

# Summary of My Thesis Work

Byoung-du Kim  
Stanford University

November 15, 2004

My areas of interest are number theory, arithmetic geometry and  $p$ -adic representation theory. One of the most sought-after problems in these areas is the Birch and Swinnerton-Dyer (BSD) conjecture. Its implication is broad, however it is a very difficult problem. Because of its difficulty, people often try to prove a weakened version, and one of the weakened versions is the parity conjecture for a Selmer group, which still provides a strong evidence for the BSD conjecture. I proved the parity conjecture for a Selmer group, which I call simply the parity conjecture in this summary, in one of the two major cases.

Those two major cases are a good ordinary reduction prime case and a good supersingular reduction prime case (each named after its reduction type). The parity conjecture for the first case was proved by J. Nekovar. However applying his method to the second case was hard, because  $p$ -Selmer groups do not behave properly in that case.

In my paper, available at <http://math.stanford.edu/~byoung>, I present the proof of the parity conjecture for good supersingular reduction primes (the second case among the two mentioned above). The proof develops new understanding of  $p$ -Selmer groups and Iwasawa theory techniques. I would like to discuss the details in the following section.

The study of the parity conjecture for a good supersingular reduction prime naturally led me to the study of plus/minus ( $\pm$ -)Selmer groups defined by S. Kobayashi. Among possible properties of  $\pm$ -Selmer groups, the algebraic functional equations of those groups over field extensions  $\mathbb{Q}(\mu_{p^\infty})$  were predicted by the analytic functional equations and the main conjecture of Iwasawa theory. In the same paper, I proved the algebraic functional equations.

I also verified the non-existence of non-trivial finite submodules of Pontryagin duals of  $\pm$ -Selmer groups. In addition, I constructed a series of elliptic curves with arbitrarily large  $\lambda^\pm$ -invariants. They will appear in [Kim2].

In subsequent sections, I describe the problems I addressed and my contribution to solving them in the order presented in the preceding paragraphs. They are independent results, and can be read in any order. In a separate research proposal, I suggest my next problems.

# 1 The Parity Theorem

In this section, I want to discuss the parity conjecture (now theorem for almost all  $p$ ) and my contribution to the solution of it. If you are not familiar with the terminology, you can see the appendix at the end of this summary. The parity conjecture is the following:

**Conjecture 1 (parity conjecture).** *For every prime  $p$ ,*

$$\text{ord}_{s=1} L_{\mathbb{Q}}(E, s) \equiv \text{corank}_{\mathbb{Z}_p} \text{Sel}_p(E/\mathbb{Q}) \pmod{2}.$$

On the other hand, the renowned BSD conjecture predicts

$$\text{ord}_{s=1} L_{\mathbb{Q}}(E, s) = \text{rank}_{\mathbb{Z}} E(\mathbb{Q})$$

Since the Tate-Shafarevich conjecture predicts that  $\text{rank}_{\mathbb{Z}} E(\mathbb{Q})$  is equal to  $\text{corank}_{\mathbb{Z}_p} \text{Sel}_p(E/\mathbb{Q})$ , the parity conjecture is a modulo 2 version of the BSD conjecture. In my paper ([Kim1]), I proved the following:

**Theorem 2 (parity theorem, B.D. Kim, 2004, [Kim1]).** *Assume  $p > 3$  is a good supersingular reduction prime for  $E$ . Then,*

$$\text{ord}_{s=1} L_{\mathbb{Q}}(E, s) \equiv \text{corank}_{\mathbb{Z}_p} \text{Sel}_p(E/\mathbb{Q}) \pmod{2}.$$

As mentioned, the same theorem for a good ordinary reduction prime was proved by Nekovar([Nek1]). However, applying Nekovar's technique to a good supersingular reduction prime case may prove to be difficult, because  $p$ -Selmer groups for a good supersingular reduction prime  $p$  do not have good properties held by the ones for a good ordinary reduction prime  $p$ .

To overcome this difficulty, in my work, I replaced the traditional Selmer groups with the plus/minus Selmer groups that are introduced in the next section. More precisely, using the orthogonality of the local conditions of  $\pm$ -Selmer groups in [Kob] and Howard's theorem on a Cassels-Tate's pairing defined on a  $\pm$ -Selmer group ([How]), I obtained the symmetric structure of  $\pm$ -Selmer groups over the anticyclotomic  $\mathbb{Z}_p$ -extension. Then, I computed the explicit corank of the plus/minus Selmer groups over anti-cyclotomic  $\mathbb{Z}_p$ -extension, using the distribution of Heegner points (see [BeDa1], [Gro], [Vat1], [Vat2]). Using this result combined with the control theorem of Kobayashi, I completed the proof of the parity conjecture.

# 2 The Algebraic Functional Equations

The algebraic functional equations are a classical example of what the main conjecture of Iwasawa theory can predict. Its origin goes back to B. Mazur ([Maz]) and possibly further. My work was mainly inspired by R. Greenberg's work ([Gre1]).

To present my work, first, I would define plus/minus( $\pm$ -)Selmer groups. Assume  $p > 3$ . Let  $\mathbb{Q}(\mu_{p^n})_p$  be the local field of  $\mathbb{Q}(\mu_{p^n})$  at the unique prime

of  $\mathbb{Q}(\mu_{p^n})$  lying over  $p$ . In his monumental paper ([Kob]), Kobayashi defined  $E^\pm(\mathbb{Q}(\mu_{p^n})_p)$  as subgroups of  $E(\mathbb{Q}(\mu_{p^n})_p)$ . Subsequently, he defined

$$\begin{aligned} Sel_p^\pm(E/\mathbb{Q}(\mu_{p^n})) &= ker(H^1(\mathbb{Q}(\mu_{p^n}), E[p^\infty])) \\ &\rightarrow \frac{H^1(\mathbb{Q}(\mu_{p^n})_p, E[p^\infty])}{E^\pm(\mathbb{Q}(\mu_{p^n})_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \cdot \prod_{\nu \nmid p} \frac{H^1(\mathbb{Q}(\mu_{p^n})_\nu, E[p^\infty])}{E(\mathbb{Q}(\mu_{p^n})_\nu) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \end{aligned}$$

Let  $Sel_p^\pm(E/\mathbb{Q}(\mu_{p^\infty})) = \varinjlim Sel_p^\pm(E/\mathbb{Q}(\mu_{p^n}))$ . Kobayashi proved that the Pontryagin dual of  $Sel_p^\pm(E/\mathbb{Q}(\mu_{p^\infty}))$  is  $\mathbb{Z}_p[[Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]$ -torsion ([Kob]).

Let an involution map  $\iota : \mathbb{Z}_p[[Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]] \rightarrow \mathbb{Z}_p[[Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]$  be induced from  $\gamma \mapsto \gamma^{-1}$  for  $\gamma \in Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ , and denote  $Hom(Sel_p^\pm(E/\mathbb{Q}(\mu_{p^\infty})), \mathbb{Q}_p/\mathbb{Z}_p)$  by  $X^\pm(E/\mathbb{Q}(\mu_{p^\infty}))$ . My result is the following:

**Theorem 3 (the algebraic functional equation, B.D. Kim, 2004, [Kim1]).**

$$X^\pm(E/\mathbb{Q}(\mu_{p^\infty}))^\iota \sim X^\pm(E/\mathbb{Q}(\mu_{p^\infty})).$$

Here,  $\sim$  means there is a  $Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ -homomorphism with a finite kernel and cokernel. Note that this equation is slightly stronger than what is predicted by the main conjecture of Iwasawa theory, since the prediction of that conjecture is about the generator of the characteristic ideal of  $X^\pm(E/\mathbb{Q}(\mu_{p^\infty}))$  whereas theorem 3 is about  $X^\pm(E/\mathbb{Q}(\mu_{p^\infty}))$  itself.

To prove it, in my paper ([Kim1]), I studied the orthogonality of the local conditions I defined to prove the parity conjecture, and I employed the technique Greenberg developed in [Gre1].

### 3 The non-existence of a non-trivial finite submodule of the Pontryagin dual of plus/minus Selmer groups

In this section and the next, I present a study about purely Iwasawa theoretical properties of  $\pm$ -Selmer groups.

Let  $p$  be a prime number, and  $\mathbb{Q}_\infty/\mathbb{Q}$  be the unique  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}$ . It is known that if  $p$  is a good ordinary reduction prime, the Pontryagin dual of  $Sel_p(E/\mathbb{Q}_\infty)$  has no non-trivial finite  $\mathbb{Z}_p[[Gal(\mathbb{Q}_\infty/\mathbb{Q})]]$ -submodule under a mild condition on  $E[p^\infty]$  (see [Gre2]) This property is known to be useful when we extract information about  $Sel_p(E/\mathbb{Q})$  from  $Sel_p(E/\mathbb{Q}_\infty)$ . My contribution is the following:

**Theorem 4 (B.D. Kim, 2004, [Kim2]).** *Let  $p > 3$  be a good supersingular prime. Then, the Pontryagin dual of  $Sel_p^\pm(E/\mathbb{Q}_\infty)$  has no non-trivial finite  $\mathbb{Z}_p[[Gal(\mathbb{Q}_\infty/\mathbb{Q})]]$ -submodule.*

## 4 The unboundedness of $\lambda^\pm$ invariants

Assume the same assumptions as in the preceding section. For a  $p$ -group  $M$ ,  $M^\vee$  denotes  $\text{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ . By Kobayashi's work and the structure theorem for modules over the Iwasawa algebra (see [Was]),

$$\text{Sel}_p^\pm(E/\mathbb{Q}_\infty)^\vee \sim \prod_{i=1}^s \mathbb{Z}_p[[X]]/(p^{n_i}) \oplus \prod_{j=1}^{t^\pm} \mathbb{Z}_p[[X]]/(f_j^\pm(X))$$

where each  $f_j^\pm(X)$  is a distinguished polynomial ( $\sim$  means there is a  $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ -homomorphism with a finite kernel and cokernel).

Then, define  $\mu = \sum_{i=1}^s n_i$ ,  $\lambda^\pm = \sum_{j=1}^{t^\pm} \text{deg}(f_j^\pm(X))$ . The question is whether  $\lambda^\pm$  can be arbitrarily large. In a comment in [GrVa], Greenberg and Vatsal gave an affirmative answer to a similar question for  $p$ -Selmer groups when  $p$  is a good ordinary reduction prime.

In [Kim2], I construct a series of elliptic curves whose  $\lambda^\pm$ -invariants for  $\pm$ -5-Selmer groups are arbitrarily large, and  $\mu$ -invariants of them are zero, using Rubin and Silverberg's result about a series of elliptic curves with the same Galois representation modulo 3 and 5 ([RuSi]) and Greenberg's result on bad reduction ([Gre2]).

## 5 Appendix-Terminology

Suppose  $E$  is an elliptic curve defined over  $\mathbb{Q}$ . Thus, we can assume  $E$  is a global minimal Weierstrass model. Fix a prime  $p$ . Then, the group of  $p$ -power torsions  $E[p^\infty]$  is isomorphic to  $(\mathbb{Q}_p/\mathbb{Z}_p)^2$ , as groups.

On the other hand, when  $\hat{E}$  is an elliptic curve defined over  $\mathbb{F}_p (= \mathbb{Z}/p\mathbb{Z})$ ,  $\hat{E}[p^\infty]$  is isomorphic to either  $\mathbb{Q}_p/\mathbb{Z}_p$  or 0 as groups.

Now, once again, suppose  $E$  is an elliptic curve defined over  $\mathbb{Q}$  (assumed to be a global minimal Weierstrass model). Then,  $E$  can be reduced to  $\tilde{E}$ , a curve over  $\mathbb{F}_p$ . For all but finitely many primes  $p$ ,  $\tilde{E}$  is non-singular (therefore an elliptic curve over  $\mathbb{F}_p$ ). We say such a prime  $p$  has good reduction. The remaining primes are said to have bad reduction. They are, in turn, either additive bad reduction or multiplicative bad reduction.

Suppose  $p$  has good reduction. If  $\tilde{E}[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p$ , then  $p$  is called a good ordinary reduction prime. Otherwise,  $p$  is called a good supersingular reduction prime.

We now define a  $p$ -Selmer group as follows:

$$\text{Sel}_p(E/\mathbb{Q}) = \ker \left( H^1(\mathbb{Q}, E[p^\infty]) \rightarrow \prod_{l: \text{a prime of } \mathbb{Q}, \text{ or } \infty} \frac{H^1(\mathbb{Q}_l, E[p^\infty])}{E(\mathbb{Q}_l) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

On the analytic side, we also define an  $L$ -function:

$$L_{/\mathbb{Q}}(E, s) = \prod_{l: \text{a prime of } \mathbb{Q}} L_l(l^{-s})^{-1}$$

where

$$L_l(T) = 1 - a_l T + lT^2, \quad a_l = l + 1 - \#\tilde{E}_l(\mathbb{F}_l)$$

if  $l$  is a good reduction prime. We define  $L_l(T)$  in a different way for bad reduction primes.

Since  $E$  is defined over  $\mathbb{Q}$ , by the well-known result of A. Wiles *et al.*, it is known that  $L_{/\mathbb{Q}}(E, s)$  has a meromorphic continuation to the entire complex plane.

Finally, note that  $E(\mathbb{Q})$  has a group structure, and as a group, it is known to be finitely generated by the Mordell-Weil theorem. The famous BSD conjecture claims that the order of zero of  $L_{/\mathbb{Q}}(E, s)$  at  $s = 1$  is equal to the rank of  $E(\mathbb{Q})$ .

## References

- [BeDa1] Bertolini, M.; Darmon, H. *Kolyvagin's descent and Mordell-Weil groups over ring class fields*. J. Reine Angew. Math. **412** (1990), 63–74.
- [Gre1] Greenberg, R. *Iwasawa theory for  $p$ -adic representations*, Algebraic number theory. Papers in honor of K. Iwasawa on the occasion of his 70th birthday on September 11, 1987. Edited by J. Coates, R. Greenberg, B. Mazur and I. Satake. Advanced Studies in Pure Mathematics, **17**. Academic Press, Inc., Boston, MA; Kinokuniya Company Ltd., Tokyo, 1989.
- [Gre2] Greenberg, R. *Iwasawa theory for elliptic curves. (51–144) Arithmetic theory of elliptic curves. Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12–19, 1997. Edited by C. Viola*. Lecture Notes in Mathematics, **1716**. Springer-Verlag, Berlin; Centro Internazionale Matematico Estivo (C.I.M.E.), Florence, 1999.
- [Gro] Gross, B. *Heights and the special values of  $L$ -series*. Number theory (Montreal, Que., 1985), 115–187, CMS Conf. Proc., 7, Amer. Math. Soc., Providence, RI, 1987.
- [GrVa] Greenberg, R.; Vinayak, V. *On the Iwasawa invariants of elliptic curves*. Invent. Math. **142**. (2000), no. 1, 17–63.
- [How] Howard, B. *Iwasawa theory of Heegner points on abelian varieties of  $GL_2$  type* Duke Math. J. **124** (2004), no. 1, 1–45.
- [Kim1] Kim, B.D. *The Parity Theorem of Elliptic Curves and Algebraic Functional Equations at Primes with Supersingular Reduction*. preprint, see <http://math.stanford.edu/~byoung>
- [Kim2] Kim, B.D. *Iwasawa Theoretic Properties of Plus/Minus Selmer Groups* in preparation
- [Kob] Kobayashi, S. *Iwasawa theory for elliptic curves at supersingular primes*. Invent. Math. **152** (2003), no. 1, 1–36.

- [Maz] Mazur, Barry *Rational points of abelian varieties with values in towers of number fields*. *Invent. Math.* **18** (1972), 183–266.
- [Nek1] Nekovar, J. *On the parity of ranks of Selmer groups. II*. *C. R. Acad. Sci. Paris Sr. I Math.* **332** (2001), no. 2, 99–104.
- [Nek2] Nekovar, J. *Selmer complexes* preprint.
- [RuSi] Rubin, K.; Silverberg, A. *Families of elliptic curves with constant mod  $p$  representations*. *Elliptic curves, modular forms, & Fermat’s last theorem* (Hong Kong, 1993), 148–161, *Ser. Number Theory, I*, Internat. Press, Cambridge, MA, 1995.
- [Vat1] Vatsal, V. *Uniform distribution of Heegner points*. *Invent. Math.* **148** (2002), no. 1, 1–46.
- [Vat2] Vatsal, V. *Special values of anticyclotomic  $L$ -functions*. *Duke Math. J.* **116** (2003), no. 2, 219–261.
- [Was] Washington, L. *Introduction to Cyclotomic Fields. Second edition*. *Graduate Texts in Mathematics*, **83**. Springer-Verlag, New York, 1997.