Mathematical Research Letters **3**, 309–318 (1996)

EFFECTIVE BOUNDS ON THE SIZE OF THE TATE-SHAFAREVICH GROUP

Dorian Goldfeld and Daniel Lieman

Throughout this paper we will work over $\mathbb{Q}$, although our methods generalize quite naturally to any number field.

Consider an elliptic curve E defined over $\mathbb{Q}$. We use the following notation: $Ш_E$ denotes the Tate-Shafarevich group of E, N_E denotes the conductor of E, $\mathrm{j}(E)$ denotes the j-invariant of E, $\Delta(E)$ denotes the discriminant of E, and $|\mathcal{S}|$ denotes the cardinality of any set $\mathcal{S}$. It has been conjectured by Goldfeld and Szpiro [GS] that for every $\epsilon > 0$ there exists an effectively computable constant $c > 0$ depending only on ϵ such that

$$|Ш_E| < c\,N^{\frac{1}{2}+\epsilon}.$$

Goldfeld and Szpiro also show that if this conjecture holds for rank zero semistable elliptic curves, a version of the ABC conjecture follows. In particular, for coprime integers A, B and C satisfying $A + B + C = 0$ one has

$$|ABC|^{1/3} = O\left(\prod_{p\,|\,ABC} p\right)^{3+2\epsilon};$$

if in addition one assumes a Lindelöf hypothesis, one may improve this to

$$|ABC|^{1/3} = O\left(\prod_{p\,|\,ABC} p\right)^{1+\frac{13}{6}\epsilon}.$$

We prove the conjecture of Goldfeld and Szpiro (subject to various standard conjectures) for any collection $\mathcal{C}$ of elliptic curves which has the properties that: 1) the set $\{\mathrm{j}(E)\,|\,E \in \mathcal{C}\}$ is finite; and 2) $\mathcal{C}$ does not contain any curves with j-invariant 0 or 1728. In many cases, the conjectures we assume

Received November 30, 1995.

Both authors are partially supported by the National Science Foundation.

are already known, and our results become unconditional. (In particular, as a consequence of the work of Rubin [R], we obtain the unconditional bound $|Ш_E| < c\,N^{59/120+\epsilon}$, for rank zero complex multiplication curves whose j-invariant is unequal to 0 or 1728.) In the two exceptional cases of j-invariant 0 or 1728, we obtain the slightly weaker bounds: $|Ш_E| < c\,N^{79/120+\epsilon}$, $|Ш_E| < c\,N^{37/60+\epsilon}$, respectively.

To simplify the statements of our theorems, we shall use the term "BSD curve" to refer to an elliptic curve defined over $\mathbb{Q}$ which is modular and satisfies the Birch and Swinnerton-Dyer conjecture. Our main results are:

Theorem 1. *Let j_0 be a fixed j-invariant not equal to 0 or 1728. Let E_{j_0} be a modular elliptic curve defined over $\mathbb{Q}$, of minimal discriminant with $j(E_{j_0}) = j_0$. Then for every $\epsilon > 0$, there is a computable constant c depending only on ϵ and E_{j_0} such that:*

i) *for every BSD curve E of rank at most 1 with $j(E) = j_0$,*

$$|Ш_E| < c\,N_E^{95/192+\epsilon}.$$

If, in addition, E has complex multiplication, then

$$|Ш_E| < c\,N_E^{59/120+\epsilon}.$$

ii) *For every rank 0 complex multiplication curve E with $j(E) = j_0$,*

$$|Ш_E| < c\,N_E^{59/120+\epsilon}.$$

(*We do not need the hypothesis that E is a BSD curve in this case.*)

Theorem 2. *For every $\epsilon > 0$, there is a computable constant c depending only on ϵ such that:*

i) *For every rank 0 curve E with $j(E) = 1728$,*

$$|Ш_E| < c\,N_E^{37/60+\epsilon}.$$

ii) *for every rank 1 BSD curve E with $j(E) = 1728$,*

$$|Ш_E| < c\,N_E^{37/60+\epsilon}.$$

Theorem 3. *For every $\epsilon > 0$, there is a computable constant c depending only on ϵ such that:*

i) *for every rank 0 curve E with $j(E) = 0$,*

$$|Ш_E| < c\,N_E^{79/120+\epsilon}.$$

ii) *for every rank* 1 *BSD curve* E *with* $j(E) = 0$,

$$|\text{Ш}_E| < c\, N_E^{79/120+\epsilon}.$$

Remark 4. If we assume E_{j_0} is semistable, then by the recent results of Wiles [W] and Taylor-Wiles [TW], it follows that E_{j_0} is modular. In many cases, E then satisfies the Birch and Swinnerton-Dyer conjectures (cf. Remark 7, below). In fact, if E_{j_0} is semistable, the constant c in Theorem 1 takes the form $c = c_1 \Delta \left(E_{j_0}\right)^{c_2}$. We may extend our main theorems to curves of higher rank by assuming Lang's conjecture [La, p. 161] on a lower bound of the size of the regulator of an elliptic curve. If we do not assume Lang's conjecture, but instead use estimates of Hindry and Silverman [HS], we may still extend our theorems to curves of any rank, but with weaker exponents for curves of rank larger than 1. It will be clear in the proof how these constants are affected by relaxing the hypotheses in the theorems.

One consequence of Theorems 1-3 is

Corollary 5. *For every* $\epsilon > 0$, *there is a computable constant* c *depending only on* ϵ *such that:*

i) *for every rank* 0 *curve* E *with complex multiplication,*

$$|\text{Ш}_E| < c\, N_E^{79/120+\epsilon}.$$

ii) *for every rank* 1 *BSD curve* E *with complex multiplication,*

$$|\text{Ш}_E| < c\, N_E^{79/120+\epsilon}.$$

Proof. The Corollary follows from the fact that every curve with complex multiplication is modular [D] and has one of only thirteen possible j-invariants (including both 0 and 1728, cf. [Se]).

Remark 6. If we study the behavior of Ш on average, we may obtain stronger results than we can obtain (in this paper) for individual curves (subject to the truth of the same standard conjectures). In fact, it follows from the arguments of [Li] and Remark 8 at the end of this paper that for the class of curves

$$E_D : y^2 = x^3 - 432D^2,$$

Ш_{E_D} satisfies on average

$$|\text{Ш}_{E_D}| = O\left(N_{E_D}^{1/3+\epsilon}\right).$$

(Our methods in this paper prove that for such curves,

$$|Ш_{E_D}| < cN_{E_D}^{49/120+\epsilon}.$$

The conductor of E_D is $27 \cdot n \cdot d^2$, where d is the product of the primes dividing D, and n is either 1 or 9, depending on d.) Indeed, one expects (from the full strength of the Lindelöf hypothesis for the L-functions of elliptic curves) that for the family of elliptic curves with fixed j-invariant not equal to 0 or 1728,

$$|Ш_E| < cN_E^{1/4+\epsilon},$$

while for the family of curves with j-invariant 1728

$$|Ш_E| < cN_E^{3/8+\epsilon},$$

and for the family with $\mathrm{j}(E_D) = 0$

$$|Ш_E| < cN_E^{5/12+\epsilon}.$$

(In fact, one may carry out an analysis identical to what we have done in Remark 8 to verify that these bounds are satisfied on average for all curves with j-invariant not equal to 0 or 1728.)

Proof of Theorems 1-3. There are two main ingredients in our proof. The first is an analysis of the "Birch and Swinnerton-Dyer constant," and how this number varies in a family of twists. The second is an upper bound on the size of the n^{th} derivative of the L-series of a cusp form twisted by an arbitrary character, at the center of the critical strip. We should remark at the onset that this second part of our proof is due completely to Duke, Friedlander, and Iwaniec ([DFI1], [DFI2]). In fact, they recognized the applications of their bound to elliptic curves, and began investigations into the use of their work to bound the height of Heegner points. Our insight is the use of their bound on families of twists to obtain bounds on the size of $Ш_E$. We now turn to the proof proper.

The conjecture of Birch and Swinnerton-Dyer asserts that at the center $s = \frac{1}{2}$ of the critical strip (we use this somewhat nonstandard normalization for consistency with our discussion of the L-series of cusp forms, below), we have

$$\lim_{s\to 1/2} \frac{L(E,s)}{(s-1/2)^r} = \frac{|Ш_E|\,\Omega_E\,R_E\,c_E}{|E(\mathbb{Q})_{\text{tors}}|^2} \tag{1}$$

where r is the rank, Ω_E is the period, R_E is the regulator, and c_E is a positive integer.

Remark 7. The work of Kolyvagin [K] and either Bump, Friedberg and Hoffstein [BFH1, BFH2] or Murty and Murty [MM] shows that for many modular elliptic curves of rank 1, one has an identity similar to (1) over an appropriate number field $\mathbb{K}$. In fact, their works shows that (where we use the subscript $\mathbb{K}$ to indicate we are thinking of these various quantities for the curve over $\mathbb{K}$)

$$\lim_{s\to 1/2} \frac{L(E_{\mathbb{K}}, s)}{(s-1/2)^r} = \frac{|\text{Ш}_{E_{\mathbb{K}}}|\, \Omega_{E_{\mathbb{K}}}\, R_{E_{\mathbb{K}}}\, c_{E_{\mathbb{K}}}\, m}{|E(\mathbb{K})_{\text{tors}}|^2}$$

for some positive integer m (in fact, Kolyvagin characterizes m (which is predicted to be 1) completely: its prime factors are 2 and the odd primes p where the Galois group of the extension $\mathbb{Q}(E_p)$ is smaller than expected, where E_p denotes the p-torsion points of E).

In particular,

$$\lim_{s\to 1/2} \frac{L(E_{\mathbb{K}}, s)}{(s-1/2)^r} \geq \frac{|\text{Ш}_{E_{\mathbb{K}}}|\, \Omega_{E_{\mathbb{K}}}\, R_{E_{\mathbb{K}}}\, c_{E_{\mathbb{K}}}}{|E(\mathbb{K})_{\text{tors}}|^2}$$

(cf. [Gr, Thm 1.3 (Kolyvagin)]). Rubin [R] has proved a similar result for CM curves of rank 0, and in these cases our results are unconditional (as we mention below, we do not need Lang's conjecture or the results of Hindry-Silverman in this case of low rank). In particular, Rubin's work also applies to curves over $\mathbb{Q}$; this is why the main theorems are unconditional for CM curves of rank 0. As will be clear in the proof, we do not require the full Birch and Swinnerton-Dyer conjecture, just an inequality in the direction of those of Kolyvagin and Rubin.

We now note that:

a) Mazur's theorem [M] asserts that $|E(\mathbb{Q})_{\text{tors}}|^2 \leq 256$.

b) It is easy to see (cf. [Si2, C.15.2.1]) that $1 \leq c_E \leq 4\tau(N_E)$, where $\tau(N_E)$ is the number of primes dividing N_E.

c) Fix a j-invariant j_0, and let n be the integer

$$n = \begin{cases} 2 & j_0 \neq 0 \text{ or } 1728, \\ 4 & j_0 = 1728, \\ 6 & j_0 = 0. \end{cases}$$

Again, let E_{j_0} be a curve with minimal discriminant satisfying $\mathrm{j}\,(E_{j_0}) = j_0$. Then every curve E with $\mathrm{j}(E) = j_0$ is a twist of E_{j_0} by a rational number $D \in \mathbb{Q}^\times/\mathbb{Q}^{\times^n}$. In particular, we may assume (without loss of generality) that D is an integer (by clearing denominators by multiplying by an n^{th}

power) and $n^{\rm th}$ power free. We will assume from this point on that our D is of this form. It thus follows that

$$\Omega_E = D^{-\frac{1}{n}}\,\Omega_{E_{j_0}}.$$

Further, it follows from the work of Goldfeld [Go] that if E_{j_0} is semistable, one may bound $\Omega_{E_{j_0}}$ from below:

$$\Omega_{E_{j_0}} \geq c_3 \Delta\left(E_{j_0}\right)^{-c_4}$$

where the constants c_3, c_4 are effectively computable absolute constants.

d) When the rank of E is zero, R_E is just 1. When the rank of E is 1, R_E is just the height of a point of infinite order, and has been bounded below by Silverman [Si1] and by Hindry and Silverman [HS]. These bounds are of the shape

$$R_E \gg \log(\Delta_E) + c$$

for some constant c independent of E, where Δ_E is the discriminant of E. When the rank of E is greater than 1, Hindry and Silverman (assuming Szpiro's conjecture) have obtained the bound

$$R_E \gg N^{-\gamma}$$

for some constant γ independent of E. Lang's conjecture [La, p. 161], which implies that there is an absolute constant c_0 such that if r_E denotes the rank of E, one has

$$R_E \gg c_0^{r_E^2} \log\left(|\Delta(E)|\right)^{r_E},$$

asserts that for curves of any fixed rank one may take $\gamma = \epsilon$ where $\epsilon > 0$ is arbitrarily small.

Note that when the rank is 0, we may take $\gamma = 0$, and that when the rank is 1, we may take γ arbitrarily small. For higher ranks, we have to assume either Lang's conjecture [La], or Szpiro's conjecture (and then use [HS]). We will keep track of γ in what follows, in order to allow the dependence on Lang's conjecture (which would allow us to remove γ entirely) to be clear.

e) If E is a twist of E_{j_0} then

$$N_E \gg \overline{D}^2 N_{E_{j_0}},$$

where D is defined as in (c), $\overline{D}$ is the product of the primes dividing D (cf. [Sh]), and the implied constant depends on E_{j_0}. It immediately follows that

$$\overline{D} \ll N_E^{1/2}.$$

Further, since $D \in \mathbb{Q}/\mathbb{Q}^n$, it is plain that

$$D \leq \overline{D}^{n-1} \ll N_E^{(n-1)/2}.$$

We now return to the proof of Theorems 1-3. Fix j_0 and a choice of E_{j_0}, and let n, $\overline{D}$, γ be as in (c), (d), (e), above. For any curve with $\mathrm{j}(E) = j_0$, let D denote the integer so that E is a twist by D of E_{j_0}. We then have

$$\begin{aligned} |\text{Ш}_E| &= \lim_{s\to 1/2} \frac{L(E,s)|E(\mathbb{Q})_{\text{tors}}|^2}{(s-1/2)^r\,\Omega_E\,R_E\,c_E} \\ &\ll \Omega_{E_{j_0}}^{-1} D^{1/n} N_E^{\gamma} \lim_{s\to 1/2} \frac{L(E,s)}{(s-1/2)^r} \\ &\leq \Omega_{E_{j_0}}^{-1}\, \overline{D}^{(n-1)/n} N_E^{\gamma} \lim_{s\to 1/2} \frac{L(E,s)}{(s-1/2)^r} \\ &\ll \Omega_{E_{j_0}}^{-1} N_E^{(n-1)/(2n)+\gamma} \lim_{s\to 1/2} \frac{L(E,s)}{(s-1/2)^r}, \end{aligned} \tag{2}$$

where the implied constants depend on γ. This completes our analysis of the Birch and Swinnerton-Dyer constant.

We now turn to the second part of our argument which consists of applying a bound from analytic number theory to estimate the size of the right-hand side of (2). Duke, Friedlander and Iwaniec ([DFI1] and [DFI2]) have proved that if f is a weight 2 holomorphic newform, and χ is a character with conductor q which is relatively prime to the conductor N_f of f, then one has ([DFI2, (22)])

$$L(f,\chi,1/2) \ll (N_f)^{47/192+\epsilon}\, q^{47/96+\epsilon} \tag{3}$$

where the implied constant is effective, and depends only on ϵ.

In fact, they prove much more. In particular, they obtain a bound for the value of the L-function anywhere on the line at the center of the critical strip, and they obtain a bound for every derivative of the L-function on the left-hand side of (3). In this latter case (which we will indeed need), the implied constant is effective, and depends on the order of the derivative and on ϵ. Finally, we mention that in the case where the coefficients of f are not small too often (in the sense of [DFI2, Corollary 4]), then one has ([DFI2, Theorem 3])

$$L(f,\chi,1/2) \ll (N_f)^{29/120+\epsilon}\, q^{29/60+\epsilon}.$$

This additional hypothesis is satisfied when f is the form associated to an elliptic curve with complex multiplication ([DFI2, Corollary 5]), and hence we may use these sharper bounds in that case, cf. the second assertion of Theorem 1, Theorems 2 and 3, Corollary 5, and the remarks at the end of the second paragraph of this paper.

We now note the connection between the two parts of our argument. If E is a twist of E_{j_0} by an integer D, and n is as above, then the L-series of E is just the L-series of E_{j_0} twisted by a character of order n and modulus $\overline{D}$ (this follows for the cases of j-invariants 0 and 1728 from the explicit computations of Ireland and Rosen [IR]; for $j \neq 0,\ 1728$, it follows immediately from the definition of twisting, cf. [Si2, X.2.4]). Combining (2) and (3) with this observation yields

$$|\text{Ш}_E| \ll \Delta\left(E_{j_0}\right)^{c_2} N_E^{(n-1)/(2n)+\gamma} \lim_{s\to 1/2} \frac{L(E,s)}{(s-1/2)^r}$$
$$\ll \Delta\left(E_{j_0}\right)^{c_2} N_E^{(n-1)/(2n)+\gamma} D^{47/96+\epsilon} \ll \Delta\left(E_{j_0}\right)^{c_2} N_E^{(n-1)/(2n)+47/192+\epsilon+\gamma}$$
$$\ll \Delta\left(E_{j_0}\right)^{c_2} N_E^{(96(n-1)+47n)/(192n)+\epsilon+\gamma}.$$

This is precisely the statement of Theorems 1, 2, and 3. (In order to obtain the sharper bounds given in the second claim of Theorem 1 and Theorems 2 and 3, we must replace the fraction 47/96 with the slightly sharper 29/60 which does apply, as we mentioned above, in this case.)

Remark 8. Finally, we offer a comparison between results for individual curves, and results which may be obtained on average. The central focus of [Li] was the family of curves

$$E_m : y^2 = x^3 - 432m^2.$$

In that paper, Lieman showed that the Dirichlet series

$$\sum_{\substack{m,n\in\mathbb{Z}\\ m,n\neq 0}} \frac{L\left(E_{mn^2},1\right)}{\left(mn^2\right)^s}$$

has a pole at $s = 1$. It has proven quite difficult to evaluate the order of this pole; in particular, the function has a pole of order 2, but Lieman was not able to verify that the residue at this pole is non-zero. He did show, however, that if the residue is zero at the pole of order two, then the function has a non-zero residue at a pole of order 1 (again at s=1). Accordingly,

$$\sum_{m<X} L(E_m,1) \sim cX\left(\log X\right)^e$$

with e either 0 or 1, for some constant c. This class of curves has trivial torsion when $m \geq 3$; the period of the curve E_m is just $c_m m^{-1/3}\Omega_1$ where Ω_1 is the period of $x^3 + y^3 = 1$, and c_m is either 1 or 9 depending on the congruence class of m mod 9. Remark 6 follows from these observations.

Acknowledgements

We wish to thank Bill Duke and Joe Silverman for several helpful conversations. In addition, we would like to thank Bill Duke, Andrew Granville, Ken Ribet and the referee for catching several errors in preliminary versions of this paper, and Henri Darmon, Andrew Granville, and Karl Rubin for helpful conversations about Kolyvagin's work.

References

[BFH1] D. Bump, S. Friedberg, and J. Hoffstein, *A nonvanishing theorem for derivatives of automorphic L-functions with applications to elliptic curves*, Bull. Amer. Math. Soc. **21** (1989), 89–93.

[BFH2] ———, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), 543–618.

[D] M. Deuring, *Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins, I, II, III, IV*, Gott. Nach. (1953, 1955, 1956, 1957).

[DFI1] W. Duke, J. B. Friedlander, and H. Iwaniec, *Bounds for automorphic L-functions*, Invent. Math. **112** (1993), 1–8.

[DFI2] ———, *Bounds for automorphic L-functions. II*, Invent. Math. **115** (1994), 219–239.

[Go] D. Goldfeld, *Modular elliptic curves and diophantine problems*, in Number Theory, Proc. Conf. of the Canadian Number Thy. Assoc., Banff, Alberta, Canada, 1988 (1990), 157–176.

[GS] D. Goldfeld and L. Szpiro, *Bounds for the order of the Tate-Shafarevich group*, Compositio Math. **97** (1995), 71–87.

[Gr] B. Gross, *Kolyvagin's work on modular elliptic curves*, in L-functions and Arithmetic, Proc. of the Durham Symposium, July, 1989 (1991), 235–256.

[HS] M. Hindry and J. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), 419–450.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag GTM 84, 1982.

[K] V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and Ш $(E/\mathbb{Q})$ for a class of Weil curves*, Izv. Akad. Nauk SSSR **52** (1988).

[La] S. Lang, *Conjectured Diophantine estimates on elliptic curves*, Progr. Math. **35** (1983), Birkäuser, 155–172.

[Li] D. Lieman, *Nonvanishing of L-series associated to cubic twists of elliptic curves*, Ann. of Math. **140** (1994), 81–108.

[M] B. Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. **47** (1977), 33–186.

[MM] K. Murty and R. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. **133** (1991), 447–475.

[R] K. Rubin, *Tate-Shafarevich groups and L−functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527–559.

[Se] J.-P. Serre, *Complex Multiplication*, in Algebraic Number Theory, J. Cassels and A. Fröhlich, eds. (1967), Academic Press, 292–296.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, 1971.

[Si1] J. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. **48** (1981), 633–648.

[Si2] ______, *The Arithmetic of Elliptic Curves*, Springer-Verlag GTM 106, 1986.

[TW] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553–572.

[W] A. Wiles, *Modular elliptic curves and Fermat's last theorem.*, Ann. of Math. **141** (1995), 443–551.

Department of Mathematics, Columbia University, New York, NY 10027
E-mail address: goldfeld@columbia.edu, lieman@math.columbia.edu

Department of Mathematics, University of Missouri, Columbia, MO 65211
E-mail address: lieman@math.missouri.edu