

# The method of Coates and Wiles for integral points

Minhyong Kim

October 12, 2007

Principle of Birch and Swinnerton-Dyer for elliptic curves  $E/\mathbb{Q}$ :

$L(E, 1) \neq 0 \Rightarrow E(\mathbb{Z})$  is finite.

Does this extend to hyperbolic curves?

Consider

$$X := E \setminus \{0\},$$

where  $E/\mathbb{Q}$  is an elliptic curve with complex multiplication by an imaginary quadratic field  $K$ .

Coates and Wiles resolved (this part of) BSD for  $E$  using the ‘method of  $p$ -adic  $L$ -functions’.

Notation:

$S$ , a set of primes including  $\infty$  and those of bad reduction for  $E$

$$\Gamma := \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

$$N := \text{Gal}(\bar{\mathbb{Q}}/K)$$

$p = \pi\bar{\pi}$  a prime of good reduction for  $E$ , split in  $K$

$$M = K(E[\pi^\infty]), \quad \bar{M} = K(E[\bar{\pi}^\infty])$$

$$G = \text{Gal}(M/K), \quad \bar{G} = \text{Gal}(\bar{M}/K)$$

$$\Lambda = \mathbb{Z}_p[[G]], \quad \bar{\Lambda} = \mathbb{Z}_p[[\bar{G}]]$$

$\psi : \Lambda \rightarrow \mathbb{Q}_p$  defined by action of  $G$  on  $T_\pi(E)$

$\bar{\psi} : \bar{\Lambda} \rightarrow \mathbb{Q}_p$  defined by action of  $\bar{G}$  on  $T_{\bar{\pi}}(E)$

$V_p = T_p(E) \otimes \mathbb{Q}$ ,  $V_\pi$ , etc.

Have corresponding  $p$ -adic  $L$ -functions:

$$\mathcal{L}_p \in \Lambda, \quad \bar{\mathcal{L}}_p \in \bar{\Lambda}$$

$p$ -adic polylogarithms for  $E$ :

Choose differentials  $\alpha, \beta$  of second kind for  $X$  and define, for  $n \geq 2$ ,

$$\mathcal{P}_n(z) = \int_b^z \alpha^n \beta$$

$$\bar{\mathcal{P}}_n(z) = \int_b^z \beta^n \alpha$$

These are locally analytic Coleman functions on  $X(\mathbb{Z}_p)$ .

**Corollary 0.1** *There is a non-trivial polynomial*

$$f = f(\mathcal{P}_n, \bar{\mathcal{P}}_n)$$

*of the  $\mathcal{P}_n, \bar{\mathcal{P}}_n$  restricting to a non-zero convergent power series on each residue disk of  $X(\mathbb{Z}_p)$ , such that*

$$f(z) = 0$$

*for each point  $z \in X(\mathbb{Z}_S) \subset X(\mathbb{Z}_p)$ .*

$$r = \dim H_f^1(\Gamma, V_p(E))$$

$$s = |s|$$

**Corollary 0.2** *Suppose  $\psi^{-k}(\mathcal{L}_p) \neq 0$  and  $\bar{\psi}^{-k}(\bar{\mathcal{L}}_p) \neq 0$  for all  $k > 0$ . Then there is a non-trivial polynomial*

$$f = f(\mathcal{P}_., \bar{\mathcal{P}}_.)$$

*of the  $\mathcal{P}_n, \bar{\mathcal{P}}_n$ , for  $n \leq r + s$ , restricting to a non-zero convergent power series on each residue disk of  $X(\mathbb{Z}_p)$ , such that*

$$f(z) = 0$$

*for each point  $z \in X(\mathbb{Z}_S) \subset X(\mathbb{Z}_p)$ .*

$U$ :  $\mathbb{Q}_p$ -pro-unipotent étale fundamental group for  $(\bar{X}, b)$ .

$$U^1 = U, U^n = [U, U^{n-1}].$$

$$U_n = U/U^{n+1}.$$

Fundamental diagram:

$$\begin{array}{ccc} X(\mathbb{Z}_S) & \hookrightarrow & X(\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ H_f^1(\Gamma, U_n) & \rightarrow & H_f^1(\Gamma_p, U_n) \end{array}$$

$$x \mapsto [\pi_1^{\mathbb{Q}_p}(\bar{X}; b, x)]$$

The subscript ' $f$ ' corresponds to the condition that the cohomology classes be unramified outside  $T = S \cup \{p\}$  and crystalline at  $p$ .

$U$  is somewhat complicated. Replace by a quotient

$$U \longrightarrow W$$

with the property that

$$U_2 \simeq W_2$$

and

$$W^n / W^{n+1} \simeq \psi^{n-2}(1) \oplus \bar{\psi}^{n-2}(1)$$

viewed as a representation of  $\Gamma$  in the natural way.

Construction:

$\Gamma = N \langle \sigma \rangle$ , where  $\sigma$  is complex conjugation.

Choose a  $\mathbb{Q}_p$ -basis  $e$  of  $T_\pi(E) \otimes \mathbb{Q}_p$  so that  $f := \sigma(e)$  is a  $\mathbb{Q}_p$ -basis of  $T_{\bar{\pi}}(E) \otimes \mathbb{Q}_p$ .

Recall that

$$\mathcal{U} := \text{Lie}U$$

can be realized as the primitive elements in

$$T(U_1) = T(V_p)$$

where  $T(\dots)$  refers to the tensor algebra (but with a different Galois action).

For example, if  $\gamma \in N$ , then

$$\gamma[e, [e, f]] = \psi(\gamma)^2 \bar{\psi}(\gamma)[e, [e, f]] + \text{Lie monomials of higher degree}$$

and

$$\sigma[e, [e, f]] = [f, [f, e]] + \text{Lie monomials of higher degree}$$

That is,  $\mathcal{U}$  has a bi-grading

$$\mathcal{U} = \overline{\bigoplus_{i,j \geq 1} \mathcal{U}_{i,j}}$$

corresponding to  $e$  and  $f$  degrees, but which is not preserved by the Galois action.

However, easy to check:

$$\mathcal{U}_{\geq n, \geq m} := \overline{\bigoplus_{i \geq n, j \geq m} \mathcal{U}_{i,j}}$$

is preserved by  $N$ , while

$$\sigma(\mathcal{U}_{\geq n, \geq m}) = \mathcal{U}_{\geq m, \geq n}$$

So

$$\mathcal{U}_{\geq n, \geq n}$$

is Galois invariant for each  $n$ .

Furthermore, it is a Lie ideal.

Hence, there is a well-defined quotient  $W$  of  $U$  corresponding to

$$\mathcal{U}/\mathcal{U}_{\geq 2, \geq 2}$$

We then see that

$$\begin{aligned} & W^n / W^{n+1} \\ & \simeq \langle \text{ad}(e)^{n-1}(f) \rangle \oplus \langle \text{ad}(f)^{n-1}(e) \rangle \pmod{W^{n+1}} \\ & \simeq \psi^{n-2}(1) \oplus \bar{\psi}^{n-2}(1) \end{aligned}$$

Fundamental diagram can thus be extended to

$$\begin{array}{ccc} X(\mathbb{Z}_S) & \hookrightarrow & X(\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ H_f^1(\Gamma, U_n) & \rightarrow & H_f^1(\Gamma_p, U_n) \\ \downarrow & & \downarrow \\ H_f^1(\Gamma, W_n) & \rightarrow & H_f^1(\Gamma_p, W_n) \end{array}$$

The map

$$j_n : X(\mathbb{Z}_p) \rightarrow H_f^1(\Gamma_p, W_n)$$

is described by non-abelian  $p$ -adic Hodge theory:

$$H_f^1(\Gamma_p, W_n) \simeq F^0 \setminus W_n$$

according to which

$$j_n^*(\text{Coordinate ring of } H_f^1(\Gamma_p, W_n))$$

is contained in the ring generated by  $\mathcal{P}_m, \bar{\mathcal{P}}_m$  for  $m \leq n$ .

Meanwhile:

**Theorem 0.3**

$$\dim H_f^1(\Gamma, W_n) < \dim H_f^1(\Gamma_p, W_n)$$

*for  $n \gg 0$ .*

Also:

**Theorem 0.4** *Assume*

$$(*) \quad \psi^{-k}(\mathcal{L}_p) \neq 0 \text{ and } \bar{\psi}^{-k}(\bar{\mathcal{L}}_p) \neq 0 \text{ for all } k > 0.$$

*Then*

$$\dim H_f^1(\Gamma, W_n) < \dim H_f^1(\Gamma_p, W_n)$$

*for*  $n = r + s$ .

The earlier corollaries follow immediately from the theorems.

Proof of theorem uses main conjecture for  $K$ . To fix ideas, we will concentrate on (0.4).

We need the exact sequence

$$0 \rightarrow W^n / W^{n+1} \rightarrow W_n \rightarrow W_{n-1} \rightarrow 0$$

As for the Hodge filtration,

$$\dim W_1 / F^0 = 1$$

and

$$F^0[W^n / W^{n+1}] = 0$$

for  $n \geq 2$ , so that

$$\dim H_f^1(\Gamma_p, W_n) = 2 + 2(n - 2) = 2n - 2$$

for  $n \geq 2$ .

Meanwhile,

$$\dim H_f^1(\Gamma, W_1) = r$$

$$\dim H_f^1(\Gamma, W^1/W^2) = \dim H_f^1(\Gamma, \mathbb{Q}_p(1)) = s - 1$$

so that

$$\dim H_f^1(\Gamma, W_2) = r + s - 1$$

As we go down the lower central series, we have, in any case, the Euler characteristic formula (where  $T = S \cup \{p\}$ )

$$\begin{aligned} \dim H^1(\Gamma_T, W^n/W^{n+1}) - \dim H^2(\Gamma_T, W^n/W^{n+1}) \\ = \dim (W^n/W^{n+1})^{\sigma=-1} = 1 \end{aligned}$$

and

$$H_f^1(\Gamma, W^n/W^{n+1}) = H^1(\Gamma_T, W^n/W^{n+1})$$

for  $n \geq 2$ , so we need to compute the  $H^2$  term.

Claim (still assuming (\*)):

$$H^2(\Gamma_T, W^n/W^{n+1}) = 0$$

for  $n \geq 3$ .

Clearly, it suffices to prove this after restricting to  $N_T \subset \Gamma_T$  with obvious notation. Then we have

$$W^n/W^{n+1} \simeq \psi^{n-2}(1) \oplus \bar{\psi}^{n-2}(1)$$

We will show

$$H^2(N_T, \psi^{n-2}(1)) = 0$$

for  $n \geq 3$ .

Consider the localization sequence

$$0 \rightarrow Sha_T^2(\psi^{n-2}(1)) \hookrightarrow H^2(N_T, \psi^{n-2}(1)) \rightarrow \bigoplus_{v|T} H^2(N_v, \psi^{n-2}(1))$$

that defines the vector space  $Sha^2(\psi^{n-2}(1))$ . By local duality,

$$H^2(N_v, \psi^{n-2}(1)) \simeq H^0(N_v, \psi^{2-n})^* = 0$$

since the representation  $\psi^{2-n}$  is potentially unramified or potentially crystalline.

So we have

$$H^2(N_T, \psi^{n-2}(1)) \simeq Sha_T^2(\psi^{n-2}(1)) \simeq Sha_T^1(\psi^{2-n})^*$$

by Poitou-tate duality. But

$$Sha_T^1(\psi^{2-n}) \simeq \text{Hom}_\Lambda(A \otimes \mathbb{Q}, \psi^{2-n})$$

where  $A$  is the Galois group of the maximal abelian unramified pro- $p$  extension of  $M(= K(E[\pi^\infty]))$  split above the primes dividing  $T$ .

In particular,  $A \otimes \mathbb{Q}$  is annihilated by  $\mathcal{L}_p$ .

Since we are assuming  $\psi^{2-n}(\mathcal{L}_p) \neq 0$  for  $n \geq 3$ , we get the desired vanishing:

$$H^2(N_T, \psi^{n-2}(1)) = 0$$

Similarly,

$$H^2(N_T, \bar{\psi}^{n-2}(1)) = 0$$

Finally, we conclude that

$$\dim H_f^1(\Gamma, W^n / W^{n+1}) = 1$$

for  $n \geq 3$  so that

$$\dim H_f^1(\Gamma, W_n) = r + s + n - 3$$

for  $n \geq 2$ .

Thus,

$$H_f^1(\Gamma_p, W_n) = 2n - 2 > r + s + n - 3 = \dim H_f^1(\Gamma, W_n)$$

as soon as  $n \geq r + s$ .

Note that even without (\*), we have

$$\psi^{2-n}(\mathcal{L}_p) \neq 0 \quad \bar{\psi}^{2-n}(\bar{\mathcal{L}}_p) \neq 0$$

and hence,

$$H^2(\Gamma_T, W^n/W^{n+1}) = 0$$

for  $n$  sufficiently large. Therefore,

$$\dim H_f^1(\Gamma, W_n) < \dim H_f^1(\Gamma_p, W_n)$$

for  $n$  sufficiently large, yielding finiteness of

$$X(\mathbb{Z}_S)$$

in any case.