ELLIPTIC CURVES OF RANK ZERO SATISFYING THE p-PART OF THE BIRCH AND SWINNERTON-DYER CONJECTURE

DONGHO BYEON AND NAYOUNG KIM

Abstract. Let $p \in \{3, 5, 7\}$ and $E/\mathbb{Q}$ an elliptic curve with a rational point P of order p. Let D be a square-free integer and E_D the D-quadratic twist of E. Vatsal [V] found some conditions such that E_D has (analytic) rank zero and Frey [F] found some conditions such that the p-Selmer group of E_D is trivial. In this paper, we will consider a family of E_D satisfying both of the conditions of Vatsal and Frey and show that the p-part of the Birch and Swinnerton-Dyer conjecture is true for these elliptic curves E_D. As a corollary we will show that there are infinitely many elliptic curves $E/\mathbb{Q}$ such that for a positive portion of D, E_D has rank zero and satisfies the 3-part of the Birch and Swinnerton-Dyer conjecture. Previously only a finite number of such curves were known, due to James [J].

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E, given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$ and $L(E, s)$ its Hasse-Weil L-function. Let D be a square-free integer and $h(D)$ the class number of the quadratic field $\mathbb{Q}(\sqrt{D})$. Let E_D be the D-quadratic twist of E which is given by

$$E_D : y^2 = x^3 + b_2Dx^2 + 8b_4D^2x + 16b_6D^3,$$

where $b_2 := a_1^2 + 4a_2$, $b_4 := 2a_4 + a_1a_3$, $b_6 := a_3^2 + 4a_6$.

If E_D has analytic rank zero, the Birch and Swinnerton-Dyer Conjecture predicts that

$$\frac{L(E_D, 1)}{\Omega_{E_D}} = \frac{\#Ш(E_D/\mathbb{Q}) \prod_q c_q(E_D/\mathbb{Q})}{\#E_D(\mathbb{Q})^2_{\text{tor}}},$$

where $\Omega_{E_D}, Ш(E_D/\mathbb{Q})$ and $c_q(E_D/\mathbb{Q})$ denote the real period, Tate-Shafarevich group and local Tamagawa number at $q|N_{E_D}$ of E_D, respectively.

In [V] Vatsal found some conditions such that E_D has (analytic) rank zero and in [F], [A-B-F] Frey found some conditions such that the p-Selmer group of E_D is trivial. In this paper, we will consider a family of E_D satisfying both of the conditions of Vatsal and Frey and show that the p-part of the Birch and Swinnerton-Dyer conjecture is true for these elliptic curves E_D.

Theorem 1.1. *Let $p \in \{3, 5, 7\}$ and $E/\mathbb{Q}$ be an optimal elliptic curve with a rational point P of order p and good, ordinary reduction at p. Suppose that $2, 3 \nmid N_E$, E has no*

additive reduction, and $\mathrm{ord}_q(j_E) \equiv 0 \pmod p$ *for each odd prime* $q|N_E$ *with* $q \equiv -1 \pmod p$. *Then*

$$\mathrm{ord}_p\left(\frac{L(E_D,1)}{\Omega_{E_D}}\right) = \mathrm{ord}_p\left(\frac{\#Ш(E_D/\mathbb{Q})\prod_q c_q(E_D/\mathbb{Q})}{\#E_D(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0,$$

for every negative square-free integer D *prime to* pN_E *such that* $h(D) \not\equiv 0 \pmod p$ *and*

$$\left(\frac{D}{q}\right) = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction at } q, \\ 1 & \text{if } E \text{ has nonsplit multiplicative reduction at } q. \end{cases}$$

As a corollary we will show that there are infinitely many elliptic curves $E/\mathbb{Q}$ such that for a positive portion of D, E_D has rank zero and satisfies the 3-part of the Birch and Swinnerton-Dyer conjecture. Previously only a finite number of such curves were known, due to James [J].

Corollary 1.2.
(1) *For* $p = 3$, *there are infinitely many elliptic curves* $E/\mathbb{Q}$ *satisfying the conditions of Theorem 1.1, and for these elliptic curves we have*

$$\#\{-X < D < 0 : D \text{ is square-free and } \mathrm{ord}_3\left(\frac{L(E_D,1)}{\Omega_{E_D}}\right) = \mathrm{ord}_3\left(\frac{\#Ш(E_D/\mathbb{Q})\prod_q c_q(E_D/\mathbb{Q})}{\#E_D(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0\} \gg_E X.$$

(2) *For* $p = 5$, *there are infinitely many elliptic curves* $E/\mathbb{Q}$ *satisfying the conditions of Theorem 1.1, and for these elliptic curves if there is at least one odd* D_0 *satisfying the further conditions of Theorem 1.1 such that at least one prime factor of* D_0 *is larger than* $\frac{[\Gamma_0(1):\Gamma_0(4\cdot 5^2\cdot(4N_E)^4)]}{8} + 1$, *we have*

$$\#\{-X < D < 0 : D \text{ is square-free and } \mathrm{ord}_5\left(\frac{L(E_D,1)}{\Omega_{E_D}}\right) = \mathrm{ord}_5\left(\frac{\#Ш(E_D/\mathbb{Q})\prod_q c_q(E_D/\mathbb{Q})}{\#E_D(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0\} \gg_E \frac{\sqrt{X}}{\log X}.$$

2. Proof of Theorem 1.1

In [V], Vatsal proved the following theorem.

Theorem 2.1. [Corollary (3.4), V]) *Let* p *be an odd prime and* $E/\mathbb{Q}$ *be an elliptic curve with a rational point* P *of order* p *and good, ordinary reduction at* p. *Assume that each prime of additive reduction is congruent to* 1 *modulo* p. *Then* $L(E_D,1) \neq 0$ *for every negative square-free integer* D *prime to* N_E *such that* $h(D) \not\equiv 0 \pmod p$ *and*

$$\left(\frac{D}{q}\right) = \begin{cases} -1 & \text{if } E \text{ has additive or split multiplicative reduction at } q; \\ -q \pmod p & \text{if } E \text{ has nonsplit multiplicative reduction at } q. \end{cases}$$

Remark. In fact, Vatsal [Theorem (2.10) and Theorem (3.3), V] proved that for E_D in Theorem 1.1,

$$\mathrm{ord}_p\left(\tau(\chi_D)\frac{L(E_D,1)}{(-2\pi i)\Omega_f^-}\right)=0\ ,$$

where $\tau(\chi_D)$ is the Gauss sum of the quadratic character χ_D and Ω_f^- is the canonical period of the cuspform f corresponds to E. If E is optimal, then the imaginary period Ω_E^- of E is equal to $(-2\pi i)\Omega_f^-$ up to a p-adic unit (See [Proposition (3.1), G-V]). Pal [Proposition 2.5 and Theorem 3.2, Pa] proved that $\Omega_{E_D}=\frac{\tilde{u}}{\sqrt{D}}c_\infty(E_D)\Omega_E^-$, where $c_\infty(E_D)=1$ or 2 is the number of connected components of $E_D(\mathbb{R})$ and $\tilde{u}$ is a rational number not divisible by p. So Ω_E^- is equal to $\sqrt{D}\Omega_{E_D}$ up to a p-adic unit. Since $\tau(\chi_D)=\sqrt{D}$, we have that if E is optimal, then

$$\mathrm{ord}_p\left(\frac{L(E_D,1)}{\Omega_{E_D}}\right)=0\ .$$

The following theorem is an effective form of [Proposition 1.5, A-B-F].

Theorem 2.2. ([A-B-F]) *Let p be an odd prime and $E/\mathbb{Q}$ be an elliptic curve with a rational point P of order p and good reduction at p. Suppose that $2\nmid N_E$, E has no additive reduction, and $\mathrm{ord}_q(j_E)\equiv 0 \pmod p$ for each odd prime $q|N_E$ with $q\equiv -1 \pmod p$. Then the p-Selmer group $S(E_D/\mathbb{Q})_p$ of E_D is trivial for every negative square-free integer D prime to pN_E such that $h(D)\not\equiv 0 \pmod p$ and*

$$\left(\frac{D}{q}\right)=\begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction at } q;\\ 1 & \text{if } E \text{ has nonsplit multiplicative reduction at } q.\end{cases}$$

Lemma 2.3. *Let p be an odd prime and $E/\mathbb{Q}$ be an elliptic curve with a rational point P of order p and good reduction at p. Assume that E has no additive reduction. For a prime $q(\neq 2,3)|N_E$,*

(1) *if P reduces to a singular point in $\tilde{E}(\mathbb{F}_q)$, then E has split multiplicative reduction at q,*
(2) *if P reduces to a non-singular point in $\tilde{E}(\mathbb{F}_q)$, then*

$$q\equiv\begin{cases} 1 \pmod p & \text{if and only if } E \text{ has split multiplicative reduction at } q;\\ -1 \pmod p & \text{if and only if } E \text{ has nonsplit multiplicative reduction at } q.\end{cases}$$

Proof. We may assume $P=(0,0)$ is a rational torsion point of order p. If $P=(0,0)$ is a singular point in $\tilde{E}(\mathbb{F}_q)$, then we easily see that $a_2=a_3=a_4=a_6=0$. Since $y^2+a_1xy-x^3=y(y+a_1x)-x^3$, E has split multiplicative reduction at q. This proves the first part of the lemma. If P is a non-singular point in $\tilde{E}(\mathbb{F}_q)$, then p divides the order of the non-singular part $\tilde{E}(\mathbb{F}_q)_{ns}$ of $\tilde{E}(\mathbb{F}_q)$. So the second part comes from the order of $\tilde{E}(\mathbb{F}_q)_{ns}$, which is equal to $q-1$ if E has split multiplicative reduction at q and is equal to $q+1$ if E has nonsplit multiplicative reduction at q (See [p.59, Mi]). □

From Theorem 2.1, Theorem 2.2 and Lemma 2.3, we obtain the following proposition.

Proposition 2.4. *Let p be an odd prime and $E/\mathbb{Q}$ be an elliptic curve with a rational point P of order p and good, ordinary reduction at p. Suppose that $2, 3 \nmid N_E$, E has no additive reduction, and $\mathrm{ord}_q(j_E) \equiv 0 \pmod{p}$ for each odd prime $q|N_E$ with $q \equiv -1 \pmod{p}$. Then the p-Selmer group $S(E_D/\mathbb{Q})_p$ of E_D is trivial and $L(E_D, 1) \neq 0$ for every negative square-free integer D prime to pN_E such that $h(D) \not\equiv 0 \pmod{p}$ and*

$$\left(\frac{D}{q}\right) = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction at } q; \\ 1 & \text{if } E \text{ has nonsplit multiplicative reduction at } q. \end{cases}$$

Lemma 2.5. ([p.59, Mi]) *Let $l \neq 2, 3$ be a prime, and $E/\mathbb{Q}$ be an elliptic curve given by*

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Z}.$$

Assume that this equation is minimal at l and E has bad reduction at l. Then

$$-2ab = \begin{cases} 0 \text{ in } \mathbb{F}_l & \text{if } E \text{ has additive reduction at } l, \\ a \text{ square in } \mathbb{F}_l & \text{if } E \text{ has split multiplicative reduction at } l, \\ a \text{ non-square in } \mathbb{F}_l & \text{if } E \text{ has nonsplit multiplicative reduction at } l. \end{cases}$$

From Lemma 2.5, we can prove the following lemma which is needed to compute Tamagawa numbers of E_D in the proof of Theorem 1.1.

Lemma 2.6. *Let $E/\mathbb{Q}$ be an elliptic curve. Assume that E has no additive reduction. Then E_D has nonsplit multiplicative reduction at $q(\neq 2, 3)|N_E$ for every negative square-free integer D such that*

$$\left(\frac{D}{q}\right) = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction at } q; \\ 1 & \text{if } E \text{ has nonsplit multiplicative reduction at } q. \end{cases}$$

Proof. By assumption $q \neq 2, 3$, we may assume that E has a minimal Weierstrass equation at q of the form $y^2 = x^3 + ax + b$ for some $a, b \in \mathbb{Z}$. Then E_D is given by: $y^2 = x^3 + aD^2x + bD^3$ and this equation is also minimal at q. If E has split multiplicative reduction at q, then $(\frac{-2abD^5}{q}) = (\frac{-2ab}{q})(\frac{D}{q}) = 1 \cdot (-1) = -1$. If E has nonsplit multiplicative reduction at q, then $(\frac{-2abD^5}{q}) = (\frac{-2ab}{q})(\frac{D}{q}) = (-1) \cdot 1 = -1$. Thus E_D always has nonsplit multiplicative reduction at q by Lemma 2.5. □

Proof of Theorem 1.1. Suppose that E_D is the curve in Theorem 1.1. Then the p-Selmer group $S(E_D/\mathbb{Q})_p$ of E_D is trivial by Proposition 2.4. Thus $\mathrm{rank}(E_D(\mathbb{Q})) = 0$, $\mathrm{ord}_p(\#E_D(\mathbb{Q})_{\mathrm{tor}}) = 0$, and $\mathrm{ord}_p\big(\#Ш\big(E_D/\mathbb{Q}\big)\big) = 0$, by the usual Kummer exact sequence. Furthermore since E is optimal, we have $\mathrm{ord}_p\big(\frac{L(E_D,1)}{\Omega_{E_D}}\big) = 0$ by the remark below Theorem 2.1. Since the discriminant $\Delta(E_D)$ of E_D is equal to $2^{12} \cdot D^6 \cdot \Delta(E)$, we need to compute $c_q(E_D/\mathbb{Q})$ for primes $q \,|\, 2DN_E$. By Lemma 2.6, E_D has nonsplit multiplicative reduction at $q|N_E$, thus $c_q(E_D/\mathbb{Q}) = 1$ or 2 for $q \,|\, N_E$ (See [Corollary 15.2.1, Appendix C, S]). By the case 6 of Tate's algorithm in [T], we have $c_q(E_D/\mathbb{Q}) = 1, 2$, or 4 for $q \,|\, D$. If E_D has bad reduction at 2, we have $c_2(E_D/\mathbb{Q}) = 1$ by direct computation for D in a set of representatives of $\mathbb{Q}_2/(\mathbb{Q}_2^{\times})^2$. Finally we have

$$\mathrm{ord}_p\left(\frac{L(E_D, 1)}{\Omega_{E_D}}\right) = \mathrm{ord}_p\left(\frac{\#Ш(E_D/\mathbb{Q}) \prod_q c_q(E_D/\mathbb{Q})}{\#E_D(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0.$$

□

3. Proof of Corollary 1.2

3.1. **Proof of Corollary 1.2 (1).** Let $\Phi(x) \in \mathbb{Z}[x]$ be a polynomial of degree k with positive leading coefficient. Then Perelli [Pe] and Brüdern, Kawada and Wooley [B-K-W] proved that almost all values of the polynomial $2\Phi(n)$ are the sum of two primes. With slight modification, we obtain the following proposition.

Proposition 3.1. ([B-K-W] or [B-J-K]) *Let $\Phi(x) \in \mathbb{Z}[x]$ be a polynomial of degree k with positive leading coefficient and let A, B be positive odd integers such that $\gcd(A, B) = 1$. Let $\mathcal{E}_k(N; \Phi)$ denote the number of integers $n \in [1, N]$ for which the equation*

$$2\Phi(n) = As + Bt$$

has no solution in primes s, t. Then there is an absolute constant $c > 0$ such that

$$\mathcal{E}_k(N; \Phi) \ll_\Phi N^{1-c/k}.$$

Now we can prove Corollary 1.2 (1).

Proof of Corollary 1.2 (1). Let $p_1, \cdots, p_r$ and $q_1, \cdots, q_{r'}$ be different primes ($\neq 2, 3$) such that $q_i \equiv 1 \pmod 3$ for all $i = 1, \cdots, r'$. Put $\Phi(x) := (3(2x+1)+1)^3/2 \in \mathbb{Z}[x]$ and $A := 27p_1 \cdots p_r$, $B := q_1 \cdots q_{r'}$. Then there are infinitely many positive integers n such that

$$2\Phi(n) = (3(2n+1)+1)^3 = 27p_1 \cdots p_r s + q_1 \cdots q_{r'} t$$

for some primes s, t, by Proposition 3.1. We may assume that $s, t \neq 2, 3, p_i, q_j$. For such n, s, t, put $a := 3(2n+1)+1$ and $b := p_1 \cdots p_r s$. Let $E(a, b)$ be the elliptic curve defined by

$$E(a, b) : y^2 + axy + by = x^3.$$

Then $E(a, b)$ has the point $P = (0, 0)$ of order 3 and the discriminant $\Delta(E(a, b))$ of $E(a, b)$ is

$$\Delta(E(a, b)) = b^3(a^3 - 27b) = p_1^3 \cdots p_r^3 s^3 q_1 \cdots q_{r'} t.$$

We can easily check that $2, 3 \nmid N_{E(a,b)}$, $E(a, b)$ has no additive reduction, and $\mathrm{ord}_q(j_{E(a,b)}) \equiv 0 \pmod 3$ for each odd prime $q | N_E$ with $q \equiv -1 \pmod 3$.

Let $C(E)$ denote the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in the isogeny class $\mathcal{C}$ of an elliptic curve E. For a prime q, let $C_q(E)$ be the number of $\mathbb{Q}$-isomorphism classes of elliptic curves q-power isogenous to E. Then we have the product formula (See [K])

$$C(E) = \prod_q C_q(E).$$

Since b is not a cubic number, the elliptic curve $E'(a, b) = E(a, b)/ < P >$ has no rational point of order 3 (See [Theorem 1.1, H]). So there is no 3-isogeny from $E'(a, b)$ to an elliptic curve E'' whose kernel is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Since $\Delta(E(a, b))$ is not a

cubic number, there is no 3-isogeny from an elliptic curve E" to $E(a,b)$ whose kernel is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ (See [Section 1, H]). These imply that the set of $\mathbb{Q}$-isomorphism classes of elliptic curves 3-power isogenous to E is $\{E(a,b),\ E'(a,b)\}$ and $C_3(E(a,b)) = 2$. Using the duplication formula, we can show that $E(a,b)$ has no rational points of order 2. So $C_2(E(a,b)) = 1$. For any other prime $q \neq 2,3$, if there is an elliptic curve E'' which is q-isogeneous to $E(a,b)$, then E'' or $E(a,b)$ has a rational point of order $3q$. But it is impossible. So $C_q(E(a,b)) = 1$ for any other prime $q \neq 2,3$. Thus by the product formula we have $C(E(a,b)) = 2$ and the isogeny class of $E(a,b)$ over $\mathbb{Q}$ is $\{E(a,b),\ E'(a,b)\}$. Since the optimal curve in the isogeny class should have a rational point of order 3 (See [Theorem 1.2, D]), $E(a,b)$ is optimal. Thus $E(a,b)$ satisfies the conditions of Theorem 1.1, for $p = 3$. The number of D such that $-X < D < 0$, satisfying the further conditions of Theorem 1.1 is $\gg_E X$, by the work of Davenport and Heilbronn [D-H] as improved by Nakagawa and Horie [N-H]. Hence we deduce Corollary 1.2(1). □

3.2. **Proof of Corollary 1.2 (2).** In [I], Iwaniec proved the following proposition.

Proposition 3.2. ([I]) *Let $F(x,y) = Ax^2 + Bxy + Cy^2$ be an irreducible quadratic form and n, m, r, r' be integers such that $nm \neq 0$. If $F(mx + r, ny + r')$ represents an integer prime to any arbitrary given non-zero integer , then*

$$\sum_{\substack{w \leq N\,:\,primes \\ w = F(mx+r, ny+r')}} 1 \quad \gg \quad \frac{N}{\log N}.$$

Now we can prove Corollary 1.2 (2).

Proof of Corollary 1.2 (2). Put $F(x,y) := x^2 - 11xy - y^2$. Then there are infinitely many primes of the form $F(30x + 1, 30y - 1)$, by Proposition 3.2. Such a w is necessarily congruent to 1 (mod 5). For such x, y, put $u := 30x + 1$, and $v := 30y - 1$. Let $E(u,v)$ be an elliptic curve defined by:

$$E(u,v) : y^2 + (u - v)xy - u^2vy = x^3 - uvx^2.$$

Then $E(u,v)$ has the point $P = (0,0)$ of order 5 and the discriminant $\Delta(E(u,v))$ is

$$\Delta(E(u,v)) = u^5v^5(v^2 - 11uv - u^2) = -u^5v^5w.$$

We can easily check that $2, 3 \nmid N_{E(u,v)}$, $E(u,v)$ has no additive reduction, and $\mathrm{ord}_q(j_{E(u,v)}) \equiv 0 \pmod 5$ for each odd prime $q | N_E$ with $q \equiv -1 \pmod 5$.

Using the result in [Section 2, H], we can show that the elliptic curve $E'(u,v) = E(u,v)/ < P >$ has no rational point of order 5 and there is no 5-isogeny from an elliptic curve E'' to $E(u,v)$ whose kernel is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. These imply that the set of $\mathbb{Q}$-isomorphism classes of elliptic curves 5-power isogenous to E is $\{E(u,v),\ E'(u,v)\}$ and $C_5(E(u,v)) = 2$. By the same argument to the case $p = 3$, we have $C_q(E(u,v)) = 1$ for any other prime $q \neq 5$. Thus by the product formula we have $C(E(u,v)) = 2$ and the isogeny class of $E(u,v)$ over $\mathbb{Q}$ is $\{E(u,v),\ E'(u,v)\}$. Since the optimal curve in the isogeny class should have a rational point of order 5 (See [Theorem 1.2, D]), $E(u,v)$ is optimal. Thus $E(u,v)$ satisfies the conditions of Theorem 1.1, for $p = 5$. If there is at

least one odd D_0 satisfying the further conditions of Theorem 1.1 such that at least one prime factor of D_0 is larger than $\frac{[\Gamma_0(1):\Gamma_0(4\cdot 5^2\cdot(4N_E)^4)]}{8}+1$, then the number of D such that $-X<D<0$, satisfying the further conditions of Theorem 1.1 is $\gg_E \frac{\sqrt{X}}{\log X}$, by [Theorem 13, J-O]. Hence we deduce Corollary 1.2(2). □

Finally we add the following remark suggested by the referee.

Remark.

(1) Since the p-part of the Birch and Swinnerton-Dyer conjecture is invariant under isogenies [C], Theorem 1.1 implies that if $E'/\mathbb{Q}$ is an elliptic curve which is $\mathbb{Q}$-isogeneous to $E/\mathbb{Q}$ satisfying the conditions of Theorem 1.1, then

$$\mathrm{ord}_p\left(\frac{L(E'_D,1)}{\Omega_{E'_D}}\right)=\mathrm{ord}_p\left(\frac{\#Ш(E'_D/\mathbb{Q})\prod_q c_q(E'_D/\mathbb{Q})}{\#E'_D(\mathbb{Q})^2_{\mathrm{tor}}}\right),$$

for every negative square-free integer D satisfying the conditions of Theorem 1.1.

(2) In [p.415, V], Vatsal remarks "It would be interesting to compare Frey's results to ours more explicitly; we note only that we can recover the triviality of the 3-Selmer groups in the present situation by invoking the theorem of Kolyvagin". However it seems that the theorem of Kolyvagin using Euler system can not be applied to this situation where E has a rational p-torsion point, because the mod p Galois representation for E_D will not be surjective when E has a rational p-torsion point.

Acknowledgement The authors would like to thank the referee for many valuable suggestions.

References

[A-B-F] J. A. Antoniadis, M. Bungert and G. Frey, *Properties of twists of elliptic curves*, J. Reine Angew. Math. 405 (1990), 1-28.

[B-K-W] J. Brüdern, K. Kawada and T. D. Wooley, *Additive representation in thin sequence II: The binary Goldbach problem*, Mathematica 47 (2000), 117-125.

[B-J-K] D. Byeon, D. Jeon and C.H. Kim, *Rank-one quadratic twists of an infinite family of elliptic curves*, J. Reine Angew. Math. 633 (2009), 67-76.

[C] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. 217 (1965), 180-199.

[D-H] H. Davenport and H. Heilbronn, *On the density of disciminants of cubic fields II*, Proc. Roy. Soc. London Ser. A 322 (1971), 405-420.

[D] N. Dummigan, *Rational torsion on optimal curves,* Int. J. Number Theory 1 (2005), 513-531.

[F] G. Frey, *On the Selmer group of twists of elliptic curves with $\mathbb{Q}$-rational torsion points*, Canad. J. Math. 40 (1988), 649-665.

[G-V] R. Greenberg and V. Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. 142 (2000), 17-63.

[H] T. Hadano, *Elliptic curves with a torsion point,* Nagoya Math. J. 66 (1977), 99-108.

[I] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday, V. Acta Arith. 24 (1973/74), 435-459.

[J] K. James, *Elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture mod* 3, J. Number Theory 76 (1999), 16-21.

[J-O] K. James and K. Ono, *Selmer groups of quadratic twists of elliptic curves*, Math. Ann. 314 (1999), 1-17.

[K] M. Kenku, *On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class*, J. Number Theory 15 (1982), 199-202.

[Mi] J. S. Milne, *Elliptic curves*, Book Surge Publishers, Charleston, SC (2006).

[N-H] J. Nakagawa and K. Horie, *Elliptic curves with no torsion points*, Proc. Amer. Math. Soc. 104 (1988), 20-25.
[Pa] V. Pal, *Periods of quadratic twists of elliptic curves*, Proc. Amer. Math. Soc. 140 (2012), 1513-1525.
[Pe] A. Perelli. *Goldbach numbers represented by polynomials*, Rev. Mat. Iberoamericana 12 (1996), 477-490.
[S] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, New York : Springer-Verlag (1985).
[T] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, In: Modular functions of one variable IV, Lecture Notes in Math. 476, New York: Springer-Verlag (1975), 33-52.
[V] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. 98 (1999), 397-419.

Department of Mathematics, Seoul National University, Seoul, 151-747, Republic of Korea
E-mail address: dhbyeon@math.snu.ac.kr

Department of Mathematics, Seoul National University, Seoul, 151-747, Republic of Korea
E-mail address: na0@snu.ac.kr