A CONJECTURE OF GROSS AND ZAGIER: CASE $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ OR $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$

DONGHO BYEON, TAEKYUNG KIM AND DONGGEON YHEE

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N, c the Manin constant of E, and m the product of Tamagawa numbers of E at prime divisors of N. Let K be an imaginary quadratic field where all prime divisors of N split in K, P_K the Heegner point in $E(K)$, and III(E/K) the Shafarevich-Tate group of E over K. Let $2u_K$ be the number of roots of unity contained in K. Gross and Zagier conjectured that if P_K has infinite order in $E(K)$, then the integer $c \cdot m \cdot u_K \cdot |\mathrm{III(E/K)}|^{\frac{1}{2}}$ is divisible by $|E(\mathbb{Q})_{\mathrm{tor}}|$. In this paper, we show that this conjecture is true if $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N, c the Manin constant of E and $m = \prod_{p|N} m_p$, where m_p is the Tamagawa number of E at a prime divisor p of N. Let K be an imaginary quadratic field where all prime divisors of N split in K, P_K the Heegner point in $E(K)$ and III(E/K) the Shafarevich-Tate group of E over K. Let $2u_K$ be the number of roots of unity contained in K. In [GZ], Gross and Zagier conjectured

Conjecture. ([GZ, p. 311, (2.3) Conjecture]) *If P_K has infinite order in $E(K)$, then the integer $c \cdot m \cdot u_K \cdot |\mathrm{III(E/K)}|^{\frac{1}{2}}$ is divisible by $|E(\mathbb{Q})_{\mathrm{tor}}|$.*

Rational torsion subgroups of elliptic curves E over $\mathbb{Q}$ are completely classified by Mazur [Ma]: $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to one of the following 15 groups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{for } 1 \le n \le 10,\ n = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} & \text{for } n = 2, 4, 6, 8. \end{cases}$$

From [Lo, Proposition 1.1], we know that the conjecture is true when $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for $5 \le n \le 10$, $n = 12$ or to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ (cf. [BKY, Theorem 1.1]). In [BKY, Theorem 1.2], we proved that the conjecture is true when $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

So the only remaining cases for the validity of the conjecture are those when $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to the following 5 groups: $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

In this paper, we prove the following theorem.

Theorem 1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. Then the conjecture is true.*

2. Preliminaries

The following two lemmas are needed to compute the Tamagawa number m_p of E at a prime divisor p of N.

Lemma 2.1. (i) *If E has additive reduction at p, then the prime to p part of $|E(\mathbb{Q})_{\text{tor}}|$ divides m_p.*
(ii) *Suppose that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{Q})$. If $p \neq 2$ is a prime at which E has multiplicative reduction, then $2 \mid m_p$.*

Proof. Consider the exact sequence (cf. [Si, VII Proposition 2.1])

$$0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to \widetilde{E}_{\text{ns}}(\mathbb{F}_p) \to 0.$$

We note that every element of finite order in $E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p)$ has order that is a power of p, where $\hat{E}$ is the formal group associated to E (cf. [Si, IV Proposition 3.2]).
(i) If E has additive reduction at p, every element in $\widetilde{E}_{\text{ns}}(\mathbb{F}_p) \subset \overline{\mathbb{F}}_p^+$ (cf. [Si, VII Proposition 5.1]) has order that is a power of p. From the above exact sequence, we see that the prime to p part of $E(\mathbb{Q})_{\text{tor}}$ has trivial intersection with $E_0(\mathbb{Q}_p)$. Thus the prime to p part of $E(\mathbb{Q})_{\text{tor}}$ injects into $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ and the prime to p part of $|E(\mathbb{Q})_{\text{tor}}|$ divides $m_p = |E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)|$.
(ii) If E has multiplicative reduction at p, $\widetilde{E}_{\text{ns}}(\mathbb{F}_p) \subset \overline{\mathbb{F}}_p^*$ (cf. [Si, VII Proposition 5.1]) is cyclic. Suppose $p \neq 2$. From the above exact sequence, we see that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{Q})$ has proper intersection with $E_0(\mathbb{Q}_p)$, i.e. $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \not\subseteq E_0(\mathbb{Q}_p)$. This implies that $2 \mid m_p$.

□

Lemma 2.2. *For $\lambda \in \mathbb{Q}$, let E_λ be an elliptic curve defined by the Weierstrass equation*

$$E_\lambda : y^2 + xy - \lambda y = x^3 - \lambda x^2, \tag{1}$$

with discriminant $\Delta = \lambda^4(1+16\lambda) \neq 0$. If p is a prime such that $\mathrm{ord}_{\mathrm{p}}\,\lambda > 0$, then E_λ has split multiplicative reduction of type $\mathrm{I}_{4\mathrm{ord}_{\mathrm{p}}\,\lambda}$. So $4 \mid m_p$.

Proof. See [Si, Table 15.1] and the proof of [Lo, Proposition 2.4]. □

The following two lemmas are needed to find some special elliptic curves.

Lemma 2.3. *Let u, v, w be positive integers and let p, q be odd primes. Then the system of equations*

$$2^u + 1 = p^v \text{ (resp. } 2^u - 1 = p^v); \quad 2^{u+1} + 1 = q^w \text{(resp. } 2^{u+1} - 1 = q^w) \tag{2}$$

has no other solutions than
$(p, q, u, v, w) = (3, 5, 1, 1, 1)$, $(5, 3, 2, 1, 2)$ or $(3, 17, 3, 2, 1)$ (resp. (p, q, u, v, w) $= (3, 7, 2, 1, 1)$).

Proof. Note that the Mihilescu's theorem (originally Catalan's conjecture; see e.g. [Mi]) says that when $x, y, r, s > 1$ are integers, the equation $x^r - y^s = 1$ has no other solutions than $(x, y, r, s) = (3, 2, 2, 3)$. Then the assertion follows by an easy case-by-case study using Mihilescu's theorem and the fact that the two expressions $2^u + 1$ (resp. $2^u - 1$) and $2^{u+1} + 1$ (resp. $2^{u+1} - 1$) are both primes only when $u = 1$, $2^1 + 1 = 3$ and $2^2 + 1 = 5$ (resp. $u = 2$, $2^2 - 1 = 3$, $2^3 - 1 = 7$). □

Lemma 2.4. *Let*

$$g(\alpha, \beta) := (4\alpha - \beta)(4\alpha + \beta) \quad \textit{and} \quad f(\alpha, \beta) := g(\alpha, \beta)\alpha\beta,$$

let α and β be relatively prime positive integers such that one of the two is a power of 2 and let S be the set of pairs (α, β) of such integers satisfying one of the following conditions:

- *there is at most one odd prime divisor in $f(\alpha, \beta)$,*
- *there are two distinct odd prime divisors in $f(\alpha, \beta)$, but $g(\alpha, \beta)$ has at most one odd prime divisor, or*
- *there are three distinct odd prime divisors in $f(\alpha, \beta)$, but $g(\alpha, \beta)$ has no odd prime divisors.*

Then S is a finite set:

$$S = \{(1,2),(1,3),(1,4),(1,5),(1,6),(1,8),(1,12),(1,20),(1,28),(1,36),(1,68),$$
$$(2,9),(3,4),(3,8),(3,16),(5,4),(5,16),(7,4),(9,4),(9,32),(17,4)\}.$$

Proof. Let $(\alpha,\beta) \in S$. We see that one of $|4\alpha-\beta|$ and $|4\alpha+\beta|$ is a power of 2.

Case 1. Assume $\alpha = 1$, and let $\beta > 4$ (noting $(1,\beta) \in S$ for $\beta = 2,3,4$). Then $|4 \mp \beta| = 2^n$ for some $n \geq 0 \iff \beta = 2^n \pm 4$ and $|4 \pm \beta| = |2^n \pm 8|$. We see that each of β and $4 \pm \beta$ has an odd prime divisor except when $\beta = 8$ or $\beta = 12$, so $(1,8),(1,12) \in S$. Checking $(1,5),(1,6) \in S$, we let $n \geq 4$. Now we may assume that each of β and $4 \pm \beta$ contains only one odd prime divisor; we can write $\beta = 2^n \pm 4 = 4(2^{n-2} \pm 1) = 4q^l$ for some odd prime q and $l > 0$ and $4 \pm \beta = \pm 2^n + 8 = 8(\pm 2^{n-3} + 1) = \pm 8p^k$ for some odd prime $p \neq q$ and $k > 0$. By Lemma 2.3, this is possible only if $\beta = 20, 28, 36$ or 68.

Case 2. Assume $\alpha = 2^n$ for some $n \geq 1$. Then β must be odd. As in the above Case, we have $|4\alpha - \beta| = 1$ and so $\beta = 2^{n+2} \pm 1$. Then $4\alpha + \beta$ must have an odd prime factor. In order to $(\alpha,\beta) \in S$, we may assume that each of β and $4\alpha+\beta$ has at most one odd prime divisor. As $\beta = 1$ is absurd, we write $\beta = p^l$ for some $l \geq 1$ and $4\alpha + \beta = 2^{n+3} \pm 1 = q^k$ for some $k \geq 1$. By Lemma 2.3, we then have $(2,9) \in S$.

Case 3. Now suppose that $\beta = 2^n$ for some $n \geq 0$. If $|g(\alpha,\beta)|$ is simply a power of 2, then we can see $\alpha = 3$ and $\beta = 4$, i.e. $(3,4) \in S$. So assume that $g(\alpha,\beta)$ has only one odd prime divisor. As one of $|4\alpha-\beta|$ or $|4\alpha+\beta|$ is a power of 2, $\beta \neq 1$. So $n \geq 1$ and α must be odd. As the case $\alpha = 1$ was already dealt with in Case 1, we assume α has only one odd prime divisor, i.e. $\alpha = p^l$ for some odd prime p and $l \geq 1$. Moreover we can see that $\beta = 2$ is impossible in this case. Now suppose that $\beta = 4$. If $4\alpha - \beta = 4(p^l - 1) = 2^{u+2}$ (resp. $4\alpha + \beta = 4(p^l + 1) = 2^{u+2}$) with $u \geq 1$, then $4\alpha + \beta = 4(p^l + 1) = 8(2^{u-1} + 1)$ (resp. $4\alpha - \beta = 4(p^l - 1) = 8(2^{u-1} - 1)$) has at most one odd prime divisor only if $\alpha = 3, 5, 7, 9$ or 17 by Lemma 2.3. Now assume $\beta = 2^n$ with $n \geq 3$. then $4\alpha + \beta$ cannot be a power of 2. However, $|4\alpha - \beta|$ is a power of 2 if and only if $p^l = \alpha = 2^{n-2} \pm 1$. In

this case $4\alpha+\beta = 4(2^{n-1}\pm 1)$ has at most one odd prime divisor only when $(\alpha,\beta) = (3,8), (5,16), (9,32)$ or $(3,16)$ by Lemma 2.3. □

3. Proof of Theorem 1.1

Proposition 3.1. *Let E be an elliptic curve over $\mathbb{Q}$ with $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\subseteq E(\mathbb{Q})$. Then $16 \mid m$, except for '15a1' having $m=8$, '15a3' having $m=4$ and $c=2$, '21a1' with $m=8$ and '24a1' having $m=8$. In any case we have $8 \mid m\cdot c$.*

Proof. Assume to the contrary that 16 does not divide m. Elliptic curves E having $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\subseteq E(\mathbb{Q})$ are parametrized by one parameter $\lambda\in\mathbb{Q}$ with the Weierstrass equation (1), where λ is given by $\lambda = (\alpha/\beta)^2 - 1/16 = (4\alpha-\beta)(4\alpha+\beta)/(16\beta^2)$ for some relatively prime positive integers α and β such that the discriminant of the equation $\Delta = \lambda^4(16\lambda+1)\neq 0$ (cf. [Ku, Table 3]). In this case, the j-invariant of the curve is given by

$$j = \frac{256\alpha^4+224\alpha^2\beta^2+\beta^4}{(4\alpha-\beta)^4(4\alpha+\beta)^4\alpha^2\beta^2}.$$

We note that there is no cancellation by odd primes in this expression and the equation (1) is minimal at any odd prime p dividing $\alpha\beta(4\alpha-\beta)(4\alpha+\beta)$.

By Lemma 2.1 (resp. Lemma 2.2), any odd prime p dividing $\alpha\beta$ (resp. $(4\alpha-\beta)(4\alpha+\beta)$) contributes the Tamagawa number $m=\prod_p m_p$ of the curve by $2 \mid m_p$ (resp. $4 \mid m_p$). Hence, when one of α or β is a power of 2, the pair (α,β) we need to consider is exactly contained in the set S in Lemma 2.4. By computation, we can see that the only curves that are obtained from the pair $(\alpha,\beta)\in S$ with $16\nmid m$ are '15a1', '21a1' and '24a1', all having $m=8$ (cf. [Cr]).

Now the only remaining cases to consider is when the two relatively prime positive integers α and β have at least one odd prime divisor each. We can also assume that $|(4\alpha-\beta)(4\alpha+\beta)|$ is a power of 2; write $4\alpha+\beta = 2^n$ for some $n\geq 0$ and $4\alpha-\beta = \pm 2^l$ for some $l\geq 0$. Then $8\alpha = 2^n\pm 2^l$ and $2\beta = 2^n\mp 2^l$. As $\alpha,\beta>0$, we have $n>l\geq 3$. Now β is divisible by 4 and hence α is odd. So $l=3$ and $\alpha = 2^{n-3}\pm 1$ and $\beta = 4(2^{n-3}\mp 1)$. When $n=4$, then we have $(\alpha,\beta)=(3,4)$ or $(1,12)$, which are included in the set S and computed already. When $n=5$, we have $(\alpha,\beta)=(5,12)$ or $(3,20)$, both of which give the curve '15a3' having $m=4$ and $c=2$ (cf. [Cr]).

Assuming $n \geq 6$, we get $\mathrm{ord}_2\,\lambda = \mathrm{n} + \mathrm{l} - 4 - 2\mathrm{ord}_2\,\beta = \mathrm{n} - 5 \geq 1$, so by Lemma 2.2, $4 \mid m_2$. As each of odd prime factors of α and β contributes a factor of 2, we have $16 \mid m$. □

Proposition 3.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ with $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{Q})$. Then $4 \mid m$, except for '17a2' and '32a2'. For these exceptions, we have $m = c = 2$.*

Proof. Assume to the contrary that 4 does not divide m. Elliptic curves E with $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{Q})$ have the following Weierstrass equation:

$$E : y^2 = x(x+a)(x+b) \tag{3}$$

with $a, b \in \mathbf{Z}$ and with discriminant $\Delta = 16a^2b^2(a-b)^2 \neq 0$ (cf. [Ku, Table 3]). We note that $c_4 = 16a^2 - 16ab + 16b^2$.

By Lemma 2.1 (i), we know that all bad odd primes are multiplicative. Suppose there is an odd prime p dividing both a and b. If $\mathrm{ord_p\,a}$ and $\mathrm{ord_p\,b}$ are both ≥ 2, then the equation (3) can be reduced to the equation of the same form with a and b replaced by a/p^2 and b/p^2. So we assume either $\mathrm{ord_p\,a} = 1$ or $\mathrm{ord_p\,b} = 1$. If only one of $\mathrm{ord_p\,a}$ and $\mathrm{ord_p\,b}$ is equal to 1, then $\mathrm{ord_p\,c_4} = 2$. So the equation (3) is minimal at p and E has additive reduction modulo p. Suppose that $\mathrm{ord_p\,a} = 1$ and $\mathrm{ord_p\,b} = 1$. Write $a = a'p$ $(p \nmid a')$ and $b = b'p$ $(p \nmid b')$. If $p \nmid (a' - b')$, then $\mathrm{ord_p}\,\Delta = 6$ and $\mathrm{ord_p\,c_4} > 0$. So the equation (3) is minimal at p and E has additive reduction modulo p. If $p|(a' - b')$, then $\mathrm{ord_p\,c_4} = \mathrm{ord_p\,p^2((a' - b')^2 + a'b')} = 2$. So the equation (3) is minimal at p and E has additive reduction modulo p. Thus we can assume that a, b and $a - b$ are pairwise relatively prime away from 2. By Lemma 2.1 (ii), we can further assume $ab(a-b)$ contains at most one odd prime factor.

Note that by changing variables of the equation (3) if necessary we may assume at least one of a and b is not divisible by 4. Suppose that both a and b do not have any odd prime factor. Then we can further assume $b = \pm 1$ or ± 2. Write $a = \pm 2^n$. If $|a - b|$ is also a power of 2, then we have the curves '32a2' $(m = c = 2)$ and '64a1' $(m = 4)$ (cf. [Cr]). Suppose that $a - b$ has an odd prime divisor. We can readily check that $\mathrm{ord_2\,j} = 8 - 2\mathrm{ord_2\,a}$ when $b = \pm 1$ and $\mathrm{ord_2\,j} = 10 - 2\mathrm{ord_2\,a}$ when $b = \pm 2$. If $n \geq 6$, we have $\mathrm{ord_2\,j} < 0$

so E is potentially multiplicative modulo 2 (cf. [Si, VII Proposition 5.4 and 5.5]). Moreover, as $\mathrm{ord}_2 \mathrm{j} \in 2\mathbb{Z}$, m_2 must be even in any cases (cf. [Si, Table 15.1]). If $n < 6$, we only have finitely many cases ($a \in \{\pm 2^n : 0 \leq n < 6\}$ and $b \in \{\pm 1, \pm 2\}$). By computation, we can see that all of $4 \mid m$, except for '17a2', for which we have $m = c = 2$ (cf. [Cr]).

When a (resp. b) has an odd prime factor, the change of variables $x' = x+b$ (resp. $x' = x + a$) reduces this case into the cases we treated above. This completes the proof. □

Proposition 3.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})[3] \cong \mathbb{Z}/3\mathbb{Z}$. If P_K has infinite order in $E(K)$, then $3 \mid c \cdot m \cdot u_K \cdot |\text{Ш}(\mathrm{E}/\mathrm{K})|^{\frac{1}{2}}$.*

Proof. The proof is exactly same as that of the proof of [BKY, Theorem 1.2]. □

Proof of Theorem 1.2. Theorem 1.1 follows from Proposition 3.1, 3.2 and 3.3. □

Acknowledgment. The authors thank the referees for their careful readings and many valuable suggestions.

References

[BKY] D. Byeon, T. Kim and D. Yhee, *A conjecture of Gross and Zagier: case $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$,* Int. J. Number Theory, **15** (2019), 1793–1800.

[Cr] J. Cremona, *Elliptic curve data*, available at http://johncremona.github.io/ecdata.

[Ku] D. S. Kubert, *Universal bounds on the torsion of elliptic curves,* Proc. London Math. Soc., **33** (1976), 193–237.

[GZ] B. H. Gross and D. Zagier, *Heegner points and derivatives of L-series,* Invent. Math. **84** (1986), 225–320.

[Lo] D. Lorenzini, *Torsion and Tamagawa numbers,* Annales de L'Institut Fourier, **61** (2011), 1995–2037.

[Ma] B. Mazur, *Modular curves and the Eisenstein ideal,* Publ. Math. I.H.E.S., **47** (1977), 33–186.

[Mi] P. Mihilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math., **572** (2004), 167–195.

[Si] J. H. Silverman, *The arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. **106**, Springer 2009.

Department of Mathematical Sciences, Seoul National University
Seoul, Korea,
E-mail: dhbyeon@snu.ac.kr

Center for Geometry and Physics, Institute of Basic Science
Pohang, Korea
E-mail: Taekyung.Kim.Maths@gmail.com

Department of Mathematical Sciences, Seoul National University
Seoul, Korea
E-mail: dgyhee@gmail.com