A variant of the Lang–Trotter conjecture

M. Ram Murty and V. Kumar Murty

in memory of Serge Lang

Abstract In 1976, Serge Lang and Hale Trotter formulated general conjectures about the value distribution of traces of Frobenius automorphisms acting on an elliptic curve. In this paper, we study a modular analog. More precisely, we consider the distribution of values of Fourier coefficients of Hecke eigenforms of weight $k \geq 4$.

Key words Lang-Trotter conjecture • *abc* conjecture • Ramanujan τ-function • Atkin-Serre conjecture

Mathematics Subject Classification (2010): 11F03, 11F30

1 Introduction

Let E be an elliptic curve over a number field K. If $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ and E has good reduction at $\mathfrak{p}$, denote by $a_{\mathfrak{p}}(E)$ the integer

$$N\mathfrak{p} + 1 - |E(\mathbf{F}_{\mathfrak{p}})|.$$

---

*Research of both authors partially supported by NSERC grants.

M.R. Murty (✉)
Department of Mathematics Queen's University, Kingston, Ontario, K7L 3N6, Canada
e-mail: murty@mast.queensu.ca

V.K. Murty
Department of Mathematics, University of Toronto, Toronto, Ontario, M5S 2E4, Canada
e-mail: murty@math.toronto.edu

D. Goldfeld et al. (eds.), *Number Theory, Analysis and Geometry: In Memory of Serge Lang*, DOI 10.1007/978-1-4614-1260-1_21,

In 1976, Lang and Trotter [4] formulated some conjectures about how often $a_{\mathfrak{p}}(E)$ takes a fixed value. More precisely, they conjectured that there is a constant $c_{E,a}$ (possibly zero) such that for $x \to \infty$,

$$\pi_{E,a}(x) := \#\{\mathfrak{p} : N\mathfrak{p} \leq x \text{ and } a_{\mathfrak{p}}(E) = a\} \sim c_{E,a}\frac{\sqrt{x}}{\log x},$$

provided we are in the generic case, that is, $a \neq 0$ or E does not have complex multiplication. The constant $c_{E,a}$ depends on the Galois representation attached to E. In 1981, Serre [13] proved that for any $\epsilon > 0$,

$$\pi_{E,a}(x) \ll_\epsilon x/(\log x)^{5/4-\epsilon},$$

in the generic case. The exponent $5/4$ was improved to 2 by Daqing Wan [17]. A further refinement was obtained by the second author in [5] where it is shown that

$$\pi_{E,a}(x) \ll \frac{x(\log\log x)^2}{(\log x)^2}.$$

The case $a_{\mathfrak{p}}(E) = 0$ corresponds to E having supersingular reduction at $\mathfrak{p}$. A classical result of Deuring shows that if E has complex multiplication by an order in an imaginary quadratic field F, the set of supersingular primes of K has density $1/2$ if F is not contained in K and zero if $F \subseteq K$. If E does not have complex multiplication, then Elkies, Kaneko, and R. Murty (see [1]) showed that

$$\pi_{E,0}(x) \ll x^{3/4}.$$

Recently, R. Taylor has announced the meromorphic continuation of symmetric power L-series attached to E (in the case that K is totally real and E has multiplicative reduction at some prime $\mathfrak{p}$). It is conjectured that these symmetric power L-functions extend to entire functions. If we assume this, together with an analogue of the Riemann hypothesis for them, K. Murty [6] has shown that

$$\pi_{E,a}(x) \ll x^{3/4}$$

if $a \neq 0$ or E does not have CM. A substantial generalization and reinterpretation of the Lang–Trotter conjecture can be found in [7], where a more general formulation in terms of Galois representations is made.

In this paper, we consider a normalized Hecke eigenform of weight $k \geq 4$ for the full modular group. We write

$$f(z) = \sum_{n=1}^{\infty} \lambda_f(n) e^{2\pi i n z}$$

for its Fourier expansion at $i\infty$. The field K_f generated by the values $\lambda_f(n)$ as n ranges over all positive integers is of finite degree over $\mathbf{Q}$. We write $\mathcal{O}_f$ for the ring of integers of K_f. In an earlier paper [9], we showed that if $\alpha \in \mathcal{O}_f$ is coprime to 2, then the number of solutions of the equation

$$\lambda_f(n) = \alpha \tag{1}$$

is bounded. Moreover, there is an effectively computable constant $c = c(\alpha) > 0$ such that all solutions n of the equation satisfy

$$n \leq \exp(|N(\alpha)|^c),$$

where $N(\alpha)$ is the norm of α from K_f to $\mathbf{Q}$. This means that for any given α, all the solutions of (1) can be effectively determined. If, in addition, we assume the *abc* conjecture for the number field K_f, then it was shown that the exponential bound can be improved to a polynomial bound of the form $c_1|N(\alpha)|^c$, for some constant $c_1 > 0$ and the same c as before. In the special case of the Ramanujan τ-function, we deduced that the number of solutions of the equation $\tau(n) = a$ with a odd is finite, a result obtained earlier in our joint work with Shorey [11]. Our methods are sufficiently versatile to be applied to related problems. For example, in [10], we study the greatest prime ideal factor of the ideal generated by $\lambda_f(p^n)$ for fixed p and varying n using similar techniques.

In this paper, we want to study the number $\nu_f(a)$ of solutions of the equation

$$|N(\lambda_f(n))| = a$$

for a given natural number a. We prove the following Theorem:

Theorem 1 *Let f be a normalized Hecke eigenform of weight $k \geq 4$ for the full modular group. Assume the abc conjecture for K_f. Let $d = [K_f : \mathbb{Q}]$. Then, for any $\epsilon > 0$,*

$$\sum_{a \leq x}{}' \nu_f(a) \ll x^{2/d(k-3)+\epsilon},$$

where the dash on the summation indicates that we sum over odd, positive a.

We immediately deduce the following corollary:

Corollary 2 *For any normalized Hecke eigenform f of weight $k \geq 4$ for the full modular group,*

$$\nu_f(a) \ll a^{2/d(k-3)+\epsilon},$$

provided a is odd and the abc conjecture holds for K_f.

What is interesting about this corollary is that it is consistent with the Atkin–Serre conjecture (see p.244 of [14]). This conjecture predicts that if f is of weight $k \geq 4$ and is not of CM type, then for sufficiently large primes p,

$$|\lambda_f(p)| \gg p^{(k-3)/2-\epsilon}. \qquad (2)$$

As (2) is conjectured to hold for all conjugates f^σ of f, it implies that

$$|N(\lambda_f(p))| \gg p^{\frac{d(k-3)}{2}-\epsilon}$$

and so

$$\nu_f(a) \ll |a|^{\frac{2}{d(k-3)}+\epsilon}.$$

As was shown in [9], $\lambda_f(p)$ is divisible by 2 for all odd primes p in the level-one case. This is a key fact, since it implies that for α coprime to 2, the equation $\lambda_f(n) = \alpha$ forces n to be a perfect square (see [9]). Thus, Theorem 1 can be extended to higher levels, provided this property holds for all sufficiently large primes. Indeed, Ono and Taguchi [12] have shown that this is the case for all forms of level $2^a N_0$ with a arbitrary and $N_0 = 1, 3, 5, 15$, or 17. We record this observation in the following.

Theorem 3 *Let f be a normalized Hecke eigenform of weight $k \geq 4$ and level N. Suppose that for all primes sufficiently large, $\lambda_f(p)$ is divisible by 2. Assuming the abc conjecture for K_f, we have for any $\epsilon > 0$,*

$$\sum_{a \leq x}{}' \nu_f(a) \ll x^{2/d(k-3)+\epsilon},$$

where the dash on the summation indicates that we sum over a coprime to 2 and $d = [K_f : \mathbb{Q}]$.

Acknowledgements We would like to thank the referee for useful comments on an earlier version of this paper.

2 Preliminaries

We begin by reviewing results proved in an earlier paper [9].

Proposition 4 *Let f be a normalized cuspidal eigenform of weight $k \geq 4$ and level N. There is an effectively computable constant $c_1 > 0$ such that for $m \geq 2$ and every prime p, we have*

$$|\lambda_f(p^m)| \geq |\gamma_f(p, m)| p^{\frac{k-1}{2}(m - c_1 \log m)},$$

where $\gamma_f(p, m) = 1$ if m is even and $\lambda_f(p)$ if m is odd.

Proof. This is Proposition 2.2 of [9]. □

In particular, we see from this proposition that $\lambda_f(p^m) \neq 0$ when m is even and sufficiently large.

Proposition 5 *Let f be a Hecke eigenform of weight k and level N. Then, for all p sufficiently large, either $\lambda_f(p) = 0$ or $\lambda_f(p^a) \neq 0$ for all $a \geq 1$. Moreover,* *for each m, there is a binary form f_m of degree $[m/2]$, with integeral coefficients such that*

$$\lambda_f(p^m) = \gamma_f(p, m) f_m(\lambda_f(p)^2, p^{k-1}).$$

Proof. The first part of the assertion follows from the previous proposition or from Lemma 2.3 of [9]. The second part follows from the proof of the same lemma. The binary form $f_m(x, y)$ is

$$\prod_{r=1}^{[m/2]} (x - 4y\cos^2(\pi r/(m+1))),$$

which is easily seen to have integer coefficients by simple field-theoretic considerations. □

We will also have need of a version of Roth's theorem, which we record in the following lemma.

Lemma 6 (Roth's theorem) *Let f be a binary form with integer coefficients and degree $d \geq 3$. If f has distinct irrational roots, then,*

$$|f(x, y)| \gg \max(|x|, |y|)^{d-2-\epsilon},$$

where the implied constant depends only on the coefficients of f.

Proof. This essentially follows from Roth's theorem. See also [8]. □

A number-field version of this lemma will also be needed in the later sections, and this will be recalled in Section 4.

Our line of argument has its origins in [9] and [11]. In [11], it was observed that the Ramanujan τ-function has the fortuitous property that $\tau(p)$ is even for every prime p. By an analogue of Proposition 5 for the τ-function, we see that $\tau(p^m)$ is even for every odd m. Hence, if we are interested in the equation

$$\tau(n) = a$$

for a odd, it follows that n must be a perfect square, by virtue of the multiplicativity of τ. This was the key fact that enabled the application of results from Baker's theory to establish that the number of solutions to the equation $\tau(n) = a$, with a odd, is finite. This argument was extended to any normalized eigenform for the full modular group in [9]. As indicated in [9], results of Tate [15] imply that $\lambda_f(p)$ is divisible by 2 for every prime p. This enabled us to extend the results of [11] to the full modular case. As indicated in [9], the method can be generalized to arbitrary level provided that $\lambda_f(p)$ is divisible by 2 for all primes p sufficiently large. With this background information in place, we now outline our basic strategy.

We fix a positive integer a coprime to 2 and study the equation

$$|N(\lambda_f(n))| = a.$$

As $\lambda_f(n)$ is multiplicative, we see that $\lambda_f(p^m)$ is coprime to 2 for $p^m||n$. Now suppose that $\lambda_f(p)$ is divisible by 2 for all primes $p \geq c_0$. Then by Proposition 5, we see that $\lambda_f(p^m)$ is divisible by 2 for all *odd* m and $p \geq c_0$. Thus, if we write $n = n_0 n_1 n_2$, where the prime factors of n_1 are $< c_0$ satisfying $\lambda_f(p) \neq 0$, the prime factors p of n_0 are $< c_0$ with $\lambda_f(p) = 0$, and the prime factors of n_2 are $\geq c_0$, then we see that n_2 is a perfect square. For primes $p|n_1$, we have $p < c_0$ and $\lambda_f(p) \neq 0$, so that Proposition 4 shows that

$$|\lambda_f(p^m)| \geq |\gamma_f(p,m)| p^{\frac{k-1}{2}(m - c_1 \log m)}.$$

This means that n_1 is bounded, since the primes and prime powers that divide it are bounded. If we look at n_0, then $\lambda_f(p) = 0$ for each $p|n_0$. Since $p^m||n$, m must be even, for otherwise $\lambda_f(n) = 0$. Thus, n_0 is a perfect square. In any case, n has the form ab^2 with a, b coprime and a bounded and $\lambda_f(b^2) \neq 0$. Thus, we are motivated to study the Dirichlet series

$$D_f(s) = {\sum_{n=1}^{\infty}}' |N(\lambda_f(n^2))|^{-s},$$

where the dash in the summation means we go over those n such that $\lambda_f(n^2) \neq 0$. Since $\lambda_f(n^2)$ is multiplicative, we may write this as an Euler product:

$$D_f(s) = {\prod_p}' \left(\sum_{m=0}^{\infty} \frac{1}{|N(\lambda_f(p^{2m}))|^s} \right),$$

where the dash on the product indicates we go over primes p such that $\lambda_f(p^{2m}) \neq 0$ for any $m \geq 0$. Our objective is to determine a half-plane in which this series converges absolutely.

We remark that if the series

$$\sum_{a=1}^{\infty} \frac{\nu_f(a)}{a^s}$$

converges absolutely for $\Re(s) > c$, then

$$\sum_{n \leq x} \nu_f(a) \ll \sum_{n \leq x} \nu_f(a)(x/n)^{c+\epsilon} \ll x^{c+\epsilon},$$

for any $\epsilon > 0$. We will use this remark in our discussion below.

Let us note also that as

$$|N(\lambda_f(n^2))| \leq n^{(k-1)d} d(n^2),$$

where $d(n)$ denotes the number of divisors of n, the series does not converge for

$$\Re(s) \leq \frac{1}{d(k-1)}.$$

Moreover, as $D_f(s)$ is a Dirichlet series with non-negative coefficients, it must have a singularity at its abscissa of convergence, by a celebrated theorem of Landau. In particular, we have

$$\sum_{a \leq x} \nu_f(a) = \Omega(x^{1/d(k-1)}).$$

3 The special case of Ramanujan's τ-function

For the sake of clarity, we will first consider a special case, namely, the study of the Dirichlet series

$$D_\Delta(s) = \sum_{n=1}^{\infty}{}' \frac{1}{|\tau(n^2)|^s}.$$

Since $\tau(n^2)$ is a multiplicative function, we can expand the series as an infinite product over the primes:

$$D_\Delta(s) = \prod_p{}' \left(\sum_{m=0}^{\infty} |\tau(p^{2m})|^{-s} \right).$$

Our goal is to determine a region of convergence for this series. By Proposition 4, we see that

$$|\tau(p^{2m})| \geq p^{11m(1-\epsilon)}$$

for $m \geq m_0$ (say). This means that the series

$$\sum_{m \geq m_0} |\tau(p^{2m})|^{-\Re(s)} \ll \sum_{m \geq m_0} p^{-11m(1-\epsilon)\Re(s)}$$

converges for $\Re(s) > 0$. To deal with the other part of the series, we need to estimate $\tau(p^{2m})$ for $2 \leq m \leq m_0$. We can use Propostion 5 combined with Roth's theorem to derive a lower bound for $|\tau(p^{2m})|$ for $6 \leq m \leq m_0$. Indeed, Roth's theorem allows us to deduce that

$$|f_m(\tau(p)^2, p^{11})| \gg p^{11(m/2-2-\epsilon)}.$$

We need to discuss lower bounds for $\tau(p^2)$ and $\tau(p^4)$. For this, we need to invoke the *abc* conjecture. To this end, let us define the *radical* of a natural number n, denoted by $\text{rad}(n)$, to be the product of the distinct primes dividing n. The *abc* conjecture predicts that for any two coprime integers a, b,

$$\text{rad}(ab(a+b)) \gg \max(|a|, |b|)^{1-\epsilon},$$

for any $\epsilon > 0$. The implied constant will depend on ϵ but not on a, b.

Lemma 7 *Suppose that $\tau(p) \neq 0$. The abc conjecture implies that for any $\epsilon > 0$,*

$$|\tau(p^2)| \gg p^{9/2-\epsilon}$$

and

$$|\tau(p^4)| \gg p^{10-\epsilon}.$$

Proof. We first apply the *abc* conjecture to the equation

$$\tau(p^2) = \tau(p)^2 - p^{11}.$$

Suppose first that p is coprime to $\tau(p)$. From the *abc* conjecture, we deduce that

$$\text{rad}(\tau(p)^2\tau(p^2)p^{11}) \gg p^{11(1-\epsilon)}.$$

Using $|\tau(p)| \leq 2p^{11/2}$, we obtain

$$|\tau(p^2)| \geq \text{rad}(|\tau(p^2)|) \gg p^{9/2(1-\epsilon)},$$

as desired. If $p|\tau(p)$, write $\tau(p) = p^a v_p$ with v_p coprime to p. As $\tau(p^2) \neq 0$, we deduce that

$$\text{rad}(v_p^2 p^{11-2a}(v_p^2 - p^{11-2a})) \gg p^{11-2a-\epsilon},$$

so that

$$\tau(p^2) = p^{2a}(v_p^2 - p^{11-2a}) \gg p^{9/2+a-\epsilon}.$$

This completes the proof of the first part. For the second part, consider

$$(2\tau(p)^2 - 3p^{11})^2 = 4\tau(p^4) - 5p^{22}.$$

Assuming first that p is coprime to $\tau(p)$, we can apply the *abc* conjecture to this equation to deduce

$$|\tau(p^4)| \gg p^{10(1-\epsilon)}.$$

If $p|\tau(p)$, then we write, as before, $\tau(p) = p^a v_p$ with v_p coprime to p. Then, we have

$$4\tau(p^4) = p^{4a}[(2v_p^2 - 3p^{11-2a})^2 + 5p^{22-4a}].$$

Applying the abc conjecture to the term in the square brackets, we obtain

$$|\tau(p^4)| \gg p^{10+2a-\epsilon},$$

so that the result is proved in this case also. □

We are now in a position to study the convergence of

$$\sum_{m \le m_0} |\tau(p^{2m})|^{-s}.$$

We break the sum into three parts:

$$|\tau(p^2)|^{-s} + |\tau(p^4)|^{-s} + \sum_{3 \le m \le m_0} |\tau(p^{2m})|^{-s}.$$

By our earlier discussion, the last sum is bounded by $p^{-33\Re(s)}$. By the previous lemma, the first two terms are

$$\ll p^{-\frac{9}{2}(1-\epsilon)\Re(s)}.$$

This result immediately implies that $D_\Delta(s)$ converges for $\Re(s) > 2/9$. Thus,

$$\sum_{a \le x}{}' \nu_\Delta(a) \ll x^{2/9+\epsilon}.$$

We record the following corollary for its own intrinsic interest.

Corollary 8 *If a is an odd number, the number of solutions of $\tau(n) = a$ is bounded by $O(|a|^{2/9+\epsilon})$, assuming the abc conjecture.*

4 The abc conjecture for number fields

Let K be an algebraic number field. Suppose $a, b, c \in K^*$ such that $a + b + c = 0$ Define

$$\mathrm{rad}_K(a, b, c) = \prod_{\mathfrak{p}} N_{K/\mathbb{Q}}(\mathfrak{p}),$$

where the product is over those prime ideals for which the numbers

$$||a||_{\mathfrak{p}},\ ||b||_{\mathfrak{p}},\ ||c||_{\mathfrak{p}}$$

are unequal. We will also write rad (a) to be the product of norms of the distinct prime ideal divisors of (a). We define

$$H_K(a,b,c) = \prod_v \max(||a||_v, ||b||_v, ||c||_v),$$

where the product is over all valuations of K (both finite and infinite and we normalize the archimedean valuations by $||x||_v = |x|_v^{d_v}$ with $d_v = 1$ or 2 according as v is real or complex, and the nonarchimedean valuations by $||x||_v = N_{K/\mathbb{Q}}(\mathfrak{p})^{-v(x)}$). The abc conjecture for K is the following assertion. For any $\epsilon > 0$, there is a constant $C_{K,\epsilon}$ such that

$$H_K(a,b,c) \leq C_{K,\epsilon}(\mathrm{rad}_K(a,b,c))^{1+\epsilon}.$$

A stronger version predicts that one may replace $C_{K,\epsilon}$ by

$$C_\epsilon^{[K:\mathbb{Q}]} D_K^{1+\epsilon},$$

where D_K is the absolute value of the discriminant of K. We will not be using this stronger version of the abc conjecture in our discussion below. We refer the reader to Vojta [16] for further details.

We first derive a consequence of the abc conjecture for number fields that will be applied in the subsequent discussion.

Lemma 9 *Let K be an algebraic number field and suppose that $\mathfrak{d} = \gcd((a),(b))$. Suppose for all finite primes $\mathfrak{p}$, $||a||_{\mathfrak{p}} \neq ||b||_{\mathfrak{p}}$ Assuming the abc conjecture for K, we have*

$$\mathrm{rad}(a)\mathrm{rad}(b)\mathrm{rad}(a+b)/(\mathrm{rad}(\mathfrak{d}))^2 \gg \left(\max(|N(a)|, |N(b)|, |N(a+b)|)/N(\mathfrak{d})^2\right)^{1-\epsilon},$$

where N stands for $N_{K/\mathbb{Q}}$ and the implied constant depends on K and ϵ.

Proof. Suppose first that $\mathfrak{d} = 1$. From the definition, we have

$$\mathrm{rad}_K(a,b,a+b) = \prod_{\mathfrak{p}|ab(a+b)} N(\mathfrak{p}),$$

since $a, b, (a+b)$ are mutually coprime. Let us note that for every finite v, we also have that one of

$$||a||_v,\ ||b||_v,\ ||a+b||_v,$$

is 1, so that

$$H_K(a, b, a+b) \geq \max(|N(a)|, |N(b)|, |N(a+b)|).$$

The *abc* conjecture now implies the result in this case. If $\mathfrak{d} \neq 1$, let $\mathfrak{p}$ be a prime ideal dividing $\mathfrak{d}$. By our assumption, $\mathfrak{p}$ enters into the radical. $N(\mathfrak{p})$ enters three times into the product $\mathrm{rad}(a)\mathrm{rad}(b)\mathrm{rad}(a+b)$, and to remove two of the occurences, we can divide by $N(\mathfrak{p})^2$. This completes the proof. □

In our estimations below, we will need a number field version of Lemma 6, and this we record here.

Lemma 10 *Let K be an algebraic number field and f a binary form in $\mathcal{O}_K[x, y]$ with no repeated factors. Then, assuming the abc conjecture for K, we have*

$$\mathrm{rad}_K(f(u, v)) \gg H_K(u, v)^{d-2-\epsilon},$$

where d is the degree of f and $u, v \in K^*$.

Proof. This is proved on page 105 of [2]. □

We remark that if we replace $\mathrm{rad}_K(f(u, v))$ by $|f(u, v)|$, this is essentially Roth's theorem for number fields. Thus, the *abc* conjecture is making a stronger assertion than that implied by Roth's theorem. Indeed, since $|N(f(u, v))| \geq \mathrm{rad}_K(f(u, v))$, we deduce the following:

Corollary 11 *Let K be an algebraic number field and f a binary form in $\mathcal{O}_K[x, y]$. Then,*

$$|N(f(u, v))| \gg H_K(u, v)^{d-2-\epsilon},$$

where d is the degree of f and $u, v \in K^*$, assuming the abc conjecture for K.

Lemma 12 *Suppose that $\lambda_f(p) \neq 0$. Assume the abc conjecture for K_f. Then,*

$$|N(\lambda_f(p^2))| \gg p^{d(k-3)/2-\epsilon}$$

and

$$|N(\lambda_f(p^4))| \gg p^{d(k-2)-\epsilon},$$

where $d = [K_f : \mathbb{Q}]$ and p is unramified in K_f.

Proof. As before, we apply the *abc* conjecture to the equation

$$\lambda_f(p^2) = \lambda_f(p)^2 - p^{k-1}.$$

First suppose that $\lambda_f(p)$ and p are coprime. By Lemma 9 applied to the field K_f, we obtain

$$\mathrm{rad}_{K_f}(\lambda_f(p)^2, p^{k-1}, \lambda_f(p^2)) \gg p^{d(k-1)-\epsilon},$$

where $d = [K_f : \mathbb{Q}]$. We obtain

$$p^d |N(\lambda_f(p))N(\lambda_f(p^2))| \gg p^{d(k-1)-\epsilon},$$

from which we deduce, using the Ramanujan bound $|N(\lambda_f(p))| \leq 2^d p^{d(k-1)/2}$, that

$$|N(\lambda_f(p^2))| \gg p^{d(k-3)/2-\epsilon}.$$

Now suppose that $\mathfrak{p}^a || (\lambda_f(p))$, with $a \geq 1$. Then by taking norms, we obtain the inequality

$$p^{da} \leq p^{d(k-1)/2},$$

implying $a \leq (k-1)/2$. Since k is even, this is a strict inequality. Thus, $a < (k-1)/2$. Since p is unramified,

$$||p^{k-1}||_{\mathfrak{p}} = N(\mathfrak{p})^{-(k-1)} \neq ||\lambda_f(p)^2||_{\mathfrak{p}} = N(\mathfrak{p})^{-2a}.$$

By Lemma 9, we obtain as before,

$$|N(\lambda_f(p^2))| \gg p^{d(k-3)/2-\epsilon}.$$

The lower bound for $|N(\lambda_f(p^4))|$ is derived similarly. We apply the abc conjecture to the equation

$$(2\lambda_f(p)^2 - 3p^{k-1})^2 = 4\lambda_f(p^4) - 5p^{2k-2}.$$ □

5 The Dirichlet series $D_f(s)$

We will now study the series $D_f(s)$ and determine where it converges. Since $N(\lambda_f(n^2))$ is multiplicative, we have the Euler product

$$D_f(s) = \prod_p \left(\sum_{m=0}^{\infty} \frac{1}{|N(\lambda_f(p^{2m}))|^s} \right).$$

Our goal is to determine the region where the Euler product converges absolutely. We split the product into two parts: $p \leq c_0$ and $p > c_0$, for which we have that $\lambda_f(p)$ is divisible by 2. The first product is finite and is over those p for which the $\lambda_f(p^m)$ are all coprime to 2. This product converges for $\Re(s) > 0$. Let us now consider the other product. We proceed as in the case of the τ-function. By Proposition 4, we see that for $m \geq m_0$ (say),

$$|\lambda_f(p^{2m})| \gg p^{m(k-1)(1-\epsilon)}.$$

A similar estimate holds with f replaced by any conjugate form f^{σ}. Thus the series in the Euler product converges for $\Re(s) > 0$ if we restrict $m \geq m_0$. By Corollary 11, we have

$$|f_m(\lambda_f(p)^2, p^{k-1})| \gg p^{(k-1)(m/2-2-\epsilon)}$$

for $6 \leq m \leq 2m_0$. Thus,

$$|\lambda_f(p^{2m})| \gg p^{(k-1)(m-2-\epsilon)}$$

for $3 \leq m \leq m_0$. We deduce that

$$|N(\lambda_f(p^{2m}))| \gg p^{(k-1)d(m-2-\epsilon)},$$

for $3 \leq m \leq m_0$. To complete our estimates, we need lower bounds for $|\lambda_f(p^2)|$ and $|\lambda_f(p^4)|$, which are provided by Lemma 12. From that lemma, we get that

$$|N(\lambda_f(p^2))| \gg p^{d(k-3)/2-\epsilon}, \quad |N(\lambda_f(p^4))| \gg p^{d(k-2)-\epsilon}.$$

Putting all this together shows the following:

Theorem 13 *Assume the abc conjecture for K_f. Let $d = [K_f : \mathbb{Q}]$. Then, the Dirichlet series $D_f(s)$ converges absolutely for $\Re(s) > 2/d(k-3)$. In particular,*

$$\sum_{a \leq x}{}' \nu_f(a) \ll x^{2/d(k-3)+\epsilon},$$

for any $\epsilon > 0$, where the summation is over odd, positive a.

References

1. N. Elkies, Distribution of supersingular primes, Journées Arithmétiques (Luminy, 1989), *Astérisque*, **198–200** (1991), 127–132.
2. N. Elkies, ABC implies Mordell, *International Math. Research Notices*, **1991** (1991), No. 7, 99–109.
3. M. Hindry and J. Silverman, Diophantine Geometry, an Introduction, *Graduate Texts in Mathematics*, **201**, Springer-Verlag, 2000.
4. S. Lang and H. Trotter, Frobenius Distributions in GL_2-extensions, *Lecture Notes in Mathematics*, **504** (1976), Springer.
5. V. Kumar Murty, Modular forms and the Chebotarev density theorem, II, in Analytic Number Theory, edited by Y. Motohashi, *London Math. Society Lecture Notes*, **247** (1997), 287–308, Cambridge University Press.
6. V. Kumar Murty, Explicit formulae and the Lang–Trotter conjecture, *Rocky Mountain Journal*, **15** (1985), 535–551.
7. V. Kumar Murty, Frobenius distributions and Galois representations, *Proc. Symp. Pure Math.*, **66.1** (1999), 193–211.

8. D.J. Lewis and K. Mahler, On the representation of integers by binary forms, *Acta Arith.*, **6** (1960/61), 333–363.
9. M. Ram Murty and V. Kumar Murty, Odd values of Fourier coefficients of certain modular forms, *International Journal of Number Theory*, **3** (2007), no. 3, 455–470.
10. M. Ram Murty and V. Kumar Murty, On a conjecture of Shorey, in Diophantine Equations, edited by N. Saradha, pp. 167–176, Narosa, 2008.
11. M. Ram Murty, V. Kumar Murty, and T.N. Shorey, Odd values of the Ramanujan τ-function, *Bulletin Soc. Math. France*, **115** (1987), no. 3, 391–395.
12. K. Ono and T. Taguchi, 2-adic properties of certain modular forms and their applications to arithmetic functions, *International Journal of Number Theory*, **1** (2005), no. 1, 75–101.
13. J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. IHES*, **54** (1981), 123–201.
14. J.-P. Serre, Divisibilité de certaines fonctions arithmétiques, in *Séminaire Delange-Pisot-Poitou, 16e année* (1974/75), Théorie des nombres, Fasc. 1, Exp. No. 20, 28p., Secrétariat Mathématique, Paris, 1975.
15. J. Tate, The non-existence of certain Galois extensions of $\mathbb{Q}$ unramified outside 2, *Contemporary Mathematics*, **174** (1994), 153–156, American Math. Society, Providence, Rhode Island.
16. P. Vojta, Diophantine approximations and value distribution theory, *Lecture notes in mathematics*, **1239**, Springer-Verlag, Berlin, 1987.
17. D. Wan, On the Lang–Trotter conjecture, *Journal of Number Theory*, **35**(1990), 247–268.