Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Number Theory 105 (2004) 333–343

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

An application of Mumford's gap principle

Jung-Jo Lee and M. Ram Murty[*,1]

Department of Mathematics, Queen's University, Kingston, Ont., Canada K7L 3N6

Received 3 May 2003

Communicated by A. Granville

Abstract

We study a Dirichlet series attached to a polynomial first defined by Rubin and Silverberg in their study of ranks of quadratic twists of a fixed elliptic curve. We apply Mumford's gap principle to show that the series converges if the associated polynomial has distinct roots and degree at least 5.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$. Suppose that E is defined by the Weierstrass equation

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

The quadratic twist, denoted E_D, of E is given by

$$Dy^2 = x^3 + ax + b.$$

By a celebrated theorem of Mordell, the group of rational points, $E_D(\mathbb{Q})$, of E_D is a finitely generated abelian group. Its rank has been the study of numerous papers such as [G,H,RS1,RS2].

Honda [H] has made the surprising conjecture that $\text{rank}_{\mathbb{Z}} E_D(\mathbb{Q})$ is bounded as D varies over all integers. At present, there is no evidence for or against this conjecture, although in the case of function fields over finite fields, there are analogous works by

*Corresponding author.
E-mail address: murty@mast.queensu.ca (M.R. Murty).
[1] Research partially supported by an NSERC grant.

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2003.11.006

Shafarevich and Tate [ST] and Ulmer [U]. In a related context, Goldfeld [G] has conjectured that "on average" $\mathrm{rank}_{\mathbb{Z}} E_D(\mathbb{Q})$ is $\frac{1}{2}$. More precisely, Goldfeld conjectured that

$$\#\{|D|\leqslant x : \mathrm{rank}_{\mathbb{Z}} E_D(\mathbb{Q}) = 0\} \sim \#\{|D|\leqslant x : \mathrm{rank}_{\mathbb{Z}} E_D(\mathbb{Q}) = 1\} \sim \tfrac{1}{2}\#\{|D|\leqslant x\}$$

and

$$\#\{|D|\leqslant x : \mathrm{rank}_{\mathbb{Z}} E_D(\mathbb{Q})\geqslant 2\} = o(x)$$

as $x\to\infty$.

Perhaps motivated by these conjectures, Rubin and Silverberg [RS1] derived the following equivalent formulation of Honda's conjecture.

For each natural number n, let

$$n = \prod_p p^{v_p(n)}$$

be its unique factorization as a product of prime powers. Define the square-free part of n by

$$\mathrm{sf}(n) = \prod_{v_p(n)\ \text{odd}} p.$$

If n is a negative integer, we let $\mathrm{sf}(n) = -\mathrm{sf}(-n)$.

Now let

$$g(x) = x^3 + ax + b$$

and set

$$G(u,v) = v^4\, g\left(\frac{u}{v}\right) = v(u^3 + auv^2 + bv^3).$$

For $(u,v) = 1$, define the height $h(u/v) = \max\{1, \log|u|, \log|v|\}$. It is the "naive" height with only a finite number of exceptions so that it takes positive values. Define the series

$$S_g(j,k) := \sum_{\substack{(u,v)=1\\ G(u,v)\neq 0}} \frac{1}{|\mathrm{sf}(G(u,v))|^k h(u/v)^j}.$$

Theorem 1 (Rubin, Silverberg [RS1,RS2]). *If j is a positive real number, then the following conditions are equivalent*:

(a) $\mathrm{rank}_{\mathbb{Z}} E_D(\mathbb{Q}) < 2j$ *for every* $D\in\mathbb{Z}\backslash\{0\}$;
(b) $S_g(j,k)$ *converges for some* $k\geqslant 1$;
(c) $S_g(j,k)$ *converges for every* $k\geqslant 1$.

Their theorem suggests the study of the cognate series defined as follows.

Let $f(x)$ be a monic polynomial of degree r with coefficients in $\mathbb{Z}$ and with distinct roots. Let

$$F(u,v) = \begin{cases} v^r f\left(\frac{u}{v}\right) & \text{if } r \text{ is even}, \\ v^{r+1} f\left(\frac{u}{v}\right) & \text{if } r \text{ is odd}. \end{cases}$$

Consider the sum

$$S_f(j,k) = \sum_{\substack{(u,v)=1 \\ F(u,v)\neq 0}} \frac{1}{|\mathrm{sf}(F(u,v))|^k h(u/v)^j}.$$

We prove:

Theorem 2. *If $r \geqslant 5$, then $S_f(j,k)$ converges for every $k>1$ and any positive real number j.*

We remark (as noted in [RS1]) that Theorem 2 is an immediate consequence of a conjecture of Caporaso et al. [CHM], namely that the number of rational points on a curve (defined over $\mathbb{Q}$ say) of genus g is bounded by a constant depending only on g, for $g \geqslant 2$. They prove that their conjecture is a consequence of the Bombieri–Lang–Vojta conjecture on distribution of rational points on varieties of general type. Indeed, if we write $m = \mathrm{sf}(F(u,v))$, then

$$S_f(j,k) = \sum_{m=1}^{\infty} \frac{\mu^2(m)}{m^k} \left(\sum_{\substack{(u,v)=1 \\ 0\neq F(u,v)=\pm my^2}} \frac{1}{h(u/v)^j} \right),$$

where μ is the Möbius function, and the inner sum is uniformly bounded because

$$f\left(\frac{u}{v}\right) = \pm m \left(\frac{y}{v^{r/2}}\right)^2 \quad \text{if } r \text{ is even}$$

and

$$f\left(\frac{u}{v}\right) = \pm m \left(\frac{y}{v^{(r+1)/2}}\right)^2 \quad \text{if } r \text{ is odd}$$

has a uniformly bounded number of solutions assuming the Caporaso, Harris and Mazur conjecture. Thus the series converges for $k>1$ and $j \geqslant 0$.

Our goal in this paper is to prove Theorem 2 unconditionally. We will give two proofs of Theorem 2. The first one will have fewer prerequisites. The second will use the deeper work of Vojta [V] on effective versions of Faltings theorem concerning Mordell's conjecture. Our main tool will be Mumford's gap principle (see [La, p. 120], [Mu]) which we now describe.

2. Mumford's gap principle

Let $K/\mathbb{Q}$ be a number field, C/K a hyperelliptic curve of genus $g \geqslant 2$, J/K the Jacobian variety of C. Let

$$e : C \hookrightarrow J$$

be an embedding of C into J of the form

$$P \mapsto [(P) - (P_0)]$$

for a fixed base point $P_0 \in C(\bar{K})$.

We assume that P_0 is chosen so that $\Theta = e(C^{g-1})$ is a symmetric divisor on J. Let $\hat{h}$ be the logarithmic canonical height on J with respect to Θ. (See [La, p. 113] for details.)

We have an inner product on $J(\bar{K})$ corresponding to $\hat{h}$ given by

$$\langle P, Q \rangle = \tfrac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)).$$

The norm on the points of $J(\bar{K})$ is defined accordingly as

$$|P| = \sqrt{\langle P, P \rangle}.$$

From the well-known property of the canonical height that $\hat{h}(kP) = k^2\hat{h}(P)$ for any natural number k, we have

$$|P| = \sqrt{\langle P, P \rangle} = \sqrt{\tfrac{1}{2}(\hat{h}(2P) - 2\hat{h}(P))} = \sqrt{\hat{h}(P)}.$$

Having fixed e, we identify points on $C(\bar{K})$ with their images in $J(\bar{K})$.

Proposition 3 (Mumford [Mu]). *With notations as above, there is a constant* $\gamma_2 = \gamma_2(C/K)$ *such that for any two distinct points* $P, Q \in C(\bar{K})$, *we have*

$$\langle P, Q \rangle \leqslant \frac{|P|^2 + |Q|^2}{2g} + \gamma_2.$$

As is well-known, Mumford's gap principle implies that rational points are *thinly* distributed. More precisely, Mumford [Mu] showed that if $\{x_n\}$ is a sequence of distinct points in $C(\bar{K})$ lying in some finitely generated subgroup of $J(\bar{K})$ and ordered by increasing height then there is an integer N and a number $a > 1$ such that

$$|x_{n+N}| \geqslant a|x_n|.$$

Mumford then deduced that $|x_n|$ grows exponentially. In this sense, the points of $C(\bar{K})$ are sparsely distributed in $J(\bar{K})$.

For our purpose, we need to make the argument of Mumford more explicit. To this end, the following lemma, due to Silverman [Si] will be useful.

Lemma 4. *Let $0<\theta_0<\frac{\pi}{2}$ be a fixed angle, and let $z_1, \dots, z_N \in \mathbb{R}^d$ be a collection of points in $\mathbb{R}^d$. If*

$$N > \frac{(d-1)\pi}{2\sin^{d-1}(\theta_0/2)},$$

then there are distinct indices $i \neq j$, such that

$$\langle z_i, z_j \rangle \geqslant |z_i||z_j| \cos \theta_0.$$

Proof. See [Si, p. 388]. A related packing argument can also be found in [K]. □

If we define the cosine between two vectors v and w by

$$\cos(v, w) := \frac{\langle v, w \rangle}{|v||w|},$$

we may write the Mumford's inequality as

$$g \cos(P, Q) \leqslant \frac{1}{2}\left(\frac{|P|}{|Q|} + \frac{|Q|}{|P|}\right) + \frac{\gamma_2}{|P||Q|},$$

provided $|P|$, $|Q|$ are non-zero.

Now fix θ_0 as in Lemma 4. We apply the lemma to the elements x_i with

$$R + 1 \leqslant i \leqslant R + N$$

where R is any non-negative integer and

$$N = \left[\frac{(d-1)\pi}{2\sin^{d-1}(\theta_0/2)}\right] + 1.$$

By the lemma, there is a pair $R < i < j \leqslant R + N$ such that

$$\cos \theta_0 \leqslant \cos(x_i, x_j).$$

Thus, by Mumford's inequality

$$g \cos \theta_0 \leqslant g \cos(x_i, x_j) \leqslant \frac{1}{2}\left(\frac{|x_i|}{|x_j|} + \frac{|x_j|}{|x_i|}\right) + \frac{\gamma_2}{|x_i||x_j|}.$$

The function $f(s) = \frac{1}{2}(s + s^{-1})$ is easily analyzed and we see that it takes its minimum (for $s>0$) at $s = 1$ with $f(1) = 1$.

If we insist that $|x_i| > 2\sqrt{\gamma_2}$ (say), then with θ_0 chosen close to 0, we obtain

$$g(1-\varepsilon) = g\cos\theta_0 \leqslant \frac{1}{2}\left(\frac{|x_i|}{|x_j|} + \frac{|x_j|}{|x_i|}\right) + \frac{1}{4}.$$

As $g \geqslant 2$, this implies there is an a (depending only on ε) so that

$$|x_j| \geqslant a|x_i|.$$

Moreover, $a > 1$. [In fact, if $|x_i|$ is very large, ε small, then a is approximately the number s such that $s + s^{-1} = 2g$.] The important point is that a depends only on γ_2 (with ε chosen sufficiently small). We record our observation in the following.

Lemma 5. *Let C be a curve of genus $g \geqslant 2$ defined over a number field K. Let*

$$e : C \hookrightarrow J$$

be the embedding of C into its Jacobian as before. Let $\hat{h}$ be the canonical height on J with respect to Θ. There exists a constant γ_2 depending only on C and an absolute constant $a > 1$ such that if L is any finite extension of K, and $\{x_n\}$ is the sequence of points of $C(L)$ ordered by increasing height, then for $|x_n| > 2\sqrt{\gamma_2}$, we have

$$|x_{n+N}| \geqslant a|x_n|$$

for N explicitly given in terms of $d = \operatorname{rank} J(L)$. In fact, we have $N \asymp dc_1^d$ for some constant c_1 which depends only on θ_0 of Lemma 4.

Proof. This follows immediately from the preceding discussion. It is an effective version of the Mumford's gap principle, analogous to Theorem 8.1 of [La, p. 135].

Remark. Several authors have discussed effective versions of Mumford's theorem. The first such statement seems to be in [Si] and later in [Di, p. 92]. As these latter presentations do not state the result in the form we need it, we have given the discussion above, closely following [La,Si].

We now apply this to the case of a hyper-elliptic curve. Let $f(x)$ be a polynomial with $\mathbb{Z}$-coefficients, of degree $r \geqslant 5$, and with distinct roots. Then the curve

$$C : y^2 = f(x)$$

has genus $g \geqslant 2$ (see [Si2, p. 44]).

If we are interested in the rational points of the twists

$$C_m : my^2 = f(x),$$

then these can be viewed as points of $C(L)$ with $L = \mathbb{Q}(\sqrt{m})$. The Mordell–Weil theorem tells us that if J_m is the Jacobian of C_m, then $J_m(L)$ is finitely generated.

Moreover, if $y \neq 0$, then the height of a rational point $P = (x, y) \in C_m(\mathbb{Q})$ satisfies (see [Si3])

$$\hat{h}(P) \gg \log |m|.$$

We will need the following well-known result of Northcott in later discussions.

Proposition 6 (Northcott). *Let K be a number field, V/K a projective variety and $h : V(\bar{K}) \to \mathbb{R}$ an absolute logarithmic height relative to an ample divisor on V. Then for all numbers d, and H, the set*

$$\{P \in V(\bar{K}) : [K(P) : K] \leqslant d \quad \textit{and} \ h(P) \leqslant H\}$$

is finite.

Proof. See [La, p. 59].

With a view to proving Theorem 2, we record below the consequence of the preceding discussion to our situation.

Proposition 7. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $r \geqslant 5$ and with distinct roots. Let*

$$F(u, v) = \begin{cases} v^r f\left(\frac{u}{v}\right) & \text{if } r \text{ is even,} \\ v^{r+1} f\left(\frac{u}{v}\right) & \text{if } r \text{ is odd.} \end{cases}$$

There are constants γ_3 and c, depending only on f, such that for $|m| > \gamma_3$, we have

$$\sum_{\substack{(u,v)=1 \\ 0 \neq F(u,v) = my^2}} \frac{1}{h(u/v)^j} \ll c^{\operatorname{rank}_{\mathbb{Z}} J_m(\mathbb{Q})}$$

for any positive real number j.

Proof. First, note that $y \neq 0$. We choose m sufficiently large to ensure all rational points of C_m have height $> 2\sqrt{\gamma_2}$ so that we can apply Lemma 5. The points (u, v) with u, v coprime and satisfying

$$F(u, v) = my^2$$

correspond to the points

$$P = \left(\frac{u}{v}, \pm \frac{\sqrt{m}y}{v^{r/2}}\right)$$

(if r is even) and

$$P = \left(\frac{u}{v}, \pm \frac{\sqrt{m}y}{v^{(r+1)/2}}\right)$$

(if r is odd) in the set $C(\mathbb{Q}(\sqrt{m}))$ of the hyper-elliptic curve

$$C : y^2 = f(x).$$

We order the countable set of points in $C(\mathbb{Q}(\sqrt{m}))$ in the order of increasing height to have a sequence $\{x_n\}$. (Of course, by Faltings theorem, this is a finite sequence but we are not assuming Faltings theorem.)

Let $h_x(P)$ denote the naive height on the x-coordinate of P. Then

$$h_x(P) \asymp \hat{h}(P).$$

By Northcott's theorem (Proposition 6),

$$\bigcup_K J(K)_{\text{tor}},$$

where the union is over all quadratic extensions of $\mathbb{Q}$, is a finite set. Thus, if a torsion point lies in infinitely many $C(\mathbb{Q}\sqrt{m})$, then $y = 0$ necessarily. In other words, if m is sufficiently large, then the only torsion points of $F(u, v) = my^2$ come from points with $y = 0$, and these have been eliminated from the sum under consideration. Thus we see that the convergence of the sum in question is determined by

$$\sum_{x_n \in C(\mathbb{Q}(\sqrt{m})) - C(\mathbb{Q}(\sqrt{m}))_{\text{tor}}} \frac{1}{\hat{h}(x_n)^j}.$$

We partition the indices n in this sum into residue classes (mod N) with N given as in Lemma 5. For each such residue class $t(\bmod N)$, and $n = qN + t$, we have by Lemma 5

$$\hat{h}(x_n) = |x_n|^2 > a^{2q}|x_t|^2 = a^{2\cdot(n-t)/N}|x_t|^2.$$

As $a > 1$, we find that for each residue class $t(\bmod N)$, the contribution is

$$\ll |x_t|^{-2j}.$$

Summing this for $t(\bmod N)$ gives an estimate of $O(N)$ as the bound for the sum in question. Then

$$N \asymp (\text{rank}_{\mathbb{Z}} J_m(\mathbb{Q}))c_1^{\text{rank}_{\mathbb{Z}} J_m(\mathbb{Q})}$$

gives us an upper bound

$$N \ll c^{\mathrm{rank}_{\mathbb{Z}} J_m(\mathbb{Q})}$$

with $c = 2c_1$ as our final estimate for the sum. □

3. Proof of Theorem 2

We will show that $S_f(j,k)$ converges for $k>1$ and any positive real number j. We write the sum as

$$\sum_{m=1}^{\infty} \frac{\mu^2(m)}{m^k} \sum_{\substack{(u,v)=1 \\ 0 \neq F(u,v) = \pm my^2}} \frac{1}{h(u/v)^j}.$$

If m is sufficiently large, say $m > \gamma_3$, then we can apply the estimate of Proposition 7 to deduce the convergence of the series. If $\hat{h}(P)$ is sufficiently large, say $\hat{h}(P) > 4\gamma_2$, then we still can apply Lemma 5 so that the arguments of Proposition 7 remain valid to deduce the convergence. Here γ_2 and γ_3 are as given in Lemma 5 and Proposition 7. The sum of the remaining terms is finite by the result of Northcott. (See Proposition 6.) From $\hat{h}(P) \asymp h(P)$, we know that there exists a constant H such that if $\hat{h}(P) \leqslant 4\gamma_2$ then $h(P) \leqslant H$ to apply Proposition 6.

Thus, in analyzing $S_f(j,k)$, we may apply Proposition 7. We deduce

$$S_f(j,k) \ll \sum_{m=1}^{\infty} \frac{c^{\mathrm{rank}_{\mathbb{Z}} J_m(\mathbb{Q})}}{m^k}.$$

There are several ways to complete the proof. The standard descent argument (see [Si2]) gives

$$\mathrm{rank}_{\mathbb{Z}} J_m(\mathbb{Q}) \ll v(m) + O(1)$$

where $v(m)$ denotes the number of prime divisors of m (see [H, p. 95] or [Si], [Si1]).

We have the estimate, for any $\varepsilon > 0$

$$c^{v(m)} \ll m^{\varepsilon}$$

which gives the desired result. This completes the proof of Theorem 2.

4. An alternate proof

As a consequence of his work on effective versions of Faltings theorem on Mordell's conjecture, Vojta [V], [Bo] proved the following bound. (See [HS, Exercise

E.2].) Let C/K be a curve of genus $\geqslant 2$ defined over a number field K, let $h : C(\bar{K}) \to \mathbb{R}$ be a height function on C corresponding to a projective embedding of C, and let J/K be the Jacobian variety of C. There is a constant γ (depending only on C/K) such that for all extensions L/K,

$$\#\{P \in C(L) : h(P) \geqslant \gamma\} \leqslant \#J(L)_{\text{tor}}(\log_2 \gamma) 10^{\operatorname{rank} J(L)}.$$

If we vary over extensions L of fixed degree, then Northcott's theorem (Proposition 6) implies that $\#J(L)_{\text{tor}}$ is uniformly bounded. Thus, the sum appearing in Theorem 2 is bounded by

$$\ll \sum_{m=1}^{\infty} \frac{10^{\operatorname{rank}_{\mathbb{Z}} J_m(\mathbb{Q})}}{m^k},$$

which by the previous argument, converges for $k > 1$ if we use the bound

$$v(m) = O\left(\frac{\log m}{\log \log m}\right).$$

However, Vojta's theorem is rather deep. Our purpose here was to prove Theorem 2 using the "simpler" result embodied in Mumford's gap principle.

Acknowledgments

We are thankful to Joseph Silverman, Ernst Kani, Michael Roth and the referee for providing comments and suggestions.

References

[Bo] E. Bombieri, The Mordell conjecture revisited, Ann. Scuola Norm. Sup. Pisa Ser. IV 17 (1990) 615–640;
E. Bombieri, Corrigendum, 18 (1991) 473.

[CHM] L. Caporaso, J. Harris, B. Mazur, Uniformity of rational points, J. Amer. Math. Soc. 10 (1997) 1–35.

[Di] T. de Diego, Points rationnels sur les familles de courbes de genre au moins 2, J. Number Theory 67 (1997) 85–114.

[G] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, in: M.B. Nathanson (Ed.), Number Theroy, Carbondale 1979 (Proc. Southern Illinois Conf., 1979).

[HS] M. Hindry, J. Silverman, Diophantine Geometry, GTM 201, Springer-Verlag, Berlin, 2000.

[H] T. Honda, Isogenies, rational points and section points of group varieties, Jpn. J. Math. 30 (1960) 84–101.

[K] E. Kani, Bounds on the number of non-rational subfields of a function field, Invent. Math. 85 (1986) 185–198.

[La] S. Lang, Fundamentals of Diophantine Geometry, Springer-Verlag, New York, 1994.

[Mu] D. Mumford, A remark on Mordell's conjecture, Amer. J. Math. 87 (4) (1965) 1007–1016.

[RS1] K. Rubin, A. Silverberg, Ranks of elliptic curves in families of quadratic twists, Exp. Math. 9 (4) (2000) 583–590.
[RS2] K. Rubin, A. Silverberg, Ranks of elliptic curves, Bull. Amer. Math. Soc. 39 (2002) 455–474.
[Si] J. Silverman, A uniform bound for rational points on twists of a given curve, J. London Math. Soc. 47 (2) (1993) 385–394.
[Si1] J. Silverman, Representations of integers by binary forms and the rank of the Mordell–Weil group, Invent. Math. 74 (1983) 281–292.
[Si2] J. Silverman, The Arithmetic of Elliptic Curves, Springer, Berlin, 1986.
[Si3] J. Silverman, Lower bounds for height functions, Duke Math. J. 51 (1984) 395–403.
[ST] I.R. Shafarevich, J. Tate, The rank of elliptic curves (Russian), Dokl. Akad. Nauk SSSR 175 (1967) 770–773.
[U] D. Ulmer, Elliptic curves with large rank over function fields, Ann. of Math. 155 (2,1) (2002) 295–315.
[V] P. Vojta, Siegel's theorem in the compact case, Annals of Math. 133 (1991) 509–548.