, the divisor D contains a K_υ-rational point P_υ in its support.*

6. *Duality*

Cassels constructed a pairing on the Tate–Shafarevich group, whose kernel consists of the infinitely divisible elements. It follows that a finite Tate–Shafarevich group has square order. The construction of Cassels was extended by Flach in [**Fla90**]. In order to state the duality for the fine Selmer group, we need to define another generalised version of the Selmer group, namely the group $Ω(E/K)$ defined by the exact sequence

$$0 \longrightarrow Ω(E/K) \longrightarrow H^1(K, E(p)) \longrightarrow \prod_{\upsilon \nmid p} H^1(K_\upsilon, E)(p) \times \prod_{\upsilon | p} H^1(K_\upsilon, E(p))/\,\mathrm{div}.$$

Here we denote by $A/\,\mathrm{div}$ the quotient of A by its maximal divisible subgroup whenever A is a discrete abelian group. The enlarged Selmer group $Ω(E/K)$ contains the usual Selmer group $Ш(E/K)$. Let $Ч(E/K)(p)$ be the quotient of $Ω(E/K)$ by the image of $E(K) \otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$.

THEOREM 6·1. *There is a alternating pairing on $Ř(E/K) \times Ω(E/K)$ with values in ${}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$ whose kernel on each side consists of the divisible elements. In particular this identifies $Ř(E/K)/\,\mathrm{div}$ with the dual of $Ч(E/K)/\,\mathrm{div}$.*

This is just a reformulation of the main theoren in [**Fla90**] when using the local conditions $W_\upsilon = 0$ for all places υ.

From the Poitou–Tate sequence [**NSW00**, theorem 8·6·13] we may deduce two other facts. Let Σ be any finite set of places containing the ones above p, and those where E has bad reduction. The group $Ř(E/K)$ is dual to the kernel of

$$H^2(G_\Sigma(K), T_pE) \longrightarrow \bigoplus_{\upsilon \in \Sigma} H^2(K_\upsilon, T_pE)$$

where $G_\Sigma(K)$ stands for the Galois group of the maximal extension of K which is unramified outside Σ. The target of the map is the dual of the finite group $\oplus_{\upsilon \in \Sigma} E(K_\upsilon)(p)$. Furthermore

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

there is an exact sequence

$$0 \longrightarrow \mathcal{R}(E/K) \longrightarrow H^1(G_\Sigma(K), E(p)) \longrightarrow \bigoplus_{v\in\Sigma} H^1(K_v, E(p))$$

$$\longrightarrow H^1(G_\Sigma(K), T_pE)^\wedge \longrightarrow H^2(G_\Sigma(K), E(p)) \longrightarrow 0.$$

Here $M^\wedge$ denotes the Pontryagin dual of M.

7. *The fine Mordell–Weil group*

We now turn our interest to the other side of the fine Selmer group, namely the fine Mordell-Weil group. In the limit, we have a compact version $\mathfrak{M}(E/K)$ and a discrete version $\mathcal{M}(E/K)$. Note that, even though the group $E(K)\otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}$ is divisible, the group $\mathcal{M}(E/K)$ is not necessarily divisible as we see in the following example. Let E be the elliptic curve 37A1 given by the equation

$$E: \quad y^2 + y = x^3 - x \tag{7·1}$$

defined over $\mathbb{Q}$, whose Mordell–Weil group $E(\mathbb{Q})$ is generated by the point of infinite order $P = (0, 0)$. We shall see that the fine Mordell–Weil group $\mathcal{M}(E/\mathbb{Q})$ for the prime $p = 179$ is a finite non-trivial group. The curve has good, ordinary, non-anomalous reduction at p. The point $81 \cdot P$ is the first multiple of P that lies in the kernel of reduction modulo p, but it even lies in the second layer of the formal group, i.e. the denominator of the x-coordinate is divisible by p^4. In other words, the point P is divisible by p in $E(\mathbb{Q}_p)$. Hence $\mathcal{M}(E/\mathbb{Q}) = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$.

More generally, the size of the group $\mathcal{M}(E/K)/\operatorname{div}$ measures the divisibility of the generators in $E(\mathbb{Q}_p)$. For curves of rank 1 over $\mathbb{Q}$ it can be expressed in terms of the p-adic logarithm of the generator. See [**CM94**, lemma 9]; the first table in this paper can be used to find further examples like the one above.

If A is an abelian group, we denote by $A^\star$ the p-adic completion $\varprojlim A/p^kA$ of A.

THEOREM 7·1. *We have the following exact sequence*

$$0 \longrightarrow \mathfrak{M}(E/K) \longrightarrow T_p\mathcal{M}(E/K) \longrightarrow T \longrightarrow \operatorname{Tors}_{\mathbb{Z}_p}(D) \longrightarrow \mathcal{M}(E/K)/\operatorname{div} \longrightarrow 0$$

where D is the cokernel of the map $E(K)^\star \longrightarrow \oplus_{v|p} E(K_v)^\star$ and T is the cokernel of the corresponding localisation map on the p-primary part, namely $E(K)(p) \rightarrowtail \oplus_{v|p} E(K_v)(p)$.

Proof. We split the exact sequence

$$0 \longrightarrow \mathcal{M}(E/K) \longrightarrow E(K)\otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p} \longrightarrow \oplus\, E(K_v)\otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p} \longrightarrow C \longrightarrow 0$$

by defining B to be the image of the middle map. Now, the middle terms are divisible and so is B. This provides us with two exact sequences

$$0 \longrightarrow T_p\mathcal{M}(E/K) \longrightarrow T_p\big(E(K)\otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}\big) \longrightarrow T_pB \longrightarrow \mathcal{M}(E/K)/\operatorname{div} \longrightarrow 0 \tag{7·2}$$

$$0 \longrightarrow T_pB \longrightarrow \oplus\, T_p(E(K_v)\otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}) \longrightarrow T_pC \longrightarrow 0. \tag{7·3}$$

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

We apply the snake lemma to the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)(p) & \longrightarrow & E(K)^\star & \longrightarrow & T_p(E(K)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \oplus E(K_\upsilon)(p) & \longrightarrow & \oplus E(K_\upsilon)^\star & \longrightarrow & \oplus T_p(E(K_\upsilon)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}) & \longrightarrow & 0 \end{array}$$

Defining A to be the cokernel of the vertical map on the right-hand side, we find the sequence

$$0 \longrightarrow \mathfrak{M}(E/K) \longrightarrow T_p\mathcal{M}(E/K) \longrightarrow T \longrightarrow D \longrightarrow A \longrightarrow 0$$

containing the first four terms of the sequence in the theorem. Furthermore, by the two sequences involving (7·2) and (7·3), we see that the cokernel A is in the following sequence

$$0 \longrightarrow \mathcal{M}(E/K)/\operatorname{div} \longrightarrow A \longrightarrow T_pC \longrightarrow 0.$$

The fact that T_pC is $\mathbb{Z}_p$-free proves that $\operatorname{Tors}_{\mathbb{Z}_p}(A) = \mathcal{M}(E/K)/\operatorname{div}$.

Note that if E is defined over $\mathbb{Q}$ and the rank is positive then D is torsion.

COROLLARY 7·2. *If the curve E is defined over $\mathbb{Q}$ and $E(\mathbb{Q}_p)[p]$ is trivial, then the canonical map from $\mathfrak{M}(E/\mathbb{Q})$ to $T_p\mathcal{M}(E/K)$ is an isomorphism.*

Note that this does not hold in general, as we can see in the following example. Let E be the curve

$$E: \quad y^2 + x\,y = x^3 + 1 \tag{7·4}$$

of conductor 433 and let $p = 3$. The curve E has no non-trivial torsion point defined over $\mathbb{Q}$, but two linearly independent points of infinite order, namely $P_1 = (-1, 0)$ and $P_2 = (0, 1)$. Over $\mathbb{Q}_3$ there is a 3-torsion point on E, namely

$$S = \big(2 + 2\cdot 3^3 + 3^6 + 2\cdot 3^7 + 3^9 + \mathbf{O}(3^{10}),\, 2\cdot 3^2 + 3^3 + 3^5 + 2\cdot 3^8 + \mathbf{O}(3^{10})\big).$$

The reduction of E at $p = 3$ is good anomalous with 6 points on the reduced curve $\widetilde{E}(\mathbb{F}_3)$. The reduction of the point P_2 generates $\widetilde{E}(\mathbb{F}_3)$. On the other hand the point $P_1 + 2\cdot P_2 = (13/9, 38/27)$ is in the first layer of the formal group $\widehat{E}(3\mathbb{Z}_3)$. It follows that $E(\mathbb{Q})^\star \twoheadrightarrow E(\mathbb{Q}_3)^\star$ is surjective. On the other hand the group T is not trivial since there is this point S of order 3 that it not defined over $\mathbb{Q}$. From the sequence in the above theorem, we conclude that the index of $\mathfrak{M}(E/\mathbb{Q})$ in $T_p\mathcal{M}(E/\mathbb{Q})$ is equal to p.

As a consequence of the previous theorem, we find some more information on the fine Mordell–Weil group

COROLLARY 7·3. *The compact fine Mordell–Weil group $\mathfrak{M}(E/K)$ is a free $\mathbb{Z}_p$-module of finite rank. If the rank r of the curve is zero then $\mathfrak{M}(E/K) = \mathcal{M}(E/K) = 0$, otherwise, if r is positive, then*

$$r - [K:\mathbb{Q}] \leqslant \operatorname{corank}_{\mathbb{Z}_p} \mathcal{M}(E/K) = \operatorname{rank}_{\mathbb{Z}_p} \mathfrak{M}(E/K) \leqslant r - 1.$$

If $K = \mathbb{Q}$, we have equality.

Proof. The only thing that is left to prove is the left-hand inequality. Let P be a point of infinite order on $E(K)$. A certain multiple of P will lie in all the kernels $\widehat{E}(\mathfrak{m}_\upsilon)$ of reduction modulo all places above p. Since there is an injection from $\widehat{E}(\mathfrak{m}_\upsilon)$ into $E(K_\upsilon)^\star$ for all $\upsilon \mid p$, this multiple will not lie in $\mathfrak{M}(E/K)$. (Compare to the proof of Theorem 3·5.)

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

In particular, for curves of rank 0, the sequence in Theorem 7·1 becomes simply an isomorphism between T and $\mathrm{Tors}_{\mathbb{Z}_p}(D)$. If E is defined over $\mathbb{Q}$ and has rank 1 then we get a sequence

$$0 \longrightarrow T \longrightarrow D \longrightarrow \mathcal{M}(E/\mathbb{Q}) \longrightarrow 0$$

of finite groups.

8. *Conjectures*

The purpose of this last section is to announce some conjectures on the finiteness of the fine Tate–Shafarevich group. Of course, there is a first basic

CONJECTURE 8·1. *The fine Tate–Shafarevich group $\text{Ш}(E/K)$ of an elliptic curve over a number field K is finite. For a given E/K it is trivial for all but a finite number of primes p.*

It is a weaker form of what should be believed by any gentleman namely that $\text{Ш}(E/K)$ is already finite. Note that over $\mathbb{Q}$ for a curve of positive rank the two statements are equivalent by Theorem 3·5.

The original interest in this group comes from Iwasawa theory for elliptic curves. Let E be an elliptic curve, for simplicity, defined over $\mathbb{Q}$. Using the methods of Perrin-Riou [**PR95**] one is able to compute the growth of the size of the fine Tate–Shafarevich group in certain towers of number fields. See [**Wut05**] and [**Wut04**] for more details. Let $\mathbb{Q}(\mu[p^{n+1}])$ be the cyclotomic field of p^{n+1}-th roots of unity and let ${}_n\mathbb{Q}$ be the unique subfield of $\mathbb{Q}(\mu[p^{n+1}])$ with Galois group $\mathrm{Gal}({}_n\mathbb{Q}:\mathbb{Q})$ isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. The cyclotomic $\mathbb{Z}_p$-extension ${}_\infty\mathbb{Q}$ of $\mathbb{Q}$ is defined to be the union of all ${}_n\mathbb{Q}$ as n varies over the positive integers.

Denote by e_n the integer such that $\#\text{Ш}(E/{}_n\mathbb{Q}) = p^{e_n}$. By a famous theorem of Kato [**Kat04**], we know that the integer e_n grows like $\mu \cdot p^n + \lambda \cdot n + \mathbf{O}(1)$ for some integers $\mu \geqslant 0$ and $\lambda \geqslant 0$. There is a first conjecture, a special case of conjecture A in [**CS05**], due to Coates and Sujatha.

CONJECTURE 8·2. *The growth of the order of $\text{Ш}(E/{}_n\mathbb{Q})$ is of the form $e_n = \lambda \cdot n + \mathbf{O}(1)$, i.e. $\mu = 0$.*

The striking thing about this conjecture is that a similar statement for $\text{Ш}(E/{}_n\mathbb{Q})$ is known to be false ever since the beginnings of Iwasawa theory for elliptic curves, see [**Maz72**]. For our case of a curve over $\mathbb{Q}$, the conjecture is verified if E admits an isogeny of degree p defined over $\mathbb{Q}$. This follows from [**CS05**, corollary 3·5].

As an example, we might consider the curve of conductor 11 given by

$$E: \quad y^2 + y = x^3 - x^2 - 7'820\,x - 263'580$$

for which it is known that the order of $\text{Ш}(E/{}_n\mathbb{Q})(5)$ for $p = 5$ grows like $5^{2\cdot 5^n}$, i.e. $\mu = 2$ and $\lambda = 0$. Nevertheless, the order of $\text{Ш}(E/{}_n\mathbb{Q})$ stays bounded, see [**Wut05**].

The numerical evidence computed in [**Wut04**] suggest that it might be possible that the following question has a positive answer.

QUESTION 8·3. *Is the order of $\text{Ш}(E/{}_n\mathbb{Q})$ bounded independently of n, i.e. do we have that $\mu = \lambda = 0$?*

In other words, we could ask if $\text{Ш}(E/{}_\infty\mathbb{Q})$ is finite. For the supersingular case the eventuality that the answer might be "yes" was mentioned to me by Kurihara and Pollack.

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press

Nevertheless, there is one hint that it could be wrong in the extension to the situation of ordinary reduction. In the case of a global field of positive characteristic different from p, say K is a function field of a curve over a finite field, the fine Tate–Shafarevich group of an elliptic curve E over K naturally coincides with the full Tate–Shafarevich group, since there are no places above p. Moreover it is equal to the Brauer–Grothendieck group $\mathrm{Br}(\mathcal{E})$ of the elliptic surface $\mathcal{E}$ whose generic fibre is E, see [**Tat95**]. The analogue of $Ш(E/_\infty\mathbb{Q})$ is the the Brauer group $\mathrm{Br}(\bar{\mathcal{E}})$ of the surface $\mathcal{E}$ but over the algebraic closure of the finite base field. There are certainly many examples of infinite $\mathrm{Br}(\bar{\mathcal{E}})$.

On the other hand, we know that $\mathrm{Br}(\bar{\mathcal{E}})$ is co-finitely generated over $\mathbb{Z}_p$ and so Conjecture 8·2 is known for function fields.

But at least, we can be sure that a weaker form of the question should have a positive answer, namely.

CONJECTURE 8·4. *For all but a finite number of primes p, the order of $Ш(E/_n\mathbb{Q})$ is bounded independently of n.*

Compare with the conjectures in [**Wut05**] on the density of such primes.

Acknowledgements. It is a pleasure to thank John Coates, Mike Shuter, Paola Argentin and Sylvia Guibert for their help and comments.

REFERENCES

[**CM94**] J. COATES and G. MCCONNELL. Iwasawa theory of modular elliptic curves of analytic rank at most 1. *J. London Math. Soc. (2)* **50** (1994), no. 2, 243–264.

[**Cre97**] J. E. CREMONA. *Algorithms for Modular Elliptic Curves*, second ed. (Cambridge University Press, 1997).

[**CS05**] J. COATES and R. SUJATHA. Fine Selmer groups of elliptic curves over p-adic Lie extensions. *Math. Ann.* **331** (2005), no. 4, 809–839.

[**Fla90**] M. FLACH. A generalisation of the Cassels-Tate pairing. *J. Reine Angew. Math.* **412** (1990), 113–127.

[**Kat04**] K. KATO. p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et application arithmétiques. III, *Astérisque* **295** (2004).

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

[**NSW00**] J. NEUKIRCH, A. SCHMIDT and K. WINGBERG. Cohomology of number fields. *Grundlehren der Mathematischen Wissenschaften* **323** (2000).

[**PR95**] B. PERRIN–RIOU. Fonctions L p-adiques des représentations p-adiques. *Astérisque* **229** (1995), 198.

[**Rub00**] K. RUBIN. Euler systems. *Ann. Math. Stud.* **147** (2000), Hermann Weyl Lectures. The Institute for Advanced Study.

[**Sil96**] J. H. SILVERMAN. The arithmetic of elliptic curves. *Graduate Texts in Mathematics*. vol. 99 (Springer, 1996).

[**Tat95**] J. TATE. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. *Séminaire Bourbaki* **9** (1995), pp. Exp. No. 306, 415–440.

[**Wut04**] C. WUTHRICH. The fine Selmer group and height pairings. Ph.D. Thesis (University of Cambridge, 2004).

[**Wut05**] C. WUTHRICH. Iwasawa theory of the fine Selmer group, in preparation (2005).

https://doi.org/10.1017/S0305004106009662 Published online by Cambridge University Press