Compositio Mathematica **105:** 29–41, 1997.

On the size of the Shafarevich–Tate group of elliptic curves over function fields

C. S. RAJAN
School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai – 400 005, India. e-mail: rajan@math.tifr.res.in

Received 19 June 1995; accepted in final form 3 August 1996

Abstract. Let E be a nonconstant elliptic curve, over a global field K of positive, odd characterisitc. Assuming the finiteness of the Shafarevich-Tate group of E, we show that the order of the Shafarevich-Tate group of E, is given by $O(N^{1/2+6\ \log(2)/\ \log(q)})$, where N is the conductor of E, q is the cardinality of the finite field of constants of K, and where the constant in the bound depends only on K. The method of proof is to work with the geometric analog of the Birch-Swinnerton Dyer conjecture for the corresponding elliptic surface over the finite field, as formulated by Artin-Tate, and to examine the geometry of this elliptic surface.

AMS classification: 11G05 11G25, 14G15

Key words: Elliptic curve, Shafarevich–Tate group, conductor.

1. Introduction

The class group of a number field K 'measures' the extent of departure of the ring of integers of K from being a unique factorisation domain. It is known to be finite and the class number formula of Dirichlet gives an explicit formula for the order of the class group of K, the class number. It follows from this using partial summation and the absolute lower bound for the regulator of number fields shown in ([22]), that the class number of a number field K is bounded by $\Delta_K^{(1/2)+\epsilon}$, where Δ_K is the discriminant of K. In the case of number fields, the conductor N_K of the Dedekind zeta function of K is equal to the discriminant of K, and so one has that the class number is bounded by $N_K^{(1/2)+\epsilon}$.

Let E be an elliptic curve defined over a global field K. The analogue of the class group is the Shafarevich–Tate group $\text{Ш}(E/K)$ of E over K. For a place v of K, let K_v denote the completion of K at v. The Shafarevich–Tate group $\text{Ш}(E/K)$ is defined to be

$$\text{Ш}(E/K) := \text{Ker}\left(H^1(K,E) \to \prod_v H^1(K_v,E)\right),$$

where the cohomology groups are the Galois cohomology groups, and v runs over the places of K. The Shafarevich–Tate group measures the extent to which the

Hasse principle fails for E/K. It is conjectured that $Ш(E/K)$ is finite and this is known to hold for certain classes of elliptic curves. Morever an effective bound for $Ш(E/K)$ would be useful in computing a set of generators for the Mordell–Weil group $E(K)$ of K-rational points of E. Our results indicate that one can indeed obtain a bound analogous to the bound obtained for the class numbers of number fields, for elliptic curves over global fields of positive characteristic, provided one assumes the finiteness of Ш.

Manin ([11]) and Lang ([7]), conjectured bounds for the size of Ш based on various arithmetical invariants associated to the elliptic curve. Inspired by these conjectures, Mai and Murty ([8]) in 1992, predicted the growth of $Ш(E/\mathbf{Q})$ as satisfying,

$$|Ш| = O(N^{(1/2)+\epsilon}),$$

where N is the conductor of the elliptic curve. In ([9]), they produce an infinite family of elliptic curves $E/\mathbf{Q}$ such that,

$$|Ш(E)| \gg N^{(1/4)+\epsilon}.$$

Since ([8]) has never been published, I have included their argument in an appendix.

Some of the conjectures used in the argument over number fields, viz., Szpiro's conjecture and Lang's conjecture on lower bounds for the canonical heights of rational points, are known to hold over global fields of positive characteristic ([13, 5]). It would be thus of interest to verify this conjecture for global fields of positive characteristic.

However a fundamental problem for function fields, is that the estimate on the rank of the Mordell–Weil group of an elliptic curve is not as sharp as expected for number fields. Let k be a finite field of odd characteristic, with $q = p^f$ elements. Let C denote an irreducible, smooth projective algebraic curve over k with function field K, genus g, and Euler characteristic $\chi(C) = 2 - 2g$. Let K' be the function field of C over $\bar{k}$. Let E be an elliptic curve defined over K with conductor N. A. Brumer has shown ([1])

$$r(E) \leqslant \frac{\log(N)}{2\,\log(\log_q(N) - 4g + 4)} + O\left(\frac{(\log_q(N) - 4g + 4)\log^2(q)}{\sqrt{q}\,\log^2(\log_q(N) - 4g + 4)}\right),$$

where $r(E)$ is the rank of the Mordell–Weil group $E(K)$. Using this and arguing as in the case of number fields, provides an upper bound for Ш, which grows faster than any power of N, and will not provide the conjectured $O(N^{(1/2)+\epsilon})$. For details we refer to the last remark in the Appendix. Thus it does not seem to be possible to establish the desired bounds on Ш, arguing completely in analogy with the number fields.

For an abelian group A, let $A(l)$ denote the l-primary component of A. We have

https://doi.org/10.1023/A:1000105104709 Published online by Cambridge University Press

THEOREM 1. *Let E be an elliptic curve over K as above. Assume that* $\text{Ш}(l)$ *is finite for some prime l and that the j-invariant j_E of E is transcendental over k. Then*

$$|\text{Ш}(E)| \leqslant (16q)^{-\chi(C)/2}(2^{12}q)^{-p^e\chi(C)/2}N^{p^e((1/2)+(6\log(2)/\log(q))}$$

where p^e is the inseparable degree of K over $k(j_E)$.

In our proof, we work with the corresponding elliptic surface rather than directly working with the elliptic curve, and with the analogue of the Birch–Swinnerton Dyer conjecture for the surface. Instead of the regulator and the canonical height pairing for the elliptic curve, we have the Neron–Severi group of the surface and the intersection pairing on the divisors on the surface, which takes integral values. Morever the product over the periods occuring in the Birch–Swinnerton Dyer formula, is 'replaced' by the term $q^{\alpha(X)}$, which has an expression in terms of the cohomology of the surface, and is thus easier to compute.

2. Conjectures of Artin and Tate

Let X be the proper, minimal, regular model in the birational equivalence class of surfaces fibered over C and having generic fiber isomorphic to E. Let $\bar{X} = X \times_k \bar{k}$. Let $\pi : X \to C$ denote the projection map of X onto C. X is an elliptic surface and π has a natural section associated to the zero element of $E(K)$.

Let $P_2(X,T) = \det(1 - \phi_{2,l}T)$ denote the characteristic polynomial of the endomorphism $\phi_{2,l}$ of the etale cohomology groups $H^2_{\text{et}}(\bar{X}, \mathbf{Q}_l)$ induced by the Frobenius morphism on X. Deligne has shown in ([2]), that $P_2(X,T)$ is a polynomial with rational integral coeffecients, is independent of l, and that the analogue of the Riemann hypothesis holds i.e., $P_2(X,T) = \prod(1 - \lambda_\alpha T)$ with $|\lambda_\alpha| = q$.

Inspired by the Birch–Swinnerton Dyer conjecture, Tate ([19]) conjectured that the order of zeros of the L-function should be related to geometry of the cycles on X. In our situation the conjecture predicts that q^{-1} is a root of $P_2(X,T)$ with mutiplicity exactly $\rho(X)$, where $\rho(X)$, the base number of X, is the rank of the Néron-Severi group $NS(X)$ of X. $NS(X)$ is defined to be the image of $\text{Pic}(X)$ in $NS(\bar{X})$, the Néron-Severi group of $\bar{X}$, which is the group of divisors taken modulo algebraic equivalence. Under our hypothesis on the j-invariant of E, it is known by Néron's theorem of the base ([6]), that $NS(X)$ is a finitely generated abelian group.

Let $R(X,T) = P_2(X,T)/(1 - qT)^{\rho(X)}$. By Tate's conjecture $R(X,T)$ is a polynomial with rational integral coeffecients which does not vanish when $T = q^{-1}$.

In our situation, a theorem of Artin ([20]) applies, and we have that

$$\text{Br}(X) \simeq \text{Ш}(E/K),$$

where $\text{Br}(X)$ is the Brauer group of the surface X. Led by this result Artin and Tate formulated a geometric analogue of the Birch–Swinnerton Dyer conjecture,

https://doi.org/10.1023/A:1000105104709 Published online by Cambridge University Press

describing the leading coefficient of the L-function at the center of the critical strip, where the role of the Shafarevich–Tate group $\text{Ш}(E)$ is replaced by that of the Brauer group $\text{Br}(X)$ of X:

$$R(X, q^{-1}) = \frac{|\text{Br}(X)||\det(D_i, D_j)|}{q^{\alpha(X)}|NS(X)_{\text{tors}}|^2} \tag{1}$$

where $(D_i)_{1\leqslant i\leqslant \rho}$ is a base for $NS(X)$ modulo torsion. The symbol $(D_i,\ D_j)$ denotes the total intersection multiplicity of the divisors D_i and D_j. The term $|\det(D_i,\ D_j)|$ is the regulator for the intersection pairing on $NS(X)$.

$$\alpha(X) = \chi(X, \mathcal{O}_X) - 1 + \dim\,(\text{Pic}(X)). \tag{2}$$

It is known that $\alpha(X)$ is non-negative.

In ([20]) it is shown that if Tate's conjecture is assumed to hold for X, then the subgroup of elements of $\text{Br}(X)$, of order prime to p is finite, and (1) is true upto a power of p. In ([12]), Milne showed that the conjecture of Tate is equivalent to assuming the finiteness of $\text{Br}(X)(l)$ for some prime l which can also be p. Morever Milne showed that Tate's conjecture implies the conjecture of Artin and Tate. Consequently we have that if $\text{Ш}(E)(l)$ or equivalently $\text{Br}(X)(l)$ is finite for some prime l, then

$$|\text{Ш}(E/K)| = |\text{Br}(X)| = R(X, q^{-1})q^{\alpha(X)}\frac{|\text{NS}(X)_{\text{tors}}|^2}{|\det(D_i, D_j)|}. \tag{3}$$

Thus to obtain an estimate for $|\text{Br}(X)|$, we estimate each of the terms in the above expression for $|\text{Br}(X)|$, in terms of the conductor N.

3. Estimating the regulator

We need a description of the Néron-Severi group $\text{NS}(\bar{X})$ ([15]). Let K' be the function field of C over $\bar{k}$. It is known by the theorem of Lang–Néron ([6]), that under our assumption on E, i.e., the j-invariant of E being transcendental over k, that $E(K')$ is a finitely generated abelian group. Morever the torsion of $E(K')$ is generated by at most two elements $t_j, j\ \epsilon J, |J| \leqslant 2$ with orders n_j respectively. Let r, r' denote the rank of the Mordell–Weil groups $E(K), E(K')$ respectively. We have $r \leqslant r'$. Let $s_i, 1 \leqslant i \leqslant r'$ be a set of generators of $E(K')$ modulo torsion. Since X is proper, the group $E(K')$ is canonically identified with the group of sections of $\pi\colon \bar{X} \to \bar{C}$. Denote by (s) the image in $\bar{X}$ of the section of π corresponding to a rational element $s\epsilon E(K')$, and by $D(s)$ the divisor $(s) - (0)$ on $\bar{X}$.

For a place v of C, let X_v denote the fiber over v. Let S be the finite set of places on C, the ramification locus of the map $\pi\colon X \to C$, where the fiber X_v is singular. For $v\epsilon S$, let m_v be the number of irreducible components of the fiber $\bar{X}_v$ counted

https://doi.org/10.1023/A:1000105104709 Published online by Cambridge University Press

without multiplicity. Denote by $\Theta_{v,i}, (0 \leqslant i \leqslant m_v - 1)$ the irreducible components of the fiber X_v, with the convention that the (0) divisor meets $\Theta_{v,0}$. Let u_0 be a point on C outside S. If D_1, D_2 are two divisors on $\bar{X}$, denote by (D_1, D_2) the intersection multiplicity, which is a rational integer.

By decomposing divisors into 'horizontal' sections and 'vertical' fibers, it is shown in ([15]), that the Néron–Severi group $NS(\bar{X})$ is generated by $D(s_\alpha), (1 \leqslant \alpha \leqslant r'), D(t_j), j \in J, (0), \bar{X}_{u_0}, \Theta_{v,i}, (v \in S, 1 \leqslant i \leqslant m_v - 1)$, with the following relations for $j \in J$:

$$n_j D(t_j) \simeq n_j(D(t_j), (0))\bar{X}_{u_0} + \sum_{v,i} n_j(\Theta_{v,1}, \ldots \Theta_{v,m_v-1})$$

$$\times A_v^{-1}((D(t_j), \Theta_{v,1}), \ldots, (D(t_j), \Theta_{v,m_v-1}))^t, \tag{4}$$

where $\simeq$ denotes algebraic equivalence. A_v is the intersection matrix defined by the fiber $\bar{X}_v$, i.e., $(A_v)_{ij} = (\Theta_{v,i}\Theta_{v,j}), (1 \leqslant i, j \leqslant m_v - 1)$. It is known that A_v is invertible and negative definite.

Consequently it follows that the rank $\bar{\rho} = \rho(\bar{X})$ of $\mathrm{NS}(\bar{X})$ is given by

$$\rho(\bar{X}) = r' + 2 + \sum_{v \in S}(m_v - 1). \tag{5}$$

In order to estimate the regulator, we need the following result due to Shioda ([16, Theorem 3.1]).

PROPOSITION 2. *Suppose $\bar{X}$ is a non-isotrivial elliptic surface as above. Then numerically equivalent divisors are algebraically equivalent. Hence the Néron–Severi group* $\mathrm{NS}(\bar{X})$ *is torsion-free.*

Proof. Since this fact is of basic importance to us, we give a brief outline of the proof, following Shioda ([16]). Given a divisor D on $\bar{X}$ numerically equivalent to 0, by Grothendieck–Riemann–Roch, we have $\chi(\bar{X}, \mathcal{O}(D)) = \chi(\bar{X}, \mathcal{O}_{\bar{X}})$. By the formulas (11) and (12), and by our assumption that the j-invariant j_E of E is non-constant, we see that $\chi(\bar{X}, \mathcal{O}(D)) > 0$. Hence either $h^0(\mathcal{O}(D)) > 0$ or $h^2(\mathcal{O}(D)) > 0$.

If $h^0(\mathcal{O}(D)) > 0$, then D is linearly equivalent to an effective divisor and numerically equivalent to 0, which implies that D is algebraically equivalent to 0.

If $h^2(\mathcal{O}(D)) > 0$, then by duality $K - D$ is linearly equivalent to an effective divisor D', where K is the canonical divisor of $\bar{X}$. Since on an elliptic surface K is fibral, by our assumption on D, we have $(D', \Theta) = 0$, for any vertical divisor Θ on $\bar{X}$. This forces D' and hence D to be algebraically equivalent to a vertical divisor. Morever, it is easy to see from our assumption on D, and the non-degeneracy of the intersection pairing of the divisors on any fiber, that D is algebraically equivalent to 0 on $\bar{X}$.

Since the intersection pairing is non-degenerate on the group of divisors modulo numerical equivalence, this gives us that the Néron–Severi group $NS(\bar{X})$ is torsion-free.

This allows us to estimate $|NS(X)_{\text{tors}}|^2/|\det(D_iD_j)|$. Since $NS(X)$ is a subgroup of $NS(\bar{X})$ it is torsion free. The intersection numbers being rational integers, the determinant of the intersection matrix is an integer and we know it is non-zero. Hence we have

$$\frac{|\text{NS}(X)_{\text{tors}}|^2}{|\det(D_iD_j)|} \leqslant 1. \tag{6}$$

4. Estimating $R(X, q^{-1})$

Let $B_i (1 \leqslant i \leqslant 4)$ denote the Betti numbers of the surface X, the dimension of $H^i_{\text{et}}(\bar{X}, \mathbf{Q}_l)$ over $\mathbf{Q}_l$. The degree of the polynomial $P_2(X, T)$ is B_2. By the results of Artin and Ogg–Shafarevich–Grothendieck ([14]), one has a formula for the Picard number $B_2 - \bar{\rho}$, the dimension of the space of 'transcendental cycles' on $\bar{X}$, in terms of the exponents of the conductor.

Let M be a l-torsion abelian group which is 'cofinite', i.e., is of the form $(\mathbf{Q}_l/\mathbf{Z}_l)^s \times M_0$, M_0 a finite group. Then s is called as the corank of M. It is shown in ([4]), under our hypothesis on the map $\pi : \bar{X} \to \bar{C}$, that $B_2 - \bar{\rho}$ is the corank $r_0(l)$ of the l-torsion of $\text{Br}(\bar{X}) \simeq H^2(\bar{X}, \mathbf{G}_m)$.

Let η be the generic point of C. Arguing using the Leray spectral sequnece for the map π, Artin remarks that the map $H^1(\bar{C}, \pi_* X_\eta) \to H^2(\bar{X}, \mathbf{G}_m)$ has finite kernel and cokernel and hence the coranks are same. For almost all l, then the corank of $H^1(\bar{C}, \pi_* X_\eta)$ is given by the formula of Ogg–Shafarevich–Grothendieck as

$$r_0(l) = 4g - 4 - r' + \sum_v f_v,$$

where g is the genus of the curve C and f_v is the exponent of the conductor N of the elliptic curve E at v. Hence

$$B_2 - \bar{\rho} = 4g - 4 - r' + \sum_{v \in S} f_v. \tag{7}$$

Let Δ_v denote the minimal discriminant of E at v, and let $\text{ord}_v(\Delta_v)$ denote the exponent of the minimal discriminant Δ_v at v. We have the following important formula due to Ogg([18]), relating the exponents of the discriminant, the conductor and the number m_v of irreducible components, counted without multiplicity of the singular fibers

$$\text{ord}_v(\Delta_v) = f_v + m_v - 1. \tag{8}$$

Hence by (5) and (7), we have

$$B_2 = 4g - 2 + \sum_{v \in S} \text{ord}_v(\Delta_v). \tag{9}$$

https://doi.org/10.1023/A:1000105104709 Published online by Cambridge University Press

On the assumption that $\mathrm{Br}(X)(l)$ is finite for some prime l, we have by the results of Deligne and Milne, that $R(X,T) = \prod_\beta (1 - \lambda_\beta T)$ where $|\lambda_\alpha| = q$ and $\lambda_\alpha \neq q$. Hence $R(X, q^{-1}) = \prod_\beta (1 - w_\beta)$ with $|w_\beta| = 1, w_\beta \neq 1$. Morever the degree of $R(X,T)$ is $B_2 - \rho$, which is less than $B_2 - r - 2$, where r is the rank of $E(K)$, the Mordell–Weil group of E over K. Hence

$$\deg R(X,T) \leqslant 4g - 4 - r + \sum_{v \in S} \mathrm{ord}_v(\Delta_v)$$

Hence

$$\begin{aligned} |R(X, q^{-1})| &= \prod_\beta |(1 - w_\beta)| \\ &\leqslant 2^{-r} 2^{4g-4} . 2^{\Sigma_{v \in s}\, \mathrm{ord}_v(\Delta_v)}. \end{aligned} \tag{10}$$

5. Estimating $q^{\alpha(X)}$

Let $\mathcal{O}_X$ denote the structure sheaf of X. It is known for an elliptic surface, the irregularity $q = \dim(\mathrm{Pic}(\bar{X}))$ of $\bar{X}$ is the genus g of the curve C. By Weil's theory of Jacobians one has that $B_1 = 2q = 2g$. By duality $B_3 = 2g$. Hence from (9), it follows that the topological Euler characteristic $\chi_{top}(X) = \sum_i (-1)^i B_i$ is given by the following interesting formula

$$\chi_{\mathrm{top}}(X) = \sum_{v \in S} \mathrm{ord}_v(\Delta_v). \tag{11}$$

By semicontinuity we have $\chi(X, \mathcal{O}_X) = \chi(\bar{X}, \mathcal{O}_{\bar{X}})$. Morever it is known that canonical divisor is fibral, and is of the form $\pi^*(T)$, where T is a divisor on C. This gives us $K^2 = 0$, where K is the canonical bundle of X. Hence by Grothendieck–Riemann–Roch formula, we have

$$\chi(X)_{\mathrm{top}} = 12\chi(X, \mathcal{O}_X) \tag{12}$$

We have

$$\begin{aligned} \alpha(X) &= \chi(X, \mathcal{O}_X) - 1 + \dim(\mathrm{Pic}(X)) \\ &= \frac{1}{12} \left(\sum_{v \in S} \mathrm{ord}_v \Delta_v \right) + g - 1 \end{aligned} \tag{13}$$

by (2), (11) and (12).

Remark. It is expected that a decomposition as above for $\alpha(X)$, as a sum of local contributions from the ramified primes, should hold in general for any motive.

https://doi.org/10.1023/A:1000105104709 Published online by Cambridge University Press

However it is interesting to note that even though $\alpha(X)$ is an integer, the terms corresponding to the individual ramified places need not be integral. A different formula for $\alpha(X)$ has been obtained by Milne ([12]).

We would also like to recall a conjecture of Szpiro's, and which is known to hold over function fields of arbitrary characteristic ([13]),

$$\sum_v \mathrm{ord}_v(\Delta_v) \leqslant 6p^e \left\{ \sum_v f_v + 2g - 2 \right\}, \tag{14}$$

where p^e is the inseparable degree of K over $k(j_E)$. Hence we get by (13) and (14), an estimate for the 'period',

$$\begin{aligned} q^{\alpha(X)} &= (q^{\Sigma p_v^e f})^{1/2} q^{(p^e+1)(g-1)} \\ &\leqslant q^{-(p^e+1)\chi(C)/2} N^{p^e/2}. \end{aligned} \tag{15}$$

We can also express the estimate we obtained for $|R(X, q^{-1})|$ in terms of the conductor as

$$|R(X, q^{-1})| \leqslant 2^{-r} 2^{4g-4} 2^{6p^e} (\Sigma_v f_v + 2g - 2)$$

Now $N = \prod_v q_v^{f_v} \geqslant q^{\Sigma f_v}$, where q_v is the cardinality of the residue field at $v \epsilon S$ and we have $q_v \geqslant q$. So $\log(N)/\log(q) \geqslant \sum_{v \in S} f_v$ and $2^{\Sigma f_v} \leqslant 2^{\log(N)/\log(q)} = N^{\log(2)/\log(q)}$. Thus

$$|R(X, q^{-1})| \leqslant 2^{-r} (4^{-\chi(C)} 2^{-6p^e \chi(C)}) N^{6p^e (\log(2)/\log(q)}. \tag{16}$$

6.

Under the assumption that $\mathrm{Br}(X)(l)$ is finite for some prime l, and that the j-invariant of E is transcendental over k, we get from (3), (6), (15) and (16),

$$\begin{aligned} &|\mathrm{Ш}(E/K)| \\ &\quad = |\mathrm{Br}(X)| \\ &\quad \leqslant 2^{-r} (16q)^{-\chi(C)/2} (2^{12} q)^{-p^e \chi(C)/2} N^{p^e} ((1/2) + (6 \log(2)/\log(q)). \end{aligned}$$

Remark. It is interesting to notice the terms which contribute to $N^{1/2}$ in the function field and the number field. Over number fields it is the infinite period π_∞ which satisfies the relation $|\pi_\infty| \geqslant H^{1/12}$, where H is the height of the elliptic curve which seems to be contributing to the $N^{1/2}$ term. In the function fields it is the term $q^{\alpha(X)}$ which contributes. One has an 'analogous' relationship $\chi(X)_{\mathrm{top}} = 12\chi(X, \mathcal{O}_X)$. This is in agreement with the belief that the archimedean places are to be considered as 'ramified' places for an elliptic curve, and the formula

https://doi.org/10.1023/A:1000105104709 Published online by Cambridge University Press

(13), expressing $\alpha(X)$ as a sum of contributions over the ramified primes of the elliptic curve.

Appendix*

Let E be an elliptic curve over **Q** of conductor N and minimal discriminant Δ. Let Ш denote the Shafarevich–Tate group of E. Manin ([11]) and Lang ([7]) have suggested that the Birch–Swinnerton Dyer conjecture can be used to give upper bounds for Ш. Using methods of analytic number theory Mai and Murty ([8]), conjectured the following

CONJECTURE 1. *For any* $\epsilon > 0$,

$$|Ш| = O(N^{(1/2)+\epsilon}),$$

where the implicit constant depends only on ϵ.
In fact they make the stronger

CONJECTURE 2. *There is an absolute constant* c *such that*

$$|Ш| = O\left(H^{(1/12}\exp\left(c\frac{\log N}{\log\log N}\right)\right),$$

where the implied constant is absolute and where H *is a naive height of* E *defined as follows*

Let $y^2 = x^3 + ax + b$ be an equation for E over **Q**. Define

$$H = \max(|a|^3, |b|^2).$$

Let $L_E(s)$ be the L-series associated to E. Define

$$S_E(1+it) = \arg L_E(1+it),$$

where the argument is obtained by continuous variation along the straight lines joining $2, 2+it, \frac{1}{2}+it$ starting with value zero, provided t is not the ordinate of a zero. Define $S_E(t) = \lim_{\epsilon\to 0} S_E(t+\epsilon)$, if t is the ordinate of a zero of $L_E(s)$. In analogy with a conjecture of Montgomery, we make

CONJECTURE 3. *For* $|t| > 2$

$$S_E(t) = O\left(\left(\frac{\log Nt}{\log\log Nt}\right)^{1/2}\right)$$

* I would like to thank Ram Murty for allowing me to include the results of ([8]) here. R. Murty informs me that these conjectures were presented at the Newton Institute in May 1993, but were never published.

https://doi.org/10.1023/A:1000105104709 Published online by Cambridge University Press

By arguments as in ([21], page 354) and by using the Phragmen–Lindelof theorem as in ([10]), it can be seen that

THEOREM. *Assuming Conjecture* 3, *we have*

$$|L_E(1+it)| \leqslant \exp\left(A\left(\frac{\log\ Nt}{\log\log\ Nt}\right)^{1/2}\right) \tag{17}$$

for some absolute constant A.

COROLLARY. *If* $r = \text{ord}_{s=1}L_E(s)$ *and Conjecture* 3 *is true, then*

$$r = O\left(\left(\frac{\log\ N}{\log\log\ N}\right)^{1/2}\right), \tag{18}$$

where the implied constant is absolute

Proof. Let C be a circle of radius $1/\log\log\ N$ centred at 1. By Jensen's theorem, we have

$$\begin{aligned} r &\leqslant \log \max_{z\varepsilon C}|L_E(z)| \\ &= O\left(\left(\frac{\log\ N}{\log\log\ N}\right)^{1/2}\right) \end{aligned}$$

by the above theorem.

We recall now a conjecture of Lang on lower bounds for the canonical height of rational points on E. Let h denote the canonical Neron–Tate height on E.

CONJECTURE (Lang). *For any non-torsion rational point* $P \in E(\mathbf{Q})$,

$$h(P) \gg \log\ \alpha|\Delta|$$

for some positive constant α, *which does not depend on* E.

This conjecture has been proved by Silverman in the case that E has integral j-invariant.

We also recall a conjecture of Szpiro and Hall relating the height and the conductor of the elliptic curve E.

CONJECTURE (Szpiro, Hall).

$$H \ll N^{6+\epsilon},$$

where the constant depends on ϵ.

THEOREM. *Let* E *be a modular elliptic curve over* $\mathbf{Q}$ *satisfying the Birch–Swinnerton Dyer conjecture, Conjecture* 3, *and the conjecture of Lang stated above. Then there exists an absolute constant* A *such that*

$$|\text{Ш}| \ll H^{1/12}\exp\left(A\frac{\log\ N}{\log\log\ N}\right).$$

https://doi.org/10.1023/A:1000105104709 Published online by Cambridge University Press

Proof. Let r be the order of the zero of $L_E(s)$ at $s = 1$. Birch and Swinnerton–Dyer conjecture that

$$\frac{L^{(r)}(1)}{r!} = \frac{|\text{Ш}|R}{2^r|E(\mathbf{Q})_{\text{tors}}|^2}\pi_\infty \prod_{p'} \pi_p,$$

where π_p are certain integers, R is the regulator of E and π_∞ is a suitably chosen infinite period of E. Applying Cauchy's theorem to a circle of radius $1/\log\log\ N$ centred at 1, and by the estimate (17), we have

$$\frac{L^{(r)}(1)}{r!} \ll \exp\left(c\left(\frac{\log N}{\log\log\ N}\right)^{1/2}\right)(\log\log\ N)^{r+2},$$

where c is an absolute constant. Mazur has shown that $|E(\mathbf{Q})_{\text{tors}}| \leqslant 16$. The π_p are integers. For the real period Lang has shown that

$$|\pi_\infty| \gg H^{-1/12}.$$

From Lang's conjecture stated above, it follows using Hermite's theorem (see [7]), that

$$R \gg (\sqrt{3}/2)^{r^2}(\log|\Delta|)^r.$$

This lower bound for the volume of a lattice is sharp, and neither $\sqrt{3}/2$ nor the power r^2 can be improved upon. Thus we have

$$|\text{Ш}| \ll H^{1/12}\exp\left(c\left(\frac{\log\ N}{\log\log\ N}\right)^{1/2}\right) \times(2\ \log\log\ N)^{r+2}(2/\sqrt{3})^{r^2}(\log|\Delta|)^{-r}.$$

As $r = O((\log\ N/\log\log\ N)^{1/2})$, we have

$$|\text{Ш}| \ll H^{1/12}\exp\left(A\frac{\log\ N}{\log\log\ N}\right)$$

for some absolute constant A.

COROLLARY. *If we further assume Szpiro's conjecture, then*

$$|\text{Ш}| \ll N^{(1/2)+\epsilon}.$$

Conversely, we remark that if the above upper bound for Ш fails to hold, then our arguments indicate that there should exist elliptic curves of large rank.

https://doi.org/10.1023/A:1000105104709 Published online by Cambridge University Press

Remark. In view of the fact that $(2/\sqrt{3})^{r^2}$ occurs in the estimate for III, and $2/\sqrt{3} > 1$, it is of extreme importance to have the square root in the estimate (18) for the rank r. An upper bound for r of the form $O(\log N/\log\log N)$, will give an upper bound for III, which grows faster than any power of N.

Acknowledgement

I would like to express my sincere thanks to M. Ram Murty, for suggesting this problem and for many useful discussions. This work was done when the author was at McGill University, Montreal, for the year 1994–95. I would like to express my gratitude to McGill University and my colleagues at Montreal for their warm hospitality and support.

After this paper was written, I received a preprint 'Bounds for the order of the Tate–Shafarevich group' by D. Goldfeld and L. Szpiro, which also provides estimates for III. However since their arguments are similar to that of number fields, their methods give upper bounds for III, which seem to grow faster than any power of the conductor N, and do not give the expected upper bound $O(N^{1/2+\epsilon})$.

References

1. Brumer, A.: The average rank of elliptic curves I, *Inv. Math.* 109 (1992) 445–472.
2. Deligne. P.: La conjecture de Weil *I*, *Publ. Math. IHES* 43 (1974) 273–307.
3. Goldfeld, D. and Szpiro, L.: Bounds for the order of the Tate–Shafarevich group, *Comp. Math.* 97 (1995) 71–87.
4. Grothendieck, A.: *La groupe de Brauer* II, Dix Exposés sur la cohomologie des Schemas, eds. A. Grothendieck and N. H. Kuiper, North-Holland, Amsterdam, 1968.
5. Hindry, M. and Silverman, J. S.: The canonical height and integral points on elliptic curves, *Inv. Math.* 93 (1988) 419–450.
6. Lang, S.: *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, (1983).
7. Lang, S.: *Conjectured Diophantine estimates on elliptic curves*, Arithmetic and Geometry–Papers dedicated to I. R. Shafarevich on his sixtieth birthday, Vol. I, eds. M. Artin and J. Tate, Birkhauser.
8. Mai, L. and Murty, M. R.: *On the Shafarevich–Tate group*, unpublished.
9. Mai, L. and Murty, M. R.: *A note on quadratic twists of elliptic curves*, CRM Proceedings and Lecture Notes, Vol. 4, eds. Kisilevsky and Murty, 1994.
10. Mai, L. and Murty, M. R.: *The Phragmen–Lindelof theorem and modular elliptic curves*, Contemporary Math., vol. 166, 1994.
11. Manin, Yu.: Cyclotomic fields and modular curves, *Russian Math Surveys* 26 (1971) no.6, 7–78.
12. Milne, J. S.: On a conjecture of Artin and Tate, *Ann of Math.* 102 (1975) 517–533.
13. Pesenti, J. and Szpiro, L.: *Discriminant et conducteur des courbes elliptiques non semi-stable*, preprint.
14. Raynaud, M.: *Characteristique d'Euler–Poincaré et cohomologie des variétes abeliennés*, Dix Expos'es sur la cohomologie des schemas, eds. A. Grothendieck and N. H. Kuiper, North-Holland, Amsterdam, 1968.
15. Shioda, T.: On elliptic modular surfaces, *Journal of the Math. Soc. of Japan* 24 (1972) 20–59.
16. Shioda, T.: On the Mordell–Weil lattices, *Comment. Math. Univ. St. Pauli* 39 (1990) 211–240.
17. Silverman, J. H.: *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, New York, 1986.
18. Silverman, J. H.: *Advanced topics in the arithmetic of elliptic curves*, GTM 151, Springer-Verlag, New York, 1994.
19. Tate, J.: *Algebraic cycles and poles of zeta-functions*, Arithmetical Algebraic Geometry, Harper and Row, New York (1965).

20. Tate, J.: *On a conjecture of Birch and Swinnerton–Dyer and a geometric analogue*, Dix Exposés sur la Cohomologie des Schemas, eds. A. Grothendieck and N. H. Kuiper, North-Holland, Amsterdam, 1968.
21. Titchmarsh, E. C.: *The theory of the Riemann zeta function*, revised by D. R. Heath-Brown, Oxford, 1986.
22. Zimmert, R.: Ideale kleiner Norm in Idealklassen und eine Regulatorabschatzung, *Inv. Math.* 62, 367–380, (1980).