Congruences and Unramified Cohomology

Dimitar Jetchev and William Stein

November 19, 2005

1 Unramified Cohomology

Suppose E is an elliptic curve over a number field K and let p be a prime. For any $\mathbb{F}_p$ vector space M let $\dim M$ denote the $\mathbb{F}_p$ dimension of M.

Denote by $\Phi_{E,v}$ the component group of E at v, and let

$$\tau_p = \sum_v \dim \Phi_{E,v}(\mathbb{F}_v)[p].$$

Let $\mathrm{H}^1_{\mathrm{ur}}(K, E[p])$ denote the subgroup of cohomology classes that split over an unramified extension of K_v for all v. Let

$$\mathrm{Sel}^{(p)}_{\mathrm{ur}}(E/K) = \mathrm{Sel}^{(p)}(E/K) \cap \mathrm{H}^1_{\mathrm{ur}}(K, E[p]). \tag{1.1}$$

Proposition 1.1. *We have*

$$\dim \mathrm{H}^1_{\mathrm{ur}}(K, E[p]) \geq \dim \mathrm{Sel}^{(p)}_{\mathrm{ur}}(E/K) \geq \dim \mathrm{H}^1_{\mathrm{ur}}(K, E[p]) - \tau_p \tag{1.2}$$

Proof. Consider the exact sequence

$$0 \to \mathrm{Sel}^{(p)}_{\mathrm{ur}}(E/K) \to \mathrm{H}^1_{\mathrm{ur}}(K, E[p]) \to \bigoplus_v \mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, E). \tag{1.3}$$

By [Mil86, Prop. 3.8], $\mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, E) \cong \mathrm{H}^1(\mathbb{F}_v, \Phi_{E,v})$. Because $\mathrm{Gal}(\overline{\mathbb{F}}_v/\mathbb{F}_v)$ is pro-cyclic, $\dim \mathrm{H}^1(\mathbb{F}_v, \Phi_{E,v})[p] = \dim \Phi_{E,v}(\mathbb{F}_v)[p]$. A dimension count using (1.3) then implies (1.2). $\square$

Proposition 1.2. *We have*

$$\dim \mathrm{Sel}^{(p)}(E/K) \geq \dim \mathrm{Sel}^{(p)}_{\mathrm{ur}}(E/K)$$
$$\geq \dim \mathrm{Sel}^{(p)}(E/K) - \sum_{v \nmid p} \dim \Phi_{E,v}(\mathbb{F}_v)[p] - \sum_{v \mid p} \dim E(K_v)/(pE(K_v^{\mathrm{ur}}) \cap E(K_v)).$$

Proof. We have an exact sequence

$$0 \to \mathrm{Sel}^{(p)}_{\mathrm{ur}}(E/K) \to \mathrm{Sel}^{(p)}(E/K) \to \bigoplus_v E(K_v)/(pE(K_v^{\mathrm{ur}}) \cap E(K_v)). \quad (1.4)$$

For $v \nmid p$ the group $E^0(K_v^{\mathrm{ur}})$ is p divisible (see [AS02, §3.2]). Thus for $v \nmid p$,

$$E(K_v)/(pE(K_v^{\mathrm{ur}}) \cap E(K_v)) \subset E(K_v^{\mathrm{ur}})/pE(K_v^{\mathrm{ur}}) \cong \Phi_{E,v}(\overline{\mathbb{F}}_v) \otimes \mathbb{F}_p.$$

The image of $\mathrm{Sel}^{(p)}(E/K)$ in $\Phi_{E,v}(\overline{\mathbb{F}}_v) \otimes \mathbb{F}_p$ is fixed by $\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v)$, so lies in $\Phi_{E,v}(\mathbb{F}_v) \otimes \mathbb{F}_p$. Thus for $v \nmid p$

A dimension count involving (1.4) then finishes the proof. □

Let $\mathcal{E}$ denote the Néron model of E over $\mathcal{O}_v$, and let $\mathcal{E}$ be the open subscheme that reduces to the identity component mod v.

Lemma 1.3. *Suppose E is an elliptic curve over K and suppose that $v \mid p$ is such that $e(v) < p - 1$, where $e(v)$ is the ramification degree of v. Then*

$$\begin{aligned} \dim E(K_v)/pE(K_v) &= [K_v : \mathbb{Q}_p] + \dim E(K_v)[p] \\ &\le [K_v : \mathbb{Q}_p] + \dim \mathcal{E}^0(\mathbb{F}_v)[p] + \dim \Phi_{E,v}(\mathbb{F}_v)[p] \end{aligned}$$

Proof. Since $e(v) < p - 1$ the theory of formal groups (see e.g., [Sil92, Thm. 6.4]) implies that there is an exact sequence

$$0 \to \mathcal{O}_v \to E(K_v) \to \mathcal{E}(\mathbb{F}_v) \to 0.$$

Apply the snake lemma to multiplication by p on this sequence and using that $\mathcal{O}_v$ is a ring of characteristic 0 (so $\mathcal{O}_v[p] = 0$), we obtain the exact sequence

$$0 \to E(K_v)[p] \to \mathcal{E}(\mathbb{F}_v)[p] \to \mathcal{O}_v/p\mathcal{O}_v \to E(K_v)/pE(K_v) \to \mathcal{E}(\mathbb{F}_v)/p\mathcal{E}(\mathbb{F}_v) \to 0.$$

Thus

$$\dim E(K_v)[p] - \dim \mathcal{E}(\mathbb{F}_v)[p] + \dim \mathcal{O}_v/p\mathcal{O}_v - \dim \frac{E(K_v)}{pE(K_v)} + \dim \frac{\mathcal{E}(\mathbb{F}_v)}{p\mathcal{E}(\mathbb{F}_v)} = 0.$$

Since $\dim \mathcal{O}_v/p\mathcal{O}_v = \mathrm{rank}\, \mathcal{O}_v = [K_v : \mathbb{Q}_p]$, and for any finite abelian group A, $\#A[p] = \#(A/pA)$, this becomes

$$\dim E(K_v)[p] + [K_v : \mathbb{Q}_p] - \dim \frac{E(K_v)}{pE(K_v)} = 0.$$

Since the torsion-free group $\mathcal{O}_v$ is the kernel of reduction, $E(K_v)[p] \subset \mathcal{E}(\mathbb{F}_v)[p]$. thus

$$\dim E(K_v)/pE(K_v) \leq [K_v : \mathbb{Q}_p] + \dim \mathcal{E}(\mathbb{F}_v)[p]$$

By Lang's theorem, $\mathrm{H}^1(\mathbb{F}_v, \mathcal{E}^0) = 0$, so $0 \to \mathcal{E}^0(\mathbb{F}_v) \to \mathcal{E}(\mathbb{F}_v) \to \Phi_{E,v}(\mathbb{F}_v) \to 0$ is exact, hence

$$\dim \mathcal{E}(\mathbb{F}_v)[p] \leq \dim \mathcal{E}^0(\mathbb{F}_v)[p] + \dim \Phi_{E,v}(\mathbb{F}_v)[p].$$

□

Theorem 1.4. *Suppose E is an elliptic curve over $\mathbb{Q}$ and p is a good odd non-anomalous prime that doesn't divide any Tamagawa number of E. Then there is an exact sequence*

$$0 \to \mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}, E[p]) \to \mathrm{Sel}^{(p)}(E/\mathbb{Q}) \to E(\mathbb{Q}_p)/(pE(\mathbb{Q}_p^{\mathrm{ur}}) \cap E(\mathbb{Q}_p)), \qquad (1.5)$$

and

$$\dim E(\mathbb{Q}_p)/(pE(\mathbb{Q}_p^{\mathrm{ur}}) \cap E(\mathbb{Q}_p)) \leq \dim E(\mathbb{Q}_p)/pE(\mathbb{Q}_p) \leq 1.$$

In particular $\dim \mathrm{Sel}^{(p)}(E/\mathbb{Q})/\mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}, E[p])] \leq 1$.

Proof. The Tamagawa number hypothesis implies that $\tau_p = 1$, so Proposition 1.1 implies that $\mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}, E[p]) = \mathrm{Sel}^{(p)}_{\mathrm{ur}}(E/\mathbb{Q})$, which yields the injection of (1.5). The rest of the sequence then follows from Lemma 1.3 and the *proof* of Proposition 1.2 □

2 Compare Selmer Groups via Congruences

Suppose E and F are elliptic curves over a number field K and p is a prime such that $E[p] \cong F[p]$ as G_K-modules. This isomorphism of p-torsion induces an isomorphism

$$\mathrm{H}^1_{\mathrm{ur}}(K, E[p]) \cong \mathrm{H}^1_{\mathrm{ur}}(K, F[p]).$$

If $\tau_p = 1$, then we have a diagram with vertical inclusions

$$\begin{array}{ccc} \mathrm{Sel}^{(p)}(E/K) & & \mathrm{Sel}^{(p)}(F/K) \\ \uparrow & & \uparrow \\ \mathrm{H}^1_{\mathrm{ur}}(K, E[p]) & \xrightarrow{\cong} & \mathrm{H}^1_{\mathrm{ur}}(K, F[p]) \end{array} \qquad (2.1)$$

Theorem 2.1. *Suppose E, F are elliptic curves over $\mathbb{Q}$ and p is a good odd non-anomalous prime (for both E and F) that doesn't divide any Tamagawa number of E or F. Then*

$$|\dim \mathrm{Sel}^{(p)}(E/\mathbb{Q}) - \dim \mathrm{Sel}^{(p)}(F/\mathbb{Q})| \leq 1.$$

Proof. Theorem 1.4 implies that the image of each vertical inclusion of (2.1) has codimension ≤ 1. □

Acknowledgment: A very helpful discussion with Karl Rubin.

References

[AS02] A. Agashe and W. A. Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185.

[Mil86] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.