Forum Math. **19** (2007), 677–705
DOI 10.1515/FORUM.2007.026

Forum Mathematicum

Dirichlet series and hyperelliptic curves

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

(Communicated by Peter Sarnak)

Abstract. For a fixed hyperelliptic curve C given by the equation $y^2 = f(x)$ with $f \in \mathbb{Z}[x]$ having distinct roots and degree at least 5, we study the variation of rational points on the quadratic twists C_m whose equation is given by $my^2 = f(x)$. More precisely, we study the Dirichlet series $\mathscr{D}_f(s) = \sum'_{m\neq 0} \#C_m(\mathbb{Q})|m|^{-s}$ where the summation is over all non-zero squarefree integers. We show that $\mathscr{D}_f(s)$ converges for $\Re(s) > 1$. We extend its range of convergence assuming the ABC conjecture. This leads us to study related Dirichlet series attached to binary forms. We are then led to investigate the variation of rational points on twists of superelliptic curves. We apply this study to certain classical problems of analytic number theory such as the number of powerfree values of a fixed polynomial in $\mathbb{Z}[x]$.

2000 Mathematics Subject Classification: 11G30; 11M41.

1 Introduction

The idea of attaching a Dirichlet series to study a sequence of numbers can be traced back to Riemann and Dirichlet in their foundational work concerning the distribution of prime numbers. In this paper, we employ a similar idea to the study of rational points on quadratic twists of hyperelliptic curves. Using the current knowledge of diophantine geometry we establish a half-plane of convergence for these series. Using the ABC conjecture, we can widen the half-plane of convergence. We then make precise conjectures on the abscissa of convergence for these series and discuss analogous results in the case of twists of superelliptic curves. Finally, we apply these results to the study of squarefree values and more generally, powerfree values of polynomials.

To be precise, let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $r \geq 5$ and with distinct complex roots. For each squarefree integer m, we may consider the hyperelliptic curve

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

[1] Research partially supported by an NSERC grant.

A consequence of the award-winning theorem of Faltings [Fal] is that

$$\#C_m(\mathbb{Q}) < \infty.$$

A famous conjecture of Caporaso, Harris and Mazur [CHM] predicts the existence of a constant κ_r depending only on r such that $\#C_m(\mathbb{Q}) \leq \kappa_r$, for every m and every f of degree r. In order to study this conjecture (and related conjectures) it is natural to consider the Dirichlet series

$$\mathscr{D}_f(s) = \sum_{m=-\infty}^{\infty}{}' \frac{\#C_m(\mathbb{Q})}{|m|^s},$$

and determine its abscissa of convergence, where the dash on the summation indicates (unless otherwise specified) that we run over all non-zero squarefree integers.

Using the deep work of Vojta [Voj], we proved in an earlier paper [LM] the following:

Theorem 1. *$\mathscr{D}_f(s)$ converges for $\Re(s) > 1$.*

Here is a brief sketch of the argument. The rational points of C_m can be viewed as points of $C := C_1$ with co-ordinates lying in the quadratic field $\mathbb{Q}(\sqrt{m})$. Let $h : C(\bar{\mathbb{Q}}) \to \mathbb{R}$ be a height function on C corresponding to a projective embedding of C and J the Jacobian variety of C. Then Vojta [Voj] showed that there is a constant γ depending only on C such that for all finite extensions $K/\mathbb{Q}$,

$$\#\{P \in C(K) : h(P) \geq \gamma\} \leq \#J(K)_{\text{tor}}\kappa(\gamma)10^{\operatorname{rank} J(K)},$$

where $\kappa(\gamma)$ is a constant depending only on γ and $\operatorname{rank} J(K)$ denotes the Mordell-Weil rank of $J(K)$. We apply this to $K = \mathbb{Q}(\sqrt{m})$. Using descent theory (as in p. 282 of [Silv] or p. 95 of [H]), we have

$$\operatorname{rank} J(\mathbb{Q}(\sqrt{m})) \ll \frac{\log m}{\log\log m}$$

for m sufficiently large. By a well-known theorem of Northcott, $J(\mathbb{Q}(\sqrt{m}))_{\text{tor}}$ is uniformly bounded so that from Vojta's result, we deduce

$$\#\{P \in C(\mathbb{Q}(\sqrt{m})) : h(P) \geq \gamma\} \ll m^{\varepsilon}$$

for any $\varepsilon > 0$. Thus, we see that

$$\sum_{m=-\infty}^{\infty}{}' \frac{1}{|m|^s}\#\{P \in C(\mathbb{Q}(\sqrt{m})) : h(P) \geq \gamma\}$$

converges for $\Re(s) > 1$. Since the contribution from the points of bounded height and bounded degree is finite by Northcott's theorem, the series

$$\sum_{m=-\infty}^{\infty}{}' \frac{1}{|m|^s} \#\{P \in C(\mathbb{Q}(\sqrt{m})) : h(P) \leq \gamma\}$$

converges for $\Re(s) > 1$. Thus, $\mathscr{D}_f(s)$ converges for $\Re(s) > 1$.

If we can show that the series in fact converges for $\Re(s) = 1$, then we can deduce by standard analytic number theory that

$$\sum_{|m| \leq x}{}' \#C_m(\mathbb{Q}) \leq \sum_{m}{}' \#C_m(\mathbb{Q}) \frac{x}{|m|} = O(x),$$

indicating that $\#C_m(\mathbb{Q})$ is uniformly bounded "on average." It may happen that every twist has a rational point as in the case when $f(x)$ has a rational root. In such a case, the series $\mathscr{D}_f(s)$ diverges at $s = 1$. However, if $f(x)$ has no rational root, we expect the series to converge in a wider region as the following theorem shows. In fact, if we agree that $\#C_m(\mathbb{Q})$ counts rational points (x, y) with $y \neq 0$ (a convention we will follow throughout this paper), then one of the results we will prove in this paper is:

Theorem 2. *Let $r \geq 5$ and set $\delta_r = 2/(r-4)$ if r is even and $2/(r-3)$ if r is odd. Assuming the ABC conjecture, $\mathscr{D}_f(s)$ converges for $\Re(s) > \delta_r$.*

Notice that in the above theorem, δ_r tends to zero as r tends to infinity. By standard analytic number theory, we deduce the following corollary.

Corollary 3. *For any $\varepsilon > 0$, we have under the same conditions as in Theorem 2,*

$$\sum_{|m| < x}{}' \#C_m(\mathbb{Q}) \ll x^{\delta_r + \varepsilon}.$$

The corollary implies that the number of $|m| \leq x$ for which $\#C_m(\mathbb{Q}) \geq 1$ is $O(x^{\delta_r+\varepsilon})$. This result was also observed independently by Granville. It would be interesting to prove such results without assuming ABC. This may be possible since we are only applying ABC "on average." At the moment, we are unable to do this. However, the following unconditional result will be proved below.

Theorem 4.

$$\sum_{|m| \leq x}{}' \#C_m(\mathbb{Q}) = \Omega(x^{2/r}).$$

It may be useful to the reader if we recall the Ω-notation. We write

$$f(x) = \Omega(g(x))$$

if there is a positive constant c such that for infinitely many x tending to infinity, we have

$$|f(x)| > cg(x).$$

Theorem 4 implies that the abscissa of convergence of $\mathscr{D}_f(s)$ lies somewhere between $2/r$ and δ_r and it is very likely that it is $2/r$ for $r \geq 5$. We remark that for $r = 3$ or $r = 4$, the Dirichlet series has no finite abscissa of convergence. To see this, consider the case $r = 3$ (the case $r = 4$ being similar). In both these cases, C is an elliptic curve and it is well-known that there are infinitely many m such that $C_m(\mathbb{Q})$ is infinite.

In the context of Theorem 4, we mention the important work of Stewart and Top [ST] concerning ranks of twists of elliptic curves. Theorem 2 of [ST] implies, in our context, that

$$\sum_{|m| \leq x}{}' \#C_m(\mathbb{Q}) \gg \frac{x^{2/r}}{\log^2 x}.$$

In any case, these observations imply that the abscissa of convergence of $\mathscr{D}_f(s)$ is greater than or equal to $2/r$.

We also list below some unconditional results that can be derived from the convergence of $\mathscr{D}_f(s)$. For example, one can deduce an "average form" of the ABC conjecture from Theorem 1.

Our interest in the study of $\mathscr{D}_f(s)$ was motivated by our earlier work related to some conjectures of Rubin and Silverberg [RS1]. Their work was in turn motivated by a "controversial" conjecture of Honda [H]. Here is a more precise description of this work.

Let $f(x) \in \mathbb{Z}[x]$ be a cubic polynomial with distinct complex roots. Let E be an elliptic curve defined over $\mathbb{Q}$ by

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

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

$$E_D : Dy^2 = f(x).$$

Honda [H] conjectured that there is a constant C depending only on E but not on D such that

$$\operatorname{rank}_{\mathbb{Z}} E_D(\mathbb{Q}) < C.$$

Rubin and Silverberg [RS1] made an equivalent formulation of Honda's conjecture in terms of the convergence of a certain infinite series. We begin by stating their result.

Let $\hat{h}_E : E(\bar{\mathbb{Q}}) \to \mathbb{R}_{\geq 0}$ be the canonical height function on $E(\bar{\mathbb{Q}})$ and let $\hat{h}_D = \hat{h}_{E_D}$ be the canonical height function on $E_D(\bar{\mathbb{Q}})$ for a non-zero square-free integer D.

They defined the Dirichlet series

$$T_E(j,k) = \sum_D |D|^{-k} \sum_{P \in E_D(\mathbb{Q}) - E_D(\mathbb{Q})_{\text{tor}}} \hat{h}_D(P)^{-j}$$

where the sum is over all non-zero square-free integers D.

Theorem 5 (Rubin, Silverberg). *If j is a positive real number, then the following conditions are equivalent:*

(1) $\operatorname{rank}_{\mathbb{Z}} E_D(\mathbb{Q}) < 2j$ *for every* $D \in \mathbb{Z}\backslash\{0\}$;

(2) $T_E(j,k)$ *converges for some* $k \geq 1$;

(3) $T_E(j,k)$ *converges for every* $k \geq 1$.

Now let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree ≥ 5 and with distinct roots, as before. Then the curve

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

has genus $g \geq 2$.

Consider the series $T_f(j,k)$ defined analogously to $T_E(j,k)$, where the canonical height being chosen with respect to the "theta divisor" Θ on the Jacobian variety J of C. More precisely, 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 $P_0 \in C(\bar{\mathbb{Q}})$. We assume that P_0 is chosen so that $\Theta = e(C^{g-1})$ is a symmetric divisor on J. (This is possible when C is a hyperelliptic curve.) Let $\hat{h}$ be the (logarithmic) canonical height on J with respect to Θ.

Let C_m be a twist of C given by

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

A special case of the Mordell-Weil theorem tells us that if J_m is the Jacobian of C_m and $L = \mathbb{Q}(\sqrt{m})$, then $J_m(L)$ is finitely generated. We may view rational points on C_m as points of C with co-ordinates lying in the field $\mathbb{Q}(\sqrt{m})$. With this understanding, it is natural to consider

$$T_f(j,k) = \sum_{m=-\infty}^{\infty}{}' \frac{1}{|m|^k} \sum_{P \in C_m(\mathbb{Q})\backslash C_m(\mathbb{Q})_{\text{tor}}} \frac{1}{\hat{h}(P)^j}.$$

As noted in [RS1], the series converges for $k > 1$ if one invokes the unproved hypothesis of Caporaso, Harris and Mazur [CHM], since the inner sum would be $O(1)$ by the hypothesis for any $j \geq 0$. In an earlier paper [LM] mentioned before, we proved the convergence for $k > 1$ and any $j > 0$ *without* the unproved hypothesis. The key tool used was an effective version of Mumford's gap principle. In section 2 below, we will show that this can be improved to give:

Theorem 6. *If $r \geq 5$, there is a constant c depending only on f such that $T_f(j,k)$ converges for $k = 1$ and $j > c$.*

Since the series $T_f(j,k)$ is dominated by $\mathscr{D}_f(k)$, we deduce from Theorem 2 the following improvement.

Theorem 7. *Let $r \geq 5$. Assuming the ABC conjecture, the series $T_f(j,k)$ converges for $k > \delta_r$ and all j real.*

The ABC conjecture can be stated in the following way. Let $F \in \mathbb{Z}[x,y]$ be a homogenous form of degree r, with no repeated factors. Then for any coprime integers u, v satisfying $F(u,v) \neq 0$, we have

$$\operatorname{rad} F(u,v) := \prod_{p \mid F(u,v)} p \gg \max(|u|,|v|)^{r-2-\varepsilon}$$

for any $\varepsilon > 0$. For many applications, even a "quasi"-ABC conjecture (or more precisely, a δ-quasi-ABC conjecture) of the form: there exists a $\delta > 0$ such that

$$\operatorname{rad}(F(u,v)) \gg \max(|u|,|v|)^{\delta},$$

would have tremendous consequences. In this context, an important corollary of our work in [LM] is the following estimate for the exceptional set.

Theorem 8. *For any $\delta < 2$, the number of pairs of integers $|u|, |v| \leq H$ satisfying*

$$\operatorname{rad}(F(u,v)) \leq \max(|u|,|v|)^{\delta}$$

is $O(H^{\delta+\varepsilon})$ for any $\varepsilon > 0$.

For various reasons, it is useful to have lower bounds for "stratified" radicals. More precisely, we can define the i-th *radical* $\operatorname{rad}_i(n)$ of a natural number n as follows. Let

$$n = \prod_{p \mid n} p^{v_p(n)}$$

be its unique factorization and set

$$\operatorname{rad}_i(n) = \prod_{1 \leq v_p(n) \leq i} p.$$

Then:

Theorem 9. *Assuming the ABC conjecture,*

$$\mathrm{rad}_i(F(u,v)) \gg \max(|u|,|v|)^{r-2-2/i-\varepsilon}.$$

In particular,

$$\mathrm{rad}_1(F(u,v)) \gg \max(|u|,|v|)^{r-4-\varepsilon}$$

for any $\varepsilon > 0$.

In other words, for $r \geq 5$, $F(u,v)$ is "nearly squarefree," assuming the ABC conjecture.

Motivated by these observations, we are led to introduce in section 4, a family of Dirichlet series associated to binary forms. One family of Dirchlet series is particularly interesting. Consider

$$\mathscr{R}_{F,i}(s) = \sum_{(u,v)=1,\, F(u,v)\neq 0} \frac{1}{|\mathrm{rad}_i\, F(u,v)|^s}.$$

Then, we have the following theorem.

Theorem 10. *Assuming the ABC conjecture,* $\mathscr{R}_{F,i}(s)$ *converges for*

$$\Re(s) > 2/(r-2-2/i).$$

A quasi-ABC conjecture implies convergence in some half-plane.

The Dirichlet series $\mathscr{R}_{F,1}(s)$ has a curious connection to the question of whether there are infinitely many primes p such that

$$2^{p-1} \not\equiv 1 \pmod{p^2},$$

the so-called non-Wieferich primes. Heuristics suggest that the number of primes $p \leq x$ for which

$$2^{p-1} \equiv 1 \pmod{p^2}$$

is $\asymp \log\log x$. At the moment, 1093 and 3511 are the only primes $p < 32 \times 10^{12}$ for which the congruence holds. We will show:

Theorem 11. *Suppose that for some* $r \geq 5$, *and* $F(x,y) = x^r - y^r$, *the Dirichlet series* $\mathscr{R}_{F,1}(s)$ *converges for some real number* $s = s_0$. *Then there are infinitely many non-Wieferich primes. In particular, for any* $\delta > 0$, *a* δ*-quasi ABC conjecture implies that there are infinitely many non-Wieferich primes.*

In light of this theorem, it is therefore not surprising that the study of the series $\mathscr{R}_{F,1}(s)$ or more generally $\mathscr{R}_{F,i}(s)$ seem to lie at the boundary of our understanding. We are unable to establish any half-plane of absolute convergence for them even though they resemble $\mathscr{D}_f(s)$ in many ways. The connection between ABC and non-Wieferich primes was first made by Silverman [Silv2]. However, it will be noted that his proof needs a δ-quasi-ABC, with $\delta > 1/2$, to deduce the infinitude of non-Wieferich primes whereas our proof only requires any $\delta > 0$.

Instead of considering hyperelliptic curves, we may consider in a similar fashion the superelliptic case:

$$\mathscr{C} : y^a = f(x)$$

and consider its a-th power free twists $\mathscr{C}_m$ given by

$$my^a = f(x).$$

An analysis similar to Theorem 1 and 2 leads us to the following:

Theorem 12. *Let $\mathscr{C}$ be of genus greater than* 1. *The Dirichlet series*

$$F_{\mathscr{C}}(s;\mathbb{Q}) := \sum_{m=-\infty}^{\infty}{}' \frac{\#\mathscr{C}_m(\mathbb{Q})}{|m|^s},$$

where the sum is over all a-th powerfree integers, converges for $\Re(s) > 1$. If we assume the ABC conjecture, it converges for $\Re(s) > \delta_r(a)$, where

$$\delta_r(a) = \frac{2}{r - \frac{r_0+(2-\eta)a}{a-1}}$$

where r_0 is the reduced residue class of modulo a satisfying $a|r + r_0$, and $\eta = 0$ or 1 according as $a|r$ or not. Note that $\delta_r(2) = \delta_r$ as defined in Theorem 2.

Instead of attaching a Dirichlet series to study the number of rational points of twists of hyperelliptic curves or superelliptic curves, one may also consider Dirichlet series of the form

$$F_{\mathscr{C}}(s;\mathbb{Z}) := \sum_{m=-\infty}^{\infty}{}' \frac{\#\mathscr{C}_m(\mathbb{Z})}{|m|^s},$$

where the summation is over all a-th powerfree integers. (One may even consider the series with $\mathbb{Z}$ replaced by the ring of S-integers. The results proved below hold in this general context also.)

We will prove:

Theorem 13. *Assuming the ABC conjecture, the Dirichlet series* $F_{\mathscr{C}}(s;\mathbb{Z})$ *converges for* $\Re(s) > 1/\left(r - 1 + \frac{1}{a-1}\right)$.

Here again, we can show unconditionally that

Theorem 14.

$$\sum_{|m|\le x}{}' \#\mathscr{C}_m(\mathbb{Z}) = \Omega(x^{1/r}).$$

In the special case $a = 2$, Cutter, Granville and Tucker [CGT] proved the above result assuming the ABC conjecture. They also supplied some heuristic reasoning to suggest this result is best possible. It is highly likely that

$$\sum_{|m|\le x}{}' \#\mathscr{C}_m(\mathbb{Z}) \ll x^{1/r+\varepsilon}$$

for any $\varepsilon > 0$. This would imply that the abscissa of convergence for the series $F_{\mathscr{C}}(s,\mathbb{Z})$ is $1/r$.

This observation, together with Theorem 4 leads us to formulate the *abscissa conjecture*: the series $F_{\mathscr{C}}(s;\mathbb{Q})$ and $F_{\mathscr{C}}(s;\mathbb{Z})$ have abscissa of convergence $2/r$ and $1/r$ respectively.

These results have some relevance to the classical problem of analytic number theory of determining how often a given polynomial represents squarefree numbers or more generally an a-th powerfree number. We refer the reader to the excellent survey [Pa] concerning this important question of analytic number theory. However, it is important to highlight some of the history concerning this problem. The question seems to have been first raised by Nagell in 1922 and treated in more detail by Ricci in 1933 using sieve methods. But both of these works could only address the question of how often a polynomial of degree r represented r-th powerfree numbers. It was not until in 1976, when Hooley derived an asymptotic formula for the number of $n \le x$ such that $f(n)$ is $(r-1)$-th powerfree. Already this involved non-trivial methods of sieve theory as well as an application of Weil's celebrated result of the Riemann hypothesis for zeta functions of curves over finite fields. A spectacular breakthrough was made by Mohan Nair [Na] in 1976 when he was able to use ideas of algebraic number theory to deduce an asymptotic formula for how often $f(n)$ is a-th powerfree for $a \ge (\sqrt{2} - 1/2)r$. In subsequent work, he was even able to obtain error terms of the form $O(x^{\theta})$ with $\theta < 1$. In spite of these remarkable advances, we are still unable to determine if $n^4 + 1$ is infinitely often a squarefree number. In 1998, Granville [Gran] used the ABC conjecture to derive an asymptotic formula for the number of $n \le x$ for which $f(n)$ is squarefree. We will prove:

Theorem 15. *Assume the ABC conjecture. Let* $f(x)$ *be an irreducible polynomial over* $\mathbb{Z}[x]$ *of degree r. If* $a \ge 3$, *the number of* $n \le x$ *such that* $f(n)$ *is a-th power free is equal to*

$$c_f(a)x + O(x^{1/(a-1)+\varepsilon}),$$

where

$$c_f(a) = \prod_p \left(1 - \frac{\rho(p^a)}{p^a}\right)$$

and $\rho(p^a)$ *is the number of roots of* $f(x) \bmod p^a$. *For* $a = 2$, *we get assuming the abscissa conjecture,*

$$c_f(2)x + O(x^{1-2/(r+2)+\varepsilon})$$

for $r \geq 3$.

We may also consider the allied problem of how often $f(p)$ is squarefree or a-th power free for prime numbers $p \leq x$.

Theorem 16. *Assume the ABC conjecture. Let* $f(x)$ *be an irreducible polynomial over* $\mathbb{Z}[x]$ *of degree r. If* $a \geq 3$, *the number of primes* $p \leq x$ *such that* $f(p)$ *is a-th power free is equal to*

$$\tilde{c}_f(a)\pi(x) + O\left(\frac{x}{\log^A x}\right),$$

for any $A > 1$, *where*

$$\tilde{c}_f(a) = \prod_p \left(1 - \frac{\tilde{\rho}(p^a)}{\phi(p^a)}\right),$$

and $\tilde{\rho}(p^a)$ *denotes the number of coprime residue classes mod* p^a *which are roots of* $f(x) \bmod p^a$. *If in addition, we assume the generalised Riemann hypothesis, then the error term is*

$$O(x^{1/2+1/2a} \log x).$$

If the abscissa conjecture is true, then for $a = 2$, *the number of such primes* $p \leq x$ *is*

$$\tilde{c}_f(2)\pi(x) + O(x^{1-1/(r+2)+\varepsilon}),$$

assuming in addition the generalised Riemann hypothesis.

It seems difficult to derive an asymptotic formula in the case $a = 2$ assuming only the ABC conjecture. This may be possible. But a straightforward modification of the argument in [Gran] does not seem to work.

Our final theorem concerns an equivalent formulation of the ABC conjecture in terms of double Dirichlet series.

Theorem 17. *The ABC conjecture is true if and only if*

$$B_F(j,k) := \sum_{(u,v)=1}{}' |\mathrm{rad}\, F(u,v)|^{-k} H(u/v)^{-j}$$

converges for every k and j satisfying

$$k(r-2) + j > 2$$

for every homogenous binary form F in $\mathbb{Z}[x,y]$ *of degree* $r \geq 3$. *If the convergence is established for the specific form* $F(x,y) = xy(x+y)$ *of degree 3, then the ABC conjecture follows. (Here,* $H(u/v)$ *is equal to* $\max(|u|,|v|)$ *is the exponential height function.)*

In this paper, our goal is to study these and allied Dirichlet series and indicate how some of their analytic properties give us Diophantine information. Before embarking on this task, let us review the main result of [LM]. Let $K/\mathbb{Q}$ be a number field, C/K a hyperelliptic curve of genus $g \geq 2$, and J/K the Jacobian variety of C.

Mumford [Mu] showed that if $\{x_n\}$ is a sequence of distinct points in $C(\overline{K})$ lying in some finitely generated subgroup of $J(\overline{K})$ and ordered by increasing height, then there exists an integer N and a number $a > 1$ such that

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

However, the nature of N was not specified. Using a lemma of Silverman we made Mumford's argument explicit in [LM], and obtained the following result.

Theorem 18 (J.-J. Lee, R. Murty). *If* $r \geq 5$, *then* $T_f(j,k)$ *converges for every* $k > 1$ *and any positive real number j.*

Remark. This is equivalent to Theorem 2 in [LM], where the series was expressed in terms of naive height, due to the property of

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

where $h_x(P)$ denotes the naive height on the x-coordinate of P.

In this note, we show the convergence of this series for the case when $k = 1$. This was not treated in the earlier paper [LM] since the analysis is delicate and requires a new idea. Our paper begins with this result. An interesting consequence of this result is the estimate

$$\sum_{|m| \leq x}{}' \#C_m(\mathbb{Q}) \ll x(\log x)^A$$

for some $A > 0$. Thus, "average", $\#C_m(\mathbb{Q})$ is $O(\log^A |m|)$.

2 Convergence of $T_f(j,k)$ for $k=1$

Notice that if $y \neq 0$, then the height of a rational point $P=(x,y) \in C_m(\mathbb{Q})$ satisfies

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

To see this, we may write

$$f(x) = a_r \prod_i (x-\alpha_i) = my^2$$

where a_r is the leading coefficient of $f(x)$ and α_i are the roots of $f(x)$. Writing $x=u/v$ with u and v coprime integers, we find $my^2 = f(u/v)$. Let us treat the case r even (the case r odd being similar). Thus,

$$m(v^{r/2}y)^2 = v^r f(u/v).$$

If $y \neq 0$, the right hand side is a non-zero integer. As m is squarefree, it follows that $v^{r/2}y$ is also an integer. Thus,

$$|a_r| \prod_i |u-\alpha_i v| \geq m$$

so that at least one of the factors on the left has to be at least $\gg |m|^{1/r}$. Therefore $h(u/v) \gg \log|m|$. As the naive height and the canonical height differ by $O(1)$, the result follows. Thus,

$$T_f(j,k) \ll \sum_{m=-\infty}^{\infty}{}' \frac{1}{|m|^k} \cdot \frac{\#C_m(\mathbb{Q})}{(\log|m|)^j}.$$

Before we begin, we remark that the conjecture of Caporaso, Harris and Mazur [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 $g \geq 2$, implies that $T_f(j,k)$ converges for $k=1$ and $j>1$.

We want to prove the convergence without assuming this conjecture.

We begin by ordering the finite set of points in $C(\mathbb{Q}(\sqrt{m}))$ in the order of increasing height to have a sequence $\{x_n\}$. The convergence of the sum in question is determined by

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

(See [LM, Proposition 7].)

The following is an improved estimate of our earlier proof of Proposition 7 of [LM].

Proposition 19. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $r \geq 5$ and with distinct roots. Let C be the curve $y^2 = f(x)$. There are constants γ and c, depending only on f, such that for $|m| > \gamma$, we have*

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

for any positive real number j. Here $\nu(m)$ is the number of prime divisors of m.

Proof. We partition the indices n in this sum into residue classes $(\text{mod } N)$ for some N with an estimate of $N \ll c^{\text{rank}_{\mathbb{Z}} J_m(\mathbb{Q})}$ (see [LM, Lemma 4 and Proposition 7]). For each such residue class $t \ (\text{mod } N)$ and $n = qN + t$, an effective version of Mumford's gap principle gives us

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

As $a > 1$ and $\hat{h}(x_t) \gg \log|m|$, we find that for each residue class $t \ (\text{mod } N)$, the contribution is

$$\ll |x_t|^{-2j} = \hat{h}(x_t)^{-j} \ll (\log|m|)^{-j}.$$

Summing this for $t \ (\text{mod } N)$ together with an estimate of $N \ll c^{\text{rank}_{\mathbb{Z}} J_m(\mathbb{Q})} \ll c^{\nu(m)}$ gives

$$\sum_{x_n \in C(\mathbb{Q}(\sqrt{m})) - C(\mathbb{Q}(\sqrt{m}))_{\text{tor}}} \frac{1}{\hat{h}(x_n)^j} \ll \frac{c^{\nu(m)}}{(\log|m|)^j}. \qquad \square$$

Remark. The sum of the remaining terms in $T_f(j,k)$ (that is, those terms for which $|m|$ is not large enough) is finite by the result of Northcott. (See [LM, §3].)

Thus, Proposition 19 implies that the convergence of $T_f(j,k)$ is determined by the convergence of the series

$$\sum_{m=2}^{\infty} \frac{c^{\nu(m)}}{m^k (\log m)^j}.$$

This series is now studied by standard methods of analytic number theory.

Lemma 20 (Partial Summation). *Suppose $\{a_n\}_{n=1}^{\infty}$ is a sequence of complex numbers and $f(t)$ is a continuously differentiable function on $[1, x]$. Set*

$$A(t) = \sum_{n \leq t} a_n.$$

Then

$$\sum_{n\le x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)\,dt.$$

Proof. See [M], Chapter 2. □

Proposition 21. *The series*

$$\sum_{m=2}^{\infty} \frac{c^{\nu(m)}}{m(\log m)^j}$$

converges for $j > c$.

Proof. We use the well-known theorem (see for example, Exercise 4.4.17 of [M]): there is an $A > 0$ so that

$$\sum_{m\le x} c^{\nu(m)} \sim Ax(\log x)^{c-1} \quad \text{as } x \to \infty.$$

Then the partial summation theorem tells us that

$$\sum_{m\le x} \frac{c^{\nu(m)}}{m(\log m)^j} \sim \frac{A(\log x)^{c-1}}{(\log x)^j} - \int_1^x \frac{A(\log t)^{c-1}}{t(\log t)^j}\left(1 - \frac{1}{j\log t}\right) dt,$$

which converges if $j > c$ as $x \to \infty$. □

Remark. An effective version of Faltings theorem on Mordell's conjecture, due to Vojta, that was applied in [LM] leads us to the above series with $c = 10$.

If we follow the proof of [LM, §4], our improved estimate gives us the bound

$$\sum_{x_n \in C(\mathbb{Q}(\sqrt{m}))-C(\mathbb{Q}(\sqrt{m}))_{\mathrm{tor}}} \frac{1}{\hat{h}(x_n)^j} \ll \frac{10^{\operatorname{rank} J_m(\mathbb{Q})}}{(\log m)^j} \ll \frac{10^{\nu(m)}}{(\log|m|)^j},$$

thus we have

$$T_f(j,k) \ll \sum_{m=2}^{\infty} \frac{10^{\nu(m)}}{m^k(\log m)^j},$$

which converges for $k = 1$ and $j > 10$.

As noted earlier, we may deduce from this that

$$\sum_{|m|\le x}{}' \#C_m(\mathbb{Q}) \ll \sum_{m}{}' \frac{x\log^j x}{|m|\log^j|m|} 10^{\nu(m)} \ll x(\log x)^A$$

for any $A > 10$.

3 Proofs of Theorems 2 and 4

We begin by recalling the ABC conjecture in the form we will apply it below. For each natural number n, define the *radical* of n to be

$$\mathrm{rad}(n) = \prod_{p|n} p.$$

We will also write the *squarefree part* of n to be

$$\mathrm{sf}(n) = \prod_{p^a \| n,\, a \text{ odd}} p$$

and the *radical of the square part* of n to be

$$\mathrm{sq}(n) = \prod_{p^a \| n,\, a \text{ even} \geq 2} p.$$

We note that $\mathrm{sf}(n)\,\mathrm{sq}(n) = \mathrm{rad}(n)$ and that $\mathrm{sf}(n)\,\mathrm{sq}(n)^2 \mid n$. Consequently, $\mathrm{sq}(n) \leq \sqrt{n/\mathrm{sf}(n)}$. The ABC conjecture states that whenever we have three mutually coprime integers A, B, C such that

$$A + B = C$$

then

$$\max(|A|, |B|, |C|) \ll_\varepsilon \mathrm{rad}(ABC)^{1+\varepsilon}$$

for all $\varepsilon > 0$. Elkies [Elk] showed that the ABC conjecture when combined with the celebrated Belyi theorem [Bel] implies the following the stronger (and equivalent) statement. Let $F(x, y) \in \mathbb{Z}[x, y]$ be a homogenous form of degree r, with no repeated factors. Then, for any coprime integers u, v with $F(u, v) \neq 0$, we have

$$\max(|u|, |v|)^{r-2-\varepsilon} \ll_\varepsilon \mathrm{rad}(F(u, v))$$

for any $\varepsilon > 0$. The ABC conjecture arises from the special case of $F(x, y) = xy(x + y)$. We record for future reference what this implies for $\mathrm{sf}(F(u, v))$.

Lemma 22. *Assuming the ABC conjecture,*

$$\mathrm{sf}(F(u, v)) \gg \max(|u|, |v|)^{r-4-\varepsilon},$$

for any $\varepsilon > 0$.

Proof. By the ABC conjecture, we have

$$\mathrm{sf}(F(u, v))\,\mathrm{sq}(F(u, v)) \gg \max(|u|, |v|)^{r-2-\varepsilon}.$$

Clearly,

$$\mathrm{sf}(F(u,v))[\mathrm{sq}\,F(u,v)]^2 \leq F(u,v) \ll \max(|u|,|v|)^r.$$

Inserting this into the previous inequality, we get

$$\max(|u|,|v|)^{r-2-\varepsilon} \ll \mathrm{sf}(F(u,v))^{1/2}\max(|u|,|v|)^{r/2}$$

from which we deduce the result. □

We will now apply this to prove Theorem 2. Recall that $f(x)$ is a polynomial of degree $r \geq 5$ with distinct roots. Now let $F(u,v)$ be $v^r f(u/v)$ if r is even and $v^{r+1}f(u/v)$ when r is odd. Then $F(u,v)$ is a homogenous form with no repeated factors, since f has distinct roots. Moreover, F has degree r or $r+1$ according as r is even or odd.

We begin our analysis with the r even case. Let us observe that if m is squarefree and $my^2 = f(u/v)$, with u, v coprime integers, then

$$m(v^{r/2}y)^2 = F(u,v).$$

Thus, $\mathrm{sf}(F(u,v)) = m$. Conversely, if $\mathrm{sf}(F(u,v)) = m$, then $F(u,v) = mw^2$ for some integer w. Thus $(u/v, w/v^{r/2})$ is a rational point on C_m. Therefore,

$$\sum_{m=-\infty}^{\infty}{}' \frac{1}{|m|^k}\#C_m(\mathbb{Q}) = \sum_{(u,v)=1,\,F(u,v)\neq 0}\frac{1}{|\mathrm{sf}\,F(u,v)|^k}.$$

By the lemma above, the series is dominated by

$$\sum_{(u,v)=1}\frac{1}{\max(|u|,|v|)^{kr-4k}}$$

and since the sum is symmetric, we may suppose that $|u| > |v|$ and find that the series converges if $k(r-4) > 2$ which is the statement of Theorem 2.

For the case r is odd, we proceed similarly. In this case, F has degree $r+1$ and so we see that the series converges for $\Re(s) > 2/(r-3)$. This completes the proof of Theorem 2.

As we remarked, for $j \geq 0$, we have

$$T_f(j,k) \leq \mathscr{D}_f(k).$$

Thus, Theorem 7 is immediate in case $j \geq 0$. If $j < 0$, then we write $j = -t$, with $t > 0$ and observe that

$$T_f(-t,k) = \sum_{(u,v)=1}\frac{h(u/v)^t}{|\mathrm{sf}(F(u,v))|^k}.$$

As $h(u/v) = \log \max(|u|, |v|)$, and the earlier analysis provides a lower bound for $\mathrm{sf}(F(u,v))$, we deduce Theorem 7 immediately from this.

To deduce Corollary 3, we recall that if a Dirichlet series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges absolutely for $\Re(s) > a$, then $\sum_{n \le x} a_n \ll x^b$, for any $b > a$. To see this, note that

$$\sum_{n \le x} a_n \ll \sum_{n \le x} a_n (x/n)^b \ll x^b.$$

Since the Dirichlet series $\sum'_{m=-\infty}^{\infty} \frac{1}{|m|^s} \# C_m(\mathbb{Q})$ converges for $\Re(s) > \delta_r$, the corollary is now immediate.

The corollary is interesting from another perspective. The number $\# C_m(\mathbb{Q})$ represents the number of integral solutions of

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

with $w \neq 0$. It is trivial to see that the number of solutions of the Thue inequality $|F(u,v)| \le x$ is $O(x^{2/r})$. As we record below, one can even prove an asymptotic formula with a main term like $x^{2/r}$. This means that

$$\sum_{m \le x} \# C_m(\mathbb{Q}) = \Omega(x^{2/r}).$$

This implies that the abscissa of convergence of the series is greater than $2/r$.

4 Dirichlet series attached to binary forms

Given a binary form $F(x, y) \in \mathbb{Z}[x, y]$, there are at least three natural Dirichlet series we may associate with F. These are

$$\mathscr{T}_F(s) = \sum_{(u,v)=1,\, F(u,v) \neq 0} \frac{1}{|F(u,v)|^s},$$

$$\mathscr{R}_F(s) = \sum_{(u,v)=1,\, F(u,v) \neq 0} \frac{1}{|\mathrm{rad}(F(u,v))|^s},$$

$$\mathscr{D}_F(s) = \sum_{(u,v)=1,\, F(u,v) \neq 0} \frac{1}{|\mathrm{sf}(F(u,v))|^s},$$

the last one being related to the $\mathscr{D}_f(s)$ where $f(x) = F(x,1)$ when r is even. The easiest of the three series to study is naturally the first one, which we shall call the Thue series attached to F. In 1933, Mahler [Ma] proved that the number of integers x, y satisfying $|F(x, y)| \le h$ is equal to

$$A_F h^{2/r} + O(h^{1/(r-1)})$$

where A_F is the area of region defined by the inequality $|F(x, y)| \leq 1$ for $r \geq 3$. Let us note that the coprimality condition of u and v in the definition of $\mathscr{T}_F(s)$ means that

$$\mathscr{T}_F(s)\zeta(rs) = \sum_{F(u,v)\neq 0} \frac{1}{|F(u,v)|^s}.$$

This implies that $\mathscr{T}_F(s)$ has an analytic continuation to $\Re(s) > 1/(r-1)$ except for a simple pole at $s = 2/r$. In particular, the abscissa of convergence of the Dirichlet series $\mathscr{T}_F(s)$ is $2/r$. Since for real s, we have

$$\mathscr{D}_F(s) \geq \mathscr{R}_F(s) \geq \mathscr{T}_F(s),$$

we deduce that the abscissa of convergence of both $\mathscr{D}_F(s)$ and $\mathscr{R}_F(s)$ must be greater than or equal to $2/r$. Theorem 1 implies that $\mathscr{D}_F(s)$ converges for $\Re(s) > 1$ and $r \geq 5$. Thus, $\mathscr{R}_F(s)$ converges for $\Re(s) > 1$ and $r \geq 5$.

There are also other interesting results that can be deduced from these observations. One of them is to consider the "exceptional set" for the ABC conjecture. To be precise, let us consider the set $S_\delta(H)$ of pairs (u, v) with $|u|, |v| \leq H$ satisfying $\mathrm{rad}(F(u,v)) \leq \max(|u|, |v|)^\delta$. This number of pairs is, for any $k > 1$,

$$\ll \sum_{|u|,|v|\leq H} \frac{\max(|u|,|v|)^{\delta k}}{|\mathrm{rad}(F(u,v))|^k} \ll H^{\delta k}\mathscr{R}_F(k),$$

which is $\ll H^{\delta+\varepsilon}$, since the series $\mathscr{R}_F(s)$ converges for $\Re(s) > 1$ and we may set $k = 1 + \varepsilon/\delta$. If $\delta < 2$, the result is therefore non-trivial. This completes the proof of Theorem 8.

Let us now consider the Dirichlet series $\mathscr{R}_{F,i}(s)$ defined in the introduction. Using an argument analogous to the one used in the proof of Lemma 15, we get

$$\mathrm{rad}_i(n)(\mathrm{rad}(n)/\mathrm{rad}_i(n))^{i+1} \leq n.$$

Thus,

$$\mathrm{rad}_i(n) \geq \mathrm{rad}^{1+1/i}(n)n^{-1/i}$$

which means in our context that

$$\mathrm{rad}_i(F(u,v)) \geq \mathrm{rad}^{1+1/i}(F(u,v))\max(|u|,|v|)^{-1/i} \gg \max(|u|,|v|)^{r-2-2/i-\varepsilon}.$$

This implies Theorem 9.

5 Wieferich primes and Dirichlet series

In this section, we will prove Theorem 10. Our analysis will follow closely that of Silverman [Silv2]. Let us write

$$2^n - 1 = a_n b_n$$

where $a_n = \mathrm{rad}_1(2^n - 1)$ is squarefree and b_n is squareful, $(a_n, b_n) = 1$. Then, as in [Silv2], we see that if p is a prime dividing a_n, then $2^{p-1} \not\equiv 1 \pmod{p^2}$. Indeed, if t is the order of $2 \bmod p$, we see that $t|n$. Writing $2^t = 1 + kp$, we see that $2^n = (1 + kp)^{n/t} \equiv 1 + kpn/t \pmod{p^2}$ so that $p \nmid k$ because $p|a_n$ and not b_n. Thus, $2^{p-1} = (1 + kp)^{(p-1)/t} \equiv 1 + kp(p-1)/t \pmod{p^2}$ implying that p is not a Wieferich prime. Thus, if a_n is unbounded, then there are infinitely many primes p such that $2^{p-1} \not\equiv 1 \pmod{p^2}$. This means, we must have $\mathrm{rad}_1(2^n - 1)$ unbounded. Considering the form $F(x, y) = x^r - y^r$ with $r \geq 5$ and the set of values $x = 2^n$, $y = 1$, we immediately see from this that if $\mathrm{rad}_1(2^{nr} - 1)$ is bounded, for infinitely many n, then the Dirichlet series $\mathscr{R}_{F,1}(s)$ cannot converge in any half-plane. This completes the proof of Theorem 10. We note that assuming a quasi-ABC, we get that $\mathscr{R}_{F,1}(s)$ converges in some half-plane.

6 The superelliptic case

We may also consider twists of the curve

$$y^a = f(x).$$

It is more appropriate to define the curve

$$\mathscr{C}_m : my^a = f(x).$$

One may then consider the Dirichlet series

$$F_{\mathscr{C}}(s, \mathbb{Q}) := \sum_{m=-\infty}^{\infty}{}' \frac{\#\mathscr{C}_m(\mathbb{Q})}{|m|^s},$$

where the dash on the sum now means we run over a-th power free numbers. Using the methods to prove Theorem 1, we see that this Dirichlet series converges for $\Re(s) > 1$. We will now use the ABC conjecture to deduce that this series converges in a larger half-plane.

Arguing as before, we get

$$v^r my^a = F(u, v),$$

and letting r_0 be the reduced residue class mod a so that $r + r_0 \equiv 0 \pmod{a}$, we may write this as

$$mw^a = v^{r_0} F(u, v).$$

Taking the radical of both sides of the equation, we deduce, with $\eta = 0$ or 1 according as $a|r$ or not, that

$$|m|\,|w| \gg (\max(|u|, |v|))^{r+\eta-2-\varepsilon},$$

on the ABC conjecture. However,

$$|w| \ll \left(\frac{\max(|u|,|v|)^{r+r_0}}{|m|}\right)^{1/a}$$

so that

$$|m|^{(a-1)/a} \gg \max(|u|,|v|)^{r(1-1/a)-r_0/a+\eta-2-\varepsilon}.$$

Thus, if u/v is the x co-ordinate of $\mathscr{C}_m$, the above inequality must be satisfied. This means that

$$m \gg \max(|u|,|v|)^{r-r_0/(a-1)-(2-\eta)a/(a-1)-\varepsilon}.$$

If we let $x(\mathscr{C}_m)$ denote the set of x co-ordinates of $\mathscr{C}_m$, then

$$F_{\mathscr{C}}(s,\mathbb{Q}) = \sum_{(u,v)=1} \sum_{m:u/v \in x(\mathscr{C}_m)} \frac{1}{|m|^s}.$$

From our estimates, we deduce that $F_{\mathscr{C}}(s,\mathbb{Q})$ converges for $\Re(s) > \delta_r(a)$, where

$$\frac{2}{\delta_r(a)} = r - \frac{r_0 + (2-\eta)a}{a-1} - \varepsilon.$$

This completes the proof of Theorem 12.

A consequence of this result is that we can determine the average number of points on twists of the Fermat curve. Indeed, if $f(x) = x^a + 1$ above, we let F_m be the equation

$$F_m : my^a = x^a + 1.$$

Since $\delta_a(a) = 2(a-1)/(a^2-3a)$, we deduce under the conditions of Theorem 12 that

$$\sum_{|m| \le x}{}' \#F_m(\mathbb{Q}) \ll x^{2(a-1)/(a^2-3a)+\varepsilon},$$

where the sum is over all a-th powerfree integers. In particular, for $a > 5$, we see that the number of $|m| \le x$ for which the equation

$$x^a + y^a = mz^a$$

has a non-trivial solution is $\ll x^{4/a}$, assuming the ABC conjecture.

7 Integral points on hyperelliptic curves and superelliptic curves

We begin with a simple remark. If $f(x)$ is a polynomial of degree r without repeated factors, then as noted in [Gran], we have

$$\mathrm{rad}(f(n)) \gg |n|^{r-1-\varepsilon},$$

assuming the ABC conjecture. Thus,

$$\frac{f(n)}{\mathrm{sq}(f(n))} \geq \mathrm{rad}(f(n)) \gg |n|^{r-1-\varepsilon}.$$

Thus,

$$\mathrm{sq}(f(n)) \ll n^{1+\varepsilon},$$

which means that

$$\mathrm{sf}(f(n)) \gg |n|^{r-2-\varepsilon}.$$

In other words, the Dirichlet series

$$\sum_{n=-\infty}^{\infty}{}' \frac{1}{|\mathrm{sf}(f(n))|^s},$$

where the sum is over all integers n with $f(n) \neq 0$, converges for $\Re(s) > 1/(r-2)$. This is the series

$$\sum_{m=-\infty}^{\infty}{}' \frac{\#C_m(\mathbb{Z})}{|m|^s}.$$

We deduce immediately that

$$\sum_{|m| \leq x}{}' \#C_m(\mathbb{Z}) \ll x^{1/(r-2)+\varepsilon},$$

by the ABC conjecture.

In the superelliptic case, we proceed similarly as in the previous section to deal with the series

$$\sum_{m=-\infty}^{\infty}{}' \frac{\#\mathscr{C}_m(\mathbb{Z})}{|m|^s}$$

where the dash on the summation indicates we go over non-zero a-th power free integers. Assuming the ABC conjecture, we have that if

$$my^a = f(x)$$

for some integers x, y and m a-th powerfree, then,

$$|my| \geq |\mathrm{rad}\, f(x)| \gg |x|^{r-1-\varepsilon}$$

so that

$$|m|\left(\frac{|x|^r}{|m|}\right)^{1/a} \gg |x|^{r-1-\varepsilon}.$$

Thus,

$$|x|^{r-1-r/a-\varepsilon} \ll |m|^{1-1/a}.$$

In other words,

$$|m| \gg |x|^{r-a/(a-1)-\varepsilon}.$$

Thus the series $F_{\mathscr{C}}(s, \mathbb{Z})$ converges for $\Re(s) > 1/(r-1+1/(a-1))$. This completes the proof of Theorem 13.

To deduce Theorem 14, the series

$$\sum_{m=-\infty}^{\infty}{}' \frac{1}{|f(m)|^s},$$

where the sum is over those integers m for which $f(m) \neq 0$, converges for $\Re(s) > 1/r$. Clearly,

$$F_{\mathscr{C}}(s, \mathbb{Z}) \geq \sum_{m=-\infty}^{\infty}{}' \frac{1}{|f(m)|^s}$$

since the a-th powerfree part of $f(m)$ is less than or equal to $|f(m)|$. As the latter series has abscissa of convergence $1/r$, it follows that the abscissa of convergence of $F_{\mathscr{C}}(s, \mathbb{Z})$ is $\geq 1/r$. Theorem 14 is now immediate from standard analytic number theory.

8 Powerfree values of polynomials

Notice that if $d^a \mid f(n)$, with $a \geq 2$, we deduce arguing as in the previous sections, that

$$\frac{f(n)}{d^{a-1}} \geq \mathrm{rad}(f(n)) \gg n^{r-1-\varepsilon}.$$

Thus,

$$d \ll n^{1/(a-1)+\varepsilon}.$$

This means that in the application of the simple asymptotic sieve in Hooley's book [Hoo], we can count the number of a-free values of $f(n)$ very easily and derive an asymptotic formula with very good error terms. Indeed, if $N_d(x)$ is the number of $n \le x$ for which $d^a \mid f(n)$, then the sieve of Eratosthenes gives that the number of $n \le x$ for which $f(n)$ is a-th power free is

$$\sum_{n \le x} \sum_{d^a \mid f(n)} \mu(d) = \sum_d \mu(d) N_d(x).$$

We split the sum into two parts, $d \le y$ and $d \ge y$, with y to be suitably chosen. As noted above, if $d^a \mid f(n)$, then

$$\frac{n^r}{d^{a-1}} \gg \frac{f(n)}{d^{a-1}} \ge \operatorname{rad} f(n) \gg n^{r-1-\varepsilon},$$

the last inequality coming from the ABC conjecture. Thus,

$$d^{a-1} \ll n^{1+\varepsilon}.$$

In other words, if we take $y = O(x^{1/(a-1)+\varepsilon})$, we see the contribution for $d \ge y$ is zero. If $\rho(d^a)$ is the number of solutions of

$$f(n) \equiv 0 \pmod{d^a}$$

then the above sum is equal to

$$\sum_{d \le y} \mu(d) \left(\frac{x\rho(d^a)}{d^a} + O(\rho(d^a)) \right).$$

Since $\rho(m) \ll m^{\varepsilon}$, we easily find the error term above to be $O(y^{1+\varepsilon})$. Analyzing the first expression as in [Hoo], we find that it is

$$x \sum_{d=1}^{\infty} \mu(d) \frac{\rho(d^a)}{d^a} + O\left(\frac{x}{y^{a-1-\varepsilon}} \right).$$

The summation above easily changes into an infinite product since $\rho(d^a)$ is a multiplicative function of d by virtue of the Chinese remainder theorem. Let us therefore set

$$c_f(a) = \prod_p \left(1 - \frac{\rho(p^a)}{p^a} \right).$$

Then, with our choice of y, we get assuming the ABC conjecture, that the number of $n \leq x$ for which $f(n)$ is a-th power free is

$$c_f(a)x + O(x^{1/(a-1)+\varepsilon}),$$

in the case $a \geq 3$. For $a = 2$, we use the abscissa conjecture to obtain an improved error term. As before, we write our sum as

$$\sum_{d \leq y} \mu(d) N_d(x) + \sum_{d > y} \mu(d) N_d(x),$$

with y to be suitably chosen. Indeed, the abscissa conjecture implies that

$$\sum_{m \leq x}{}' \#C_m(\mathbb{Z}) \ll x^{1/r+\varepsilon}.$$

The first term for $d \leq y$ is

$$c_f(2)x + O(y^{1+\varepsilon})$$

as in [Hoo]. Thus, in the above analysis, the summation over $d > y$ is treated as follows. The sum

$$\sum_{y < d}{}' N_d(x)$$

is dominated by

$$\sum_{m \ll x^r/y^2} \#C_m(\mathbb{Z}).$$

We can transform this into a sum over squarefree m by noting two things. Each natural number n enumerated by the penultimate sum is also counted in

$$\sum_{|m| \ll x^r/y^2}{}' \#C_m(\mathbb{Z})$$

where the sum is now over squarefree numbers. The number of repetitions of each n cannot be more than the number of divisors of $f(n)$ which is $O(x^{\varepsilon})$ for any $\varepsilon > 0$. To be precise, if $d(m)$ denotes the number of divisors of m, then we have

$$\begin{aligned} \sum_{d > y} N_d(x) &\leq \sum_{n \leq x} \sum_{m \leq x/y^2, f(n) = mu^2} 1 \\ &\leq \sum_{n \leq x} \sum_{m_1 \leq x/y^2, f(n) = m_1 v^2}{}' d(f(n)/m_1) \ll x^{\varepsilon} \sum_{m \leq x/y^2}{}' \#C_m(\mathbb{Z}), \end{aligned}$$

using the well-known estimate that $d(m) = O(m^{\varepsilon})$. Thus, the summation over $d > y$ is bounded by

$$x^{\varepsilon} \sum_{m \ll x^r/y^2}{}' \#C_m(\mathbb{Z}),$$

which is $\ll (x^r/y^2)^{1/r+\varepsilon}$ by the abscissa conjecture. Choosing $y = x^{r/r+2}$ gives a final error term of $\ll x^{1-2/(r+2)+\varepsilon}$. This completes the proof of Theorem 15.

As is well-known, it may happen that $c_f(a)$ or $\tilde{c}_f(a)$ could be zero for "trivial" reasons. For instance, the polynomial $f(x) = x(x+1)(x+2)(x+3)$ is always divisible by 8 when x is an integer and consequently will never attain squarefree values or cubefree values. This "triviality" can be eliminated as remarked in [Gran] by letting B equal the gcd of $f(n)$ as n ranges over all the integers and then defining $B'(a)$ to be the smallest divisor of B such that $B/B'(a)$ is a-th powerfree. One can then derive results for how often $f(n)/B'(a)$ is a-th powerfree. The method would then give a positive proportion of such numbers.

It is now evident that similar results can be deduced for powerfree values of homogeneous binary forms of degree r. We state this below in the following way.

Theorem 23. *Assume the ABC conjecture. Let $F(u,v)$ be a homogenous binary form of degree r without any repeated factors. Then, the number of pairs (u,v) with $1 \le u \le x$ and $1 \le v \le y$ such that $F(u,v)$ is a-th powerfree is*

$$c'_f(a)xy + O(\max(x,y)^{2/(a-1)+\varepsilon})$$

for $a \ge 3$. For $a = 2$, we get assuming the abscissa conjecture that the number for which $F(u,v)$ is squarefree is

$$c'_f(2)xy + O(\max(x,y)^{2-8/(r+4)+\varepsilon}).$$

9 Powerfree values of polynomials with prime arguments

We will now prove Theorem 16. We proceed as in the previous section with the elementary sieve formula. Let $\pi_d(x)$ be the number of primes $p \le x$ such that $d^a \mid f(p)$. If $\tilde{\rho}(d^a)$ is the number of coprime residue classes $a_i \bmod d^a$ which are roots of $f(a_i) = 0 \bmod d^a$, then

$$\pi_d(x) = \sum_{a_i} \pi(x, d^a, a_i),$$

where $\pi(x,k,a)$ denotes the number of primes $p \le x$ which are congruent to a modulo k. Thus, the number of primes $p \le x$ for which $f(p)$ is a-th powerfree is

$$\sum_d \mu(d)\pi_d(x) = \sum_d \mu(d) \sum_{a_i} \pi(x, d^a, a_i).$$

We now have several ways to proceed. We can split our sum as before

$$\sum_{d \le y} \mu(d)\pi_d(x) + \sum_{d>y} \mu(d)\pi_d(x).$$

Assuming the ABC conjecture, we see that the second sum extends only over those d with $d < x^{1/(a-1)+\varepsilon}$. Estimating $\pi_d(x)$ by

$$\frac{\tilde{\rho}(d^a)}{d^a} + O(\tilde{\rho}(d^a)),$$

we see that the second sum is bounded by

$$\ll \frac{x^{1+\varepsilon}}{y^{a-1}} + O(x^{1/(a-1)+\varepsilon}).$$

For the initial sum, we may apply the Siegel-Walfisz theorem (see page 133 of [Dav]). This theorem states that for any A and B positive,

$$\pi(x,k,a) = \frac{\pi(x)}{\phi(k)} + O\left(\frac{x}{\log^B x}\right)$$

uniformly for $k \le \log^A x$. Thus, taking $y = \log^A x$ for any $A > 0$, we deduce that the number of primes in question is

$$\tilde{c}_f(a)\pi(x) + O\left(\frac{x}{\log^B x}\right),$$

for any $B > 0$. We could have applied the Bombieri-Vinogradov theorem (see p. 135 of [Dav]) with no appreciable gain in the error term. However, if we invoke the generalized Riemann hypothesis, which is the assertion that for k and a relatively prime,

$$\pi(x,k,a) = \frac{\pi(x)}{\phi(k)} + O(x^{1/2}\log kx),$$

then the error term is easily seen to be $\ll x^{1/2} y \log x$.

Thus, choosing $y^a = x^{1/2}$ we find the error is

$$\ll x^{1/2+1/2a}\log x,$$

as indicated in Theorem 16.

Finally, if $a = 2$, and the abscissa conjecture is invoked as in our discussion of the previous section, we obtain an error term of

$$\ll x^{1-1/(r+2)+\varepsilon}$$

assuming in addition the generalized Riemann hypothesis. To see this, we split our sum as before into $d < y$ and $d \geq y$. In the initial segment, we invoke the GRH and obtain an error term of $O(x^{1/2} y \log x)$ and in the second part, we apply the abscissa conjecture as before to get an error term of

$$\left(\frac{x^r}{y^2}\right)^{1/r+\varepsilon}.$$

We choose y so that $y^{1+2/r} = x^{1/2}$ which gives us the final estimate.

Clearly, a similar result to Theorem 23 can be derived for prime arguments. We leave this as an exercise to the reader.

10 Dirichlet series related to the ABC conjecture

It now seems natural to consider the Dirichlet series

$$A_F(j,k) := \sum_{(u,v)=1}{}' |\mathrm{sf}\, F(u,v)|^{-k} H(u/v)^{-j}$$

where $H(u/v) = \exp(h(u/v))$ is the usual exponential height, and the dash on the summation indicates we sum over u, v with $F(u,v) \neq 0$. We may also consider the related series

$$B_F(j,k) := \sum_{(u,v)=1}{}' |\mathrm{rad}\, F(u,v)|^{-k} H(u/v)^{-j}$$

which can be viewed as exponential height analogues of the series considered in the earlier sections. We can now prove Theorem 17: the ABC conjecture is true if and only if $B_F(j,k)$ converges for every k and j satisfying $k(r-2) + j > 2$.

Proof. Clearly, the ABC conjecture implies the series converges if $k(r-2) + j > 2$. Conversely, for k and j satisfying $k(r-2) + j > 2$, we have that

$$\sum_{(u,v)=1}{}' H(u/v)^{(r-2)k} |\mathrm{rad}\, F(u,v)|^{-k} H(u/v)^{-j-(r-2)k}$$

converges. Choose j and k so that $k(r-2) + j = 3$. There are infinitely many such k, j. Thus, for sufficiently large $H(u/v)$, we have

$$H(u/v)^{r-2} \ll |\mathrm{rad}\, F(u,v)| H(u/v)^{3/k}$$

from which we deduce the ABC conjecture by taking k to be arbitrarily large. □

A similar result can be stated for $A_F(j,k)$. More precisely, we have

Theorem 24. *$A_F(j,k)$ converges for every k and j satisfying $k(r-4)+j>2$ if and only if*

$$\text{sf } F(u,v) \gg H(u/v)^{r-4-\varepsilon}.$$

11 Concluding remarks

A tantalizing question that arises from the previous discussion is if the ABC conjecture has anything to say about Honda's conjecture or the other way around. If $A_F(j,k)$ or $B_F(j,k)$ can be shown to converge for some $j<0$ as the ABC conjecture predicts, then we would derive a quasi-ABC conjecture from such a result. In case $j \geq 0$, let us note that

$$A_F(j,k) \leq T_F(j,k),$$

and the latter series we have shown converges for $k>1$ and $j \geq 0$ as well as $k=1$ and j sufficiently large. The ABC conjecture would emerge from understanding the behaviour of $B_F(j,k)$ for $j<0$.

It is not clear what the relationship is (if any) between the ABC conjecture and the Honda conjecture. However, in the light of the theorem of Rubin and Silverberg [RS1], we have by Theorem 21 that they have some resemblance in the context of convergence of certain (double) Dirichlet series.

If Honda's conjecture is false and there are quadratic twists of a fixed elliptic curve with arbitrarily large Mordell-Weil rank, then it seems to be very difficult to find them. One method suggested by Silverman of producing elliptic curves of large rank is to produce elliptic curves with many integral points. However, from our study of integral points on curves $my^2=f(x)$ with $f(x)$ of degree 3 or 4, we would expect

$$\sum_{|m|\leq x}{}' \#C_m(\mathbb{Z}) \ll x^{1/3+\varepsilon}$$

so that finding many integral points on twists of elliptic curves would be very difficult.

We also remark that these results are easily extended to number fields. More precisely, one may consider a hyperelliptic curve over a number field K and consider quadratic twists of this curve and study the variation of the number of rational points. The number field analogue of the ABC conjecture was formulated by Vojta [Voj2] and one has similar estimates. Thus all of the previous analysis goes through without much alteration. In this context, it is useful to remark that a beautiful theorem of Moret-Bailly says that if we had an "effective Mordell" theorem for a single curve, valid for all number fields, then the ABC conjecture would follow. Thus the variation of rational points for a single curve over all algebraic number fields suggests a fruitful line of inquiry.

Acknowledgements. We would like to thank Professors Ernst Kani and Michael Roth for their comments on an earlier version of this paper.

References

[Bel] Belyi G. V.: Galois extensions of a maximal cyclotomic field (Russian). Izv. Akad. Nauk. SSSR Ser. Mat. **43** (1979), 267–276

[CGT] Cutter P., Granville A., and Tucker T.: The number of fields generated by the square root of values of a given polynomial. Canad. Math. Bull. **46** (2003), 71–79

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

[Dav] Davenport H.: Multiplicative Number Theory, Springer-Verlag, Second Edition. Graduate Texts in Math. 74, 1980

[Elk] Elkies N.: ABC implies Mordell. Internat. Math. Research Notices **7** (1991), 99–109

[Fal] Faltings G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. **73** (1983), 349–366

[Gran] Granville A.: ABC means we can count squarefrees. Internat. Math. Research Notices **19** (1998), 991–1009

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

[Hoo] Hooley C.: Applications of Sieve Methods to the Theory of Numbers. Cambridge University Press, 1976

[LM] Lee J.-J. and Murty R.: An application of Mumford's gap principle. J. Number Theory **105** (2004), 333–343

[Ma] Mahler K.: Zur Approximation algebraischer Zahlen III, (Über die mittlere Anzahl der Darstellungen grosser Zahlen durch binäre Formen). Acta Math. **62** (1933), 91–166

[M] Murty R.: Problems in Analytic Number Theory. Graduate Texts in Math. 206. Springer-Verlag, New York 2001

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

[Na] Nair M.: Powerfree values of polynomials. Mathematika **23** (1976), 159–183

[Pa] Pappalardi F.: A survey on k-freeness. Ramanujan Mathematical Society Lecture Notes Series No. 1 (edited by S. D. Adhikari, R. Balasubramanian, K. Srinivas) 2004, pp. 71–88

[RS1] Rubin K. and Silverberg A.: Ranks of elliptic curves in families of quadratic twists. Experimental Mathematics **9** (2000), 583–590

[RS2] Rubin K. and Silverberg A.: Ranks of elliptic curves. Bull. Amer. Math. Soc. **39** (2002), 455–474

[ST] Stewart C. L. and Top J.: On ranks of twists of elliptic curves and powerfree values of binary forms. J. Amer. Math. Soc. **8** (1995), 943–973

[Silv] Silverman J.: Representations of integers by binary forms and the rank of the Mordell-Weil group. Invent. Math. **74** (1983), 281–292

[Silv2] Silverman J.: Wieferich's criterion and the abc conjecture. J. Number Theory **30** (1988), 226–237

[Voj] Vojta P.: Siegel's theorem in the compact case. Ann. of Math. **133** (1991), 509–548

[Voj2] Vojta P.: Diophantine Approximations and Value Distribution Theory. Lecture Notes in Mathematics 1239. Springer-Verlag, Berlin 1987

Received August 9, 2005

Department of Mathematics, Queen's University, Kingston, Ontario, K7L 3N6, Canada
jjlee@mast.queensu.ca
murty@mast.queensu.ca