Conjectures concerning the orders of the torsion subgroup, the arithmetic component groups, and the cuspidal subgroup

Amod Agashe*

Abstract

We make several conjectures concerning the relations between the orders of the torsion subgroup, the arithmetic component groups, and the cuspidal subgroup of an optimal elliptic curve. These conjectures have implications for the second part of the Birch and Swinnerton-Dyer conjecture.

1 Introduction

Let E be an optimal elliptic curve and let N denote its conductor. Thus E is associated to a newform f of weight 2 on $\Gamma_0(N)$ with integer Fourier coefficients, and by dualizing, E may be viewed as an abelian subvariety of $J_0(N)$, which we shall do henceforth. We may often refer to N also as the *level*. Let C denote the cuspidal subgroup of $J_0(N)$, i.e., the subgroup of $J_0(N)(\mathbf{C})$ generated by the degree zero divisors that are supported on the cusps of $X_0(N)(\mathbf{C})$. Let $C_E = E(\mathbf{C}) \cap C$; we call C_E the cuspidal subgroup of E. If p is a prime that divides N, then let $c_p(E)$ denote the order of the arithmetic component group of E at p (also called the Tamagawa number of E at p). If N is prime, then by [Maz77, Thm. II.1.2], $J_0(N)(\mathbf{Q})_{\rm tor} = C$, so that $E(\mathbf{Q})_{\rm tor} = C_E$, and it follows from parts (v) and (vi) of Theorem B in [Eme03] that $|E(\mathbf{Q})_{\rm tor}| = c_N(E)$. Thus if N is prime, then

$$|E(\mathbf{Q})_{\rm tor}| = |C_E| = \prod_p c_p(E). \qquad (1)$$

*The author was supported by the National Science Foundation under Grant No. 0603668 and by National Security Agency Grant No. Hg8230-10-1-0208. This manuscript is submitted for publication with the understanding that the United States Government is authorized to reproduce and distribute reprints.

This set of equalities in (1) has implications for the Birch and Swinnerton-Dyer (BSD) conjecture, as we now discuss. Let $L_E(s)$ denote the L-function of E. The first part of the BSD conjecture asserts that the Mordell-Weil rank of E equals the order of vanishing of $L_E(s)$ at $s = 1$. Let K_E denote the coefficient of the leading term of the Taylor series expansion of $L_E(s)$ at $s = 1$, and let R_E denote the regulator of E. Let Ω_E denote the volume of $E(\mathbf{R})$ calculated using a generator of the group of invariant differentials on the Néron model of E. Then the *second part of the BSD conjecture* asserts the formula:

$$\frac{K_E}{\Omega_E \cdot R_E} \overset{?}{=} \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2} \ . \tag{2}$$

The equalities in (1) indicate that when N is prime, there is significant cancellation on the right side of the BSD conjectural formula (2).

The quantities in (1) are not necessarily equal when N is not prime. This article is an effort to see what relations one might expect between the quantities in (1) and what cancellations one may expect on the right side of the BSD conjectural formula (2) when N need not be prime. We make several conjectures in this regard in the next section, and also make some related conjectures. Unless mentioned otherwise, all of these conjectures were tested on Cremona's database [Cre] for optimal elliptic curves of conductor up to 130000, using the mathematical software Sage.

Acknowledgements: We are very grateful to William Stein for his extensive help on this article. In particular, he provided numerical evidence for many of the conjectures made in this article, and also introduced the author to programming in Sage. Some of the computations were done on sage.math.washington.edu, which is supported by National Science Foundation Grant No. DMS-0821725. The author is also grateful to the Tata Institute of Fundamental Research for a visit during which he first started investigating the issues discussed in this article.

2 Conjectures

To start with, we conjecture the following relationship between $E(\mathbf{Q})_{\mathrm{tor}}$ and C_E:

Conjecture 2.1. *If N is square-free, then $E(\mathbf{Q})_{\mathrm{tor}} \subseteq C$.*

In other words we conjecture that $E(\mathbf{Q})_{\mathrm{tor}} = C_E$, i.e., the entire rational torsion in E is accounted for by the cuspidal subgroup of $J_0(N)$ when N is square-free. As mentioned earlier, the conjecture is known to be true if N is prime. W. Stein has checked the conjecture above for all E of conductor up to 1000. There is a partial result towards the conjecture above: by the main theorem of [Aga07], if N is square-free and r is a prime that does not divide $6N$, but divides $|E(\mathbf{Q})_{\mathrm{tor}}|$, then r divides $|C_E|$. It seems possible that the hypothesis that N is squarefree is not needed in the conjecture above (we do not have sufficient data and theoretical results to justify removing the hypothesis).

One of the inputs in the main theorem of [Aga07] quoted above is the fact (Proposition 3.5 in [Aga07]) that under the hypotheses as above on r, $w_p = -1$ for at least one prime p that divides N. This (and numerical evidence) motivates the following conjecture:

Conjecture 2.2. *If N is square-free and $E(\mathbf{Q})_{\mathrm{tor}}$ is non-trivial, then $w_p = -1$ for at least one prime p that divides N.*

The hypothesis that N is square-free is required. For example, the elliptic curve 162a1 (note that $162 = 2 * 3^4$) has a 3-torsion point, but $w_p = 1$ for all p dividing 162. At the same time, there are no examples of elliptic curves with conductor less than 130000 that have a 5 or 7-torsion point, and $w_p = 1$ for all primes p dividing the conductor.

Next we discuss the relationship between the torsion order and the Tamagawa product. First, we have:

Proposition 2.3. *Let ℓ be an odd prime such that either $\ell \nmid N$ or for all primes r that divide N, $\ell \nmid (r-1)$. If ℓ divides the order of the geometric component group of E at p for some prime $p||N$, then either $E[\ell]$ is reducible or the newform f is congruent to a newform of level dividing N/p (for all Fourier coefficients whose indices are coprime to $N\ell$) modulo a prime ideal over ℓ in a number field containing the Fourier coefficients of both newforms.*

Proof. By [Eme03, Prop. 4.2], if ℓ divides $c_p(E)$ for some prime p that divides N, then for some maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ having characteristic ℓ and containing I_f, either $\rho_{\mathfrak{m}}$ is finite at p or is reducible (here, $\rho_{\mathfrak{m}}$ is the canonical two dimensional representation associated to $\mathfrak{m}$, e.g., as in [Rib90, Prop. 5.1]). So if $E[\ell]$ is irreducible, then $\rho_{\mathfrak{m}}$ is finite at p, and by [Rib90, Thm. 1.1], in view of the hypotheses that either $\ell \nmid N$ or for all primes p that divide N, $\ell \nmid (p-1)$, f is congruent modulo ℓ to a newform of a level dividing N/p (for Fourier coefficients of index coprime to $N\ell$). □

The proposition above (and numerical evidence) motivates the following conjecture.

Conjecture 2.4. *If an odd prime ℓ divides $c_p(E)$ for some prime p that divides N, then either ℓ divides $|E(\mathbf{Q})_{\mathrm{tor}}|$ or the newform f is congruent to a newform of level dividing N/p (for all Fourier coefficients whose indices are coprime to $N\ell$) modulo a prime ideal over ℓ in a number field containing the Fourier coefficients of both newforms.*

Note that in Conjecture 2.4 above, we have dropped the hypotheses made in Proposition 2.3 above that $p||N$ and either $\ell \nmid N$ or for all primes r that divide N, $\ell \nmid (r-1)$. Also, the statement of Conjecture 2.4 is stronger than the conclusion of Proposition 2.3: we claim that ℓ divides $|E(\mathbf{Q})_{\mathrm{tor}}|$, not just that $E[\ell]$ is reducible. We checked the conjecture above for conductors up to 1010 in Sage with the help of W. Stein. Later, Randy Heaton [Hea] checked the conjecture for conductors up to 1500, and also for several conductors bigger than 1500 that are smooth.

Related to Proposition 2.3 and Conjecture 2.4 above is the following:

Conjecture 2.5. *If N is square-free and for some odd prime ℓ, $E[\ell]$ is reducible, then E has an ℓ-torsion point.*

The hypothesis that N is square-free in the conjecture above is essential. For example, for $E = 99d1$, $E[5]$ is reducible, but E has no rational 5-torsion. If N is square-free, then as mentioned in [Cal01, p. 494-495], it follows from [Ser72] that if E is a semistable elliptic curve and p is a prime such that $E[p]$ is reducible, then either E or an elliptic curve isogenous to it has a rational p-torsion point (however, we do not know if E itself has a rational p-torsion point, which is what we want).

Conjecture 2.4 is about when a prime dividing the Tamagawa product may divide the torsion order. The following conjecture goes in the other direction:

Conjecture 2.6. *Let $\ell > 3$ be a prime. Then the order of the ℓ-primary part of $E(\mathbf{Q})_{\mathrm{tor}}$ divides $\prod_p c_p(E)$.*

Of course if $\ell > 3$ is a prime such that the ℓ-primary part of $E(\mathbf{Q})_{\mathrm{tor}}$ is non-trivial, then the only possibilities for ℓ are 5 and 7, and so in Conjecture 2.6, we could have just said that $\ell = 5$ or 7 instead of saying that ℓ is a prime bigger than 3. However, the reason for phrasing the conjecture as above is the hope that its statement would hold for abelian subvarieties of $J_0(N)$ associated to newforms (that need not be elliptic curves). After this article was written, Conjecture 2.6 above was proved by D. Lorenzini [Lor] (for elliptic curves – Lorenzini's techniques involve explicit Weierstrass equations). We remark that the statement of the conjecture fails for

$\ell = 3$. For example, the elliptic curve 91b1 has torsion order 3 and Tamagawa product 1. The curve 91b1 was the only one with squarefree conductor at most 130000 where there was a counterexample for $\ell = 3$.

Conjectures 2.4 and 2.6 indicate significant cancellation on the right side of the BSD formula (2) even if N is not prime. As for how to account for the primes that do not cancel, the author only has some guesses – see the discussion towards the end of Section 1 in [Aga10].

References

[Aga07] A. Agashe, *Rational torsion in elliptic curves and the cuspidal subgroup*, submitted (2007), available at arXiv:0810.5181 or `http://www.math.fsu.edu/~agashe/math.html`.

[Aga10] ______, *A visible factor of the special L-value*, J. Reine Angew. Math. (Crelle's journal) **644** (2010), 159–187.

[Cal01] Frank Calegari, *Almost rational torsion points on semistable elliptic curves*, Internat. Math. Res. Notices (2001), no. 10, 487–503.

[Cre] J. E. Cremona, *Elliptic curve data,* `http://www.warwick.ac.uk/staff/j.e.cremona/ftp/data/index.html`.

[Eme03] Matthew Emerton, *Optimal quotients of modular Jacobians*, Math. Ann. **327** (2003), no. 3, 429–458.

[Hea] R. Heaton, *Computing congruence primes bewteen a newform with integer coefficients and the old space*, submitted.

[Lor] D. Lorenzini, *Torsion and Tamagawa numbers*, Ann. Inst. Fourier, **61** (2011), no. 5, 1995–2037.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[Rib90] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

[Ser72] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.