On the Conjecture of Birch and Swinnerton-Dyer for Elliptic Curves with Complex Multiplication

Notes by Tony Feng
for a talk by John Coates

June 13, 2016

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$. Let g_E be the rank of $E(\mathbb{Q})$. We write $r_E = \operatorname{ord}_{s=1} L(E, s)$. A special case of more general theorem I'll announce today is:

Theorem 1.1. *If $r_E = 0$ then $g_E = 0$.*

How do we prove the *converse*, $g_E = 0 \implies r_E = 0$? Even today, we know surprisingly little about this.

The *Main Conjecture* tells us:

Theorem 1.2. *If p is a sufficiently large good ordinary prime, then $L_E(1) \neq 0 \iff g_E = 0$ and $\text{Ш}(E)(p)$ is finite.*

The problem with this theorem is that it is *precisely* for the primes p as in the hypothesis that we do not know how to show that the p-primary part $\text{Ш}(E)(p)$ is finite.

We would *like* to have a statement such as:

Conjecture 1.3. *$L(E, 1) \neq 0 \iff g_E = 0$ and $\text{Ш}(E)(2)$ is finite.*

(Of course we would also like to have the result with 2 replaced by some other prime as well.) One reason why we would like this is that we could then use descent to prove specific cases of BSD which are currently out of reach. The methods we will discuss are Iwasawa-theoretic. Morally, we think that they should be able to reach the result with p being any good ordinary prime.

2 An example

Let A be a fixed elliptic curve and M the discriminant of a quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Let $E = A^{(M)}$ be the twist of A by $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$.

Example 2.1. Consider $A = X_0(49)$, which has minimal equation $y^2 + xy = x^3 - x^2 - 2x - 1$ and discriminant $\Delta = -7^3$. It has CM by $K = \mathbb{Q}(\sqrt{7})$. The prime 2 is good ordinary for this curve, so it is in some sense the simplest of elliptic curves.

Theorem 2.2 (Rubin, Gonzalez-Aviles)**.** *Let E be any quadratic twist of $X_0(49)$. Then $L(E,1) \neq 0 \iff g_E = 0$ and $Ш(E)(2)$ is finite. Moreover, when $L(E,1) \neq 0$ then $\#Ш(E)$ is finite and as predicted by BSD.*

As far as I know, this is the only family of elliptic curves for which we can prove such a theorem.

Corollary 2.3. *Assume E is a quadratic twist of $X_0(49)$. Then $g_E = 0$ and $Ш(E)(2) = 0$ if and only if it is predicted by BSD (in other words, if and only if $L(E,1) \neq 0$).*

This has some interesting numerical consequences. Let

$$\mathcal{M} = \{M = q_1 \cdot \ldots \cdot q_r \colon q_i \text{ distinct primes } \equiv 1 \mod 4, \text{ inert in } K\}.$$

Let $E = A^{(M)}$ for some $M \in \mathcal{M}$. The theorem says that $E(\mathbb{Q})$ is finite and $Ш(E)(2) = 0 \implies L(E,1) \neq 0$.

Example 2.4. A consequence of this result is that for any odd prime $p \leq 2357$, there exists $M \in \mathcal{M}$ such that $E = A^{(M)}$ has $Ш(E)$ of order p^2.

3 Consequences for the congruent number problem

Let C be the elliptic curve $y^2 = x^3 - x$. (This is the oldest elliptic curve; its quadratic twists control congruent numbers.)

Theorem 3.1 (Tian, Yuan, Zhang)**.** *Assume E is a quadratic twist of C. Then $g_E = 0$ and $Ш(E)(2) = 0 \iff$ it is predicted by BSD.*

Remark 3.2. The Tian-Yuan-Zhang proof is not Iwasawa-theoretic; they use an explicit form of a formula of Waldspurger.

Let N be any square-free positive integer. By combining the preceding results with analytic results of Heath-Brown, A. Smith showed that for $N \equiv 1, 2, 3 \pmod 8$ (i.e. when the root number of the twist $C^{(N)}$ is $+1$) roughly 50% are not congruent numbers (i.e. $g = 0$). For $N \equiv 5, 6, 7 \pmod 8$, roughly 50% are congruent numbers. Conjecturally, in the first case 100% are not congruent, and in the second case all are congruent.

4 Statement of results

Let $K = \mathbb{Q}(\sqrt{-q})$ where q is a prime $\equiv 7 \pmod 8$. Let h be the class number of K (which is odd because the discriminant is prime). Let H be the Hilbert class field of K; we know that $H = K(j(\mathcal{O}))$. Write $J = \mathbb{Q}(j(\mathcal{O}))$. Since $j(\mathcal{O})$ is real (why?), this comes with an embedding $J \hookrightarrow \mathbb{R}$. We also fix some embedding $K \hookrightarrow \mathbb{C}$.

Theorem 4.1 (Gross)**.** *There exists a unique elliptic curve $A = A(q)$ defined over J such that*

1. $\mathrm{End}_H(A) = \mathcal{O}$,
2. *the minimal discriminant of A/H is the ideal $(-q^3)$,*
3. *A is isogenous to all of its conjugates over H.*

In fact, Gross proved that this $A(q)$ has a *global* minimal Weierstrass equation.

Example 4.2. For $J = \mathbb{Q}(\alpha)$, with minimal equation $\alpha^3 - \alpha - 1 = 0$, the global minimal equation of A is

$$y^2 + \alpha^3 xy + (\alpha + 2)y = x^3 + 2x^2 - (12\alpha^2 + 27\alpha + 16)x - (73\alpha^2 + 99\alpha + 62)$$

Write $\psi_{A/H}$ for the Grossencharacter of A/H. (So the L-series of A/H is the product of that for $\psi_{A/H}$ and its conjugate.) Gross proved that $g_{A/H} = 0$, by 2-descent. Rohrlich showed that $L(A/H, 1) \neq 0$, which by aforementioned result gives another proof of this fact.

We would like to have an analogue of the theorem which we established for quadratic twists of $X_0(49)$. Careful: we cannot consider *all* quadratic extensionf of K, but only those twists coming from quadratic extensions of K.

So let $Q(A)$ be the set of twists of A by quadratic extensions of H of the form HK'/H, where K'/K is a quadratic extension of conductor prime to $2q$.

Let $E \in Q(A)$. Write $\psi_{E/H}$ for the Grossencharacter of E/H, which is $\phi \circ N_{H/K}$, where ϕ is a Grossencharacter of K (in fact, the one attached to the restriction of scalars of A from H to K). Let $\mathfrak{g}$ be the conductor of ϕ.

Now I'll describe joint work with Y. Kezuka, Y. Li, and Y. Tian. Let ω be the Neron differential, which will be a generator of the differentials for the global minimal Weierstrass equation. Let $\mathcal{L}$ be the period lattice of ω, which is of the form $\omega = \Omega_\infty \mathcal{O}$ for some $\Omega_\infty \in \mathbb{C}^*$. Let $\mathfrak{a}$ be an integral ideal of K and $\sigma_\mathfrak{a}$ the Artin symbol in $G = G(H/K)$ for $(\mathfrak{a}, \mathfrak{g}) = 1$. Then we have a canonical

$$\eta_E(\mathfrak{a})\colon E \to E^{\sigma_\mathfrak{a}}$$

Call the kernel of this map $E_\mathfrak{a}$. The Néron differential of $E^{\sigma_\mathfrak{a}}$ will be denoted $\omega^{\sigma_\mathfrak{a}}$.

Define $\xi(\mathfrak{a}) \in H^*$ by

$$\eta_E(\mathfrak{a})^*(\omega^{\sigma_\mathfrak{a}}) = \xi(\mathfrak{a})\omega.$$

Let

$$\Omega_\infty(E/H) = \prod_{\mathfrak{a}} (\xi(\mathfrak{a})\Omega_\infty)$$

Fact: for all $n \geq 1$, $\Omega_\infty(E/H)^{-n} L(\psi_{E/H}^n, n) \in K$ for all $n = 1, 2, 3, \ldots$.

Consider a prime p split in K, suppose $p\mathcal{O} = \mathfrak{p}\mathfrak{p}^*$. Suppose E has good reduction above p, and $(p, h) = 1$. Let $F_\infty = H(E[\mathfrak{p}^\infty])$.

For time reasons, let me state our result in a simplified case. Assume $p = 2$. Let M_∞ be the maximal abelian p-extension of K unramified outside $\mathfrak{p}$.

$$\begin{tikzcd}
 & M_\infty \\
F_\infty \arrow[ur, dash, "X_\infty"] & \\
H \arrow[u, dash, "\mathcal{G}"] & \\
K \arrow[u, dash] &
\end{tikzcd}$$

In this case it can be proven that X_∞ is a finitely generated $\mathbb{Z}_2$-module. We have $\mathcal{G} \cong \mathcal{O}_{\mathfrak{p}}^*$, so $\mathcal{G} = \Gamma \times \Delta$ where $\Delta = \langle 1, \delta \rangle$ is cyclic of order 2. Let $Y_\infty = X_\infty/(\delta + 1)X_\infty$.

Theorem 4.3. *Assume $L(E/H, 1) \neq 0$. Then*

$$\mathrm{ord}_{\mathfrak{p}}(\Omega_\infty(E/H)^{-1} L(\psi_{E/H}, 1)) \leq \mathrm{ord}_{\mathfrak{p}}(\#Ш(E/H)(\mathfrak{p})) + \#\mathcal{B} - 2$$

where $\mathcal{B}$ is the set of bad primes of E/H. Moreover, we have equality if and only if Y_∞ has no non-zero finite Γ-submodule.

Remark 4.4. We do not know how to prove the nonexistence of such a submodule, although it's an old theorem of Greenberg for X_∞ itself. This problem disappears for $X_0(49)$, because then $(1 + \delta)X_\infty = 0$.