International Journal of Number Theory
Vol. 3, No. 3 (2007) 455–470

World Scientific
www.worldscientific.com

ODD VALUES OF FOURIER COEFFICIENTS OF CERTAIN MODULAR FORMS

M. RAM MURTY

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

V. KUMAR MURTY

Department of Mathematics, University of Toronto
Toronto, Ontario, M5S 2E4, Canada
murty@math.toronto.edu

Received 25 September 2006
Accepted 27 April 2007

In honor of Marvin Knopp

Let f be a normalized Hecke eigenform of weight $k \geq 4$ on $\Gamma_0(N)$. Let $\lambda_f(n)$ denote the eigenvalue of the nth Hecke operator acting on f. We show that the number of n such that $\lambda_f(n)$ takes a given value coprime to 2, is finite. We also treat the case of levels $2^a N_0$ with a arbitrary and $N_0 = 1, 3, 5, 15$ and 17. We discuss the relationship of these results to the classical conjecture of Lang and Trotter.

Keywords: Modular forms; Fourier coefficients; congruences; Lang–Trotter conjecture.

Mathematics Subject Classification 2000: 11F30, 11F33, 11F11, 11J86

1. Introduction

Let f be a holomorphic cuspidal normalized eigenform of weight $k \geq 4$ of level N and trivial Nebentypus. We write

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

for its Fourier expansion at $i\infty$ with $\lambda_f(1) = 1$. It is well known that the field K_f generated by the values $\lambda_f(n)$, as n ranges over all the positive integers, is of finite degree over $\mathbb{Q}$. We write $\mathcal{O}_f$ for its ring of integers. We prove the following.

Theorem 1.1. *Let f be a holomorphic cuspidal normalized eigenform of weight $k \geq 4$ and level N with trivial Nebentypus. Suppose that*

$$\lambda_f(p) \equiv 0 \pmod 2$$

for every prime $p \geq c_0$. If $\alpha \in \mathcal{O}_f$ is coprime to 2, then the number of solutions of the equation

$$\lambda_f(n) = \alpha$$

is bounded. Moreover, there is an effectively computable constant (independent of f) $c = c(\alpha, c_0) > 0$ such that all solutions satisfy the inequality

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

where $N(\alpha)$ is the norm of α from K_f to $\mathbb{Q}$.

We make a few remarks concerning the theorem. The special case $k = 12$ and $f = \Delta$, Ramanujan's cusp form, was discussed in detail by the authors and Shorey in [15]. The fact that Δ satisfies the hypothesis of the theorem is a consequence of Jacobi's celebrated identity:

$$\prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}z^2)(1+q^{2n-1}z^{-2}) = \sum_{n=-\infty}^{\infty} q^{n^2}z^{2n}.$$

Indeed, replacing q by q^4 and z by q^2 (and taking into account the factor of two that appears on the left) gives rise to the identity

$$q\prod_{n=1}^{\infty}(1-q^{8n})(1+q^{8n})^2 = \sum_{n=0}^{\infty} q^{(2n+1)^2}.$$

Thus, if τ denotes Ramanujan's function, then

$$\begin{aligned}\sum_{n=1}^{\infty}\tau(n)q^n &= q\prod_{n=1}^{\infty}(1-q^n)^{24}\\ &\equiv q\prod_{n=1}^{\infty}(1+q^{8n})^3 \pmod 2\\ &\equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod 2.\end{aligned}$$

Thus, $\tau(n)$ is odd if and only if n is an odd square. In particular, $\tau(p)$ is even for every prime p.

Let us now discuss the level 1 case in some detail. In addition to the weight 12 case, the hypothesis of Theorem 1.1 is also satisfied by the unique normalized cuspidal eigenforms of weights $16, 18, 20, 22$ and 26. Indeed, if

$$E_4 := 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n,$$

$$E_6 := 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n,$$

are the classical Eisenstein series of weight 4 and 6 respectively, where

$$\sigma_r(n) = \sum_{d|n} d^r,$$

then we may write these cusp forms as ΔE_4, ΔE_6, ΔE_4^2, $\Delta E_4 E_6$, and $\Delta E_4^2 E_6^2$ respectively. As E_4 and E_6 are both congruent to $1 \pmod 2$, we deduce again that $\lambda_f(n)$ is odd if and only if n is an odd square, for each of these eigenforms.

For $k = 24$, there are two such cuspidal eigenforms given by [7]:

$$\Delta E_4^3 - (156 \pm 12\sqrt{144169})\Delta^2.$$

From this expression, it is clear that modulo 2 is congruent to Δ so that $\lambda_f(n)$ is odd if and only if n is an odd square. Hence, the theorem applies to all normalized cuspidal eigenforms of weight $k \leq 26$ and level 1.

In fact, thanks to some explicit computations of Rankin [17], more can be said. The normalized eigenforms of weights $k = 24, 28, 30, 32, 34$, and 38 can be written explicitly as

$$P_k + (u_k \pm \eta_k)Q_k$$

where k, P_k, Q_k, u_k, η_k are given by the following table:

k	P_k	Q_k	u_k	η_k
24	ΔE_6^2	Δ^2	1572	$12\sqrt{144169}$
28	ΔE_8^2	$\Delta^2 E_4$	-5076	$108\sqrt{18209}$
30	$\Delta E_8 E_{10}$	$\Delta^2 E_6$	4128	$96\sqrt{51349}$
32	ΔE_{10}^2	$\Delta^2 E_8$	20496	$336\sqrt{23323}$
34	$\Delta E_8 E_{14}$	$\Delta^2 E_{10}$	-61272	$72\sqrt{2356201}$
38	$\Delta E_6 E_{10}^2$	$\Delta^2 E_{14}$	96144	$48\sqrt{63737521}$

We note that $u_k \pm \eta_k$ is even in each of the above cases. Thus, the eigenform is congruent to P_k modulo 2. Now,

$$E_8 = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n,$$

$$E_{10} = 1 - 264 \sum_{n=1}^{\infty} \sigma_9(n) q^n,$$

$$E_{12} = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n,$$

and

$$E_{14} = 1 - 24 \sum_{n=1}^{\infty} \sigma_{13}(n) q^n.$$

It is easily checked that $P_k \equiv \Delta \pmod 2$ and so the hypotheses of Theorem 1.1 are satisfied in each of these cases. Thus, in each of the weights $k \leq 38$, $k \neq 36$, any normalized Hecke eigenform of weight k and level 1 satisfies the hypotheses of Theorem 1.1. For the remaining case $k = 36$, we observe with Rankin [17] that there are now 3 eigenforms and they are of the form

$$E_{10}E_{14}\Delta + \mu E_6^2\Delta^2 + \nu\Delta^3,$$

but μ and ν are not explicitly determined in Rankin's paper. In theory, this can be done since it involves only the solving of some cubic equations. However, it is possible to prove a general theorem using some deeper theorems in the theory of ℓ-adic representations.

Indeed, using the theory of modular forms modulo 2 (see, for example, [18, p. 115]), we see that any cusp form modulo 2 is a polynomial in Δ and the action of the Hecke algebra on modular forms mod 2 is locally nilpotent. This implies in particular that for any normalized Hecke cusp form f of weight k and level 1, we have $\lambda_f(p) \equiv 0$ modulo 2 for all odd primes p. More precisely, what this means is the following. Let T_p denote the pth Hecke operator. Then, modulo 2, $T_p(\Delta^i)$ is a linear combination of Δ^j with $j < i$. Hence Theorem 1.1 applies for all cuspidal eigenforms belonging to the full modular group. This can also be seen in terms of ℓ-adic representations attached to modular forms. In our context, for each prime ℓ, a normalized Hecke eigenform f gives rise to a λ-adic representation with λ a prime ideal of $\mathcal{O}_f$ above ℓ,

$$\rho_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_{f,\lambda}),$$

which is unramified at ℓ and the primes dividing N. For p coprime to ℓN, we have that

$$\mathrm{tr}(\rho(\mathrm{Frob}_p)) = \lambda_f(p),$$

and

$$\det(\rho(\mathrm{Frob}_p)) = p^{k-1},$$

by a well-known theorem of Deligne [4]. If we apply this to our context with $\ell = 2$ and $N = 1$, we get a representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_2)$$

ramified only at 2. Such representations are trivial, by a theorem of Tate [21]. Hence the trace of the Frobenius automorphism is even and we obtain our result. That is, in the level 1 case, the hypotheses of Theorem 1.1 are satisfied and so, we record these observations in the following:

Theorem 1.2. *Let f be a normalized Hecke cuspidal eigenform of weight $k \geq 4$ for the full modular group. Let $\alpha \in \mathcal{O}_f$ be coprime to 2. Then, the number of solutions of the equation*

$$\lambda_f(n) = \alpha$$

is finite. Moreover, there is an effectively computable constant $c = c(\alpha) > 0$ *such that all the solutions satisfy the inequality*

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

where $N(\alpha)$ *is the norm of* α *from* K_f *to* $\mathbb{Q}$.

Theorem 1.1 also holds for certain higher levels. For example, if the level is a power of 2 the result still holds and more generally, if the level is of the form $2^a N_0$ with $N_0 = 1, 3, 5, 15$, or 17, thanks to a theorem of Ono and Taguchi [16]. In the last section, we give a further example of modular forms for which Theorem 1.1 is true.

Theorem 1.1 resolves special cases of a conjecture that is in the spirit of Lang and Trotter [8]. They were working in the context of elliptic curves, or equivalently, with forms f of weight 2 and with $K_f = \mathbb{Q}$. They developed a probabilistic model, on the basis of which they conjectured the frequency of values of the $\lambda_f(p)$. Extrapolating that model for higher weight (as done in [10]), it is expected that for forms of weight ≥ 2 for which $[K_f : \mathbb{Q}] \geq 3$, a given value is attained by the $\lambda_f(p)$ only a finite number of times. For forms of weight ≥ 3 and for which $[K_f : \mathbb{Q}] \geq 2$ and for all forms of weight ≥ 4, it is again expected that a given value is attained by the $\lambda_f(p)$ only a finite number of times. Following [10], we refer to this as the Lang–Trotter conjecture.

One can formulate what we call the strong Lang–Trotter conjecture, that in fact, the number of natural numbers n with $\lambda_f(n) = \alpha$ is finite whenever the weight $k \geq 4$. The argument used to derive Theorem 1.1 implies

Theorem 1.3. *The Lang–Trotter conjecture implies the strong Lang–Trotter conjecture.*

The fact that these two conjectures are equivalent may be intuitively clear in the case f has rational integer coefficients (in view of the multiplicativity of the coefficients). However, in the other cases, it is far from being obvious because of the presence of infinitely many units (since it is known that K_f is totally real). In fact, we will prove Theorem 1.3 using some of the deeper results of transcendental and algebraic number theory.

If we assume the *abc* conjecture, we can deduce a substantial improvement of the bound in Theorem 1.1:

Theorem 1.4. *Let* f *be as in Theorem* 1.1 *and assume the abc conjecture for the field* K_f. *For any* $\epsilon > 0$, *there is a constant* $c = c(K_f, \epsilon)$ *such that every solution of* $\lambda_f(n) = \alpha$ *for a fixed* $\alpha \in \mathcal{O}_f$ *satisfies*

$$n \leq c|N(\alpha)|^{1+\epsilon}.$$

The value of c in the above theorem can be computed from our arguments below if one assumes a uniform version of the *abc* conjecture for number fields.

2. Proof of Theorem 1.1

To prove Theorem 1.1, we need some results from the theory of linear forms in logarithms.

Proposition 2.1 [2]. *Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers different from 0 and $b_1, \ldots, b_n$ be rational integers. Let $A_i = \max(H(\alpha_i), e)$ and $H(\alpha)$ denote the naive height (maximum of the coefficients of the minimal polynomial) and*

$$B = \max(|b_1|, \ldots, |b_n|, e).$$

Set

$$\Omega = \prod_{i=1}^{n} \log A_i,$$

and $d = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$. Let

$$\Lambda := \alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1.$$

Then, either $\Lambda = 0$ or

$$|\Lambda| > \exp(-(16nd)^{2(n+2)}\Omega(\log B)).$$

We will also need bounds on the solutions of various hyperelliptic and superelliptic curves. In 1969, Baker gave the first such bounds for rational integer solutions of the hyperelliptic equation $y^2 = f(x)$ when $f(x) \in \mathbb{Z}[x]$ has at least three simple zeros. These results have been extended to algebraic number fields by various authors, beginning with Sprindzuk, Brindza, Schmidt, Poulakis and finally Voutier [23]. To state these results, we begin with some notation.

Let K be an algebraic number field of degree d and absolute discriminant D_K and $\mathcal{O}_K$ the ring of integers of K. For a point

$$x = [x_0, \ldots, x_n] \in \mathbb{P}^n(K),$$

we define the *field height* of x as

$$H_K(x) = \prod_v \max(|x_0|_v, \ldots, |x_n|_v)^{d_v},$$

where the product is over all archimedean valuations and d_v are the local degrees (that is, $d_v = 1$ or 2 according as v is real or complex). If $\alpha \in K$, we define $H_K(\alpha)$ to be $H_K([1, \alpha])$ and if f is a polynomial in $K[x]$, we set $H_K(f)$ to be the field height of the point in projective space determined by the coefficients of f. We define the *size* of α, denoted $s(\alpha)$, to be the maximum abolute value of all the conjugates of α. We also let $\log^+ |x| = \max(1, \log |x|)$ for any non-zero real number x.

We now state a special case of the main theorem of [23] that is needed for our purpose.

Proposition 2.2 [23]. *Let K be an algebraic number field of degree d and suppose $f(x) \in K[x]$ has degree n. Suppose further that f has at least three distinct simple roots. Then, all solutions (x, y) of $y^2 = f(x)$ with $x \in \mathcal{O}_K$ satisfy*

$$\max(H_K(x), H_K(y)) < \exp(c_1(n, d)V_1(\log^+ V_1)^{6n^2 d})$$

where

$$V_1 = D_K^{6n^2} H_K(f)^{30n^2},$$

and $c_1(n,d)$ is an effectively computable constant depending on n and d.

The following proposition, due to Sprindzuk, gives upper bounds for solutions of the Thue equation in algebraic number fields.

Proposition 2.3 [20]. *Let $F(x,y) \in \mathcal{O}_K[x,y]$ be a binary form of degree n and suppose that $F(x,1)$ has at least three distinct zeros. If $0 \neq \alpha \in \mathcal{O}_K$, then all solutions $x, y \in \mathcal{O}_K$ such that*

$$F(x,y) = \alpha$$

have size bounded by

$$c_1(s(\alpha)H(F))^{c_2}$$

where c_1, c_2 are effectively computable constants depending only on the regulator and the degree of the splitting field of $F(x,1)$.

Proof. This is [20, p. 82, Theorem 6.1]. □

We begin by applying this result (as in [15]) to deduce the following:

Proposition 2.4. *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,*

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

where

$$\gamma_f(p,m) = \begin{cases} 1 & \text{if } m \text{ is even} \\ \lambda_f(p) & \text{if } m \text{ is odd.} \end{cases} \tag{1}$$

When m is odd, $\lambda_f(p^m)$ is divisible by $\lambda_f(p)$.

Proof. By Deligne [5], we may write

$$\lambda_f(p^m) = \frac{\alpha_p^{m+1} - \beta_p^{m+1}}{\alpha_p - \beta_p},$$

where $|\alpha_p| = |\beta_p| = p^{(k-1)/2}$ and $\alpha_p \beta_p = p^{k-1}$. Suppose first that m is odd. Since

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}),$$

we see that

$$\alpha_p^{m+1} - \beta_p^{m+1} = (\alpha_p^2 - \beta_p^2)(\alpha_p^{m-1} + \alpha_p^{m-3}\beta_p^2 + \cdots + \beta_p^{m-1}),$$

from which we see that $\lambda_f(p) = \alpha_p + \beta_p$ divides $\lambda_f(p^m)$ when m is odd. This proves the second assertion of the proposition. If now m is odd and $\lambda_f(p) \neq 0$, then

$$|\lambda_f(p^m)/\lambda_f(p)| = |\alpha_p^{m+1} - \beta_p^{m+1}||\alpha_p^2 - \beta_p^2|^{-1}.$$

Since

$$|\alpha_p^2 - \beta_p^2| \leq 2p^{k-1},$$

we find

$$|\lambda_f(p^m)/\lambda_f(p)| \geq \frac{1}{2}p^{(k-1)(m-1)/2}|(\alpha_p/\beta_p)^{m+1} - 1|.$$

Noting that $\log H(\alpha_p/\beta_p) \ll \log p$, an application of Proposition 2.1 gives

$$\left|\frac{\alpha_p^{m+1} - \beta_p^{m+1}}{\beta_p^{m+1}}\right| > p^{-C\log m}.$$

Therefore,

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

for some effective constant $c_1 > 0$. The proof for m even is similar. □

We remark that the constant c_1 above depends only on the weight k. In fact, the argument shows that

$$c_1 \ll k^2[K_f : \mathbb{Q}]^8.$$

We now study the implication of the previous proposition to the study of the equation $\lambda_f(n) = \alpha$ with α coprime to 2 and initiate our proof of Theorem 1.1. Indeed, starting from the equation

$$\prod_{p^\beta || n} \lambda_f(p^\beta) = \alpha,$$

we observe that all the β are even and we get

$$|N(\alpha)| = \prod_\sigma \prod_{p^\beta || n} |\lambda_{f^\sigma}(p^\beta)|,$$

where the outer product is over all distinct embeddings of K_f into $\mathbb{C}$. Since, $\gamma_{f^\sigma}(p, \beta) = 1$, by Proposition 2.4, we deduce

$$p^{\frac{k-1}{2}[K_f:\mathbb{Q}](\beta - c_1\log\beta)} \leq |N(\alpha)|$$

so that for β large, p^β is bounded.

We have to analyze what happens for small β.

Suppose for $t \geq c_2$, we have

$$\frac{1}{2}t - c_1\log t \geq 0.$$

Write $n = n_1n_2$ where $(n_1, n_2) = 1$, and n_1 is composed of prime powers p^β with $\beta < c_2$ and $p^\beta || n_2$ implies that $\beta \geq c_2$. Then, by Proposition 2.4, we get

$$|\lambda_f(n_2)| \geq n_2^{(k-1)/4}.$$

Hence,

$$|N(\alpha)| \geq |N(\lambda_f(n_1))N(\lambda_f(n_2))| \geq n_2^{[K_f:\mathbb{Q}](k-1)/4}.$$

Thus, n_2 is bounded. This means that $\lambda_f(n_2)$ can take on only a finite number of values and among these values, we consider only those that divide α. For this purpose, we will study

$$\lambda_f(n_1) = \alpha',$$

for some finite set of divisors α' of α. Since λ_f is multiplicative, we are reduced to studying the ideal equation of the form

$$(\lambda_f(p^m)) = \mathfrak{a}$$

with m bounded and $\mathfrak{a}$ an ideal divisor of (a). To study $\lambda_f(p^m)$ for $m \geq 6$, we proceed as in [15]. However, we need to refine our analysis. To this end, we prove the following lemma:

Lemma 2.5. *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 $a \geq 1$.*

Proof. As in [15, Lemma 1], we write

$$\lambda_f(p^m) = \gamma_f(p,m) \prod_{r=1}^{[m/2]} (\alpha_p - \zeta^r \beta_p)(\alpha_p - \zeta^{-r}\beta_p)$$

where ζ is a primitive $(m+1)$st root of unity. Suppose that $\lambda_f(p) \neq 0$. If $\lambda_f(p^m) = 0$ then we must have $\alpha_p = \eta\beta_p$ for some root of unity $\eta \in \mathbb{Q}(e^{\frac{2\pi i}{m+1}})$. Since α_p, β_p have degree bounded by $2[K_f : \mathbb{Q}]$, we see that η has degree bounded by $2[K_f : \mathbb{Q}]$. Since $\lambda_f(p) \neq 0$, we have $\eta \neq -1$. Also, writing $\beta_p = \theta p^{(k-1)/2}$, and using $\alpha_p\beta_p = p^{k-1}$, we get $\theta^2\eta = 1$ so that θ is also a root of unity of degree at most $4[K_f : \mathbb{Q}]$. Let $\widetilde{K}_f$ be the field obtained from K_f by adjoining all the roots of unity of degree $\leq 4[K_f : \mathbb{Q}]$. Then $\widetilde{K}_f$ has bounded degree over $\mathbb{Q}$. But then

$$\lambda_f(p) = \alpha_p + \beta_p = (1+\eta)\beta_p = p^{(k-1)/2}(\theta + \theta^{-1}).$$

As k is even, it follows that $\sqrt{p}(\theta + \theta^{-1}) \in \widetilde{K}_f$. Since $\theta \in \widetilde{K}_f$, and $\eta \neq -1$, we deduce that $\sqrt{p} \in \widetilde{K}_f$. This can happen for only finitely many p since $\widetilde{K}_f$ has only finitely many quadratic subfields. This completes the proof. □

We note for future reference that when m is even, the proof of Proposition 2.5 shows that $\lambda_f(p^m)$ is a binary form $f_m(\lambda_f(p)^2, p^{k-1})$ where f has degree $m/2$ and integer coefficients. Indeed, we have

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

since

$$(\alpha_p - \zeta^r\beta_p)(\alpha_p - \zeta^{-r}\beta_p) = \alpha_p^2 + \beta_p^2 - 2p^{k-1}\cos 2\pi r/(m+1),$$

which is easily seen to be

$$\lambda_f(p)^2 - 4p^{k-1}\cos^2 \pi r/(m+1).$$

We are now ready to complete the proof of Theorem 1.1. We have already observed that if α is coprime to 2, then the equation

$$\lambda_f(n) = \alpha$$

implies that n is of the form ab with the prime factors of a bounded by c_0 (as given in Theorem 1.1) and with b an odd square since for any prime $p^\beta || b$ with β odd, we have $\lambda_f(p)$ which is divisible by 2 divides $\lambda_f(p^\beta)$, under the conditions of Theorem 1.1. (There is no connection between this factorization of n and the earlier factorization of $n = n_1 n_2$ needed for our preliminary analysis.) By Proposition 2.4, we may assume that if we write

$$n = \prod_{p^m || n} p^m,$$

then m is bounded. Thus a is bounded. Let us consider now the shape of b and $p^m || b$. For $m \geq 6$, m even, $\lambda_f(p^m)$ is a binary form in $\lambda_f(p)$ and p^{k-1} of degree ≥ 3. Let h be the class number of K_f. Writing

$$(\alpha) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t},$$

we have for some $f_i \leq e_i$

$$(\lambda_f(p^m)) = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_t^{f_t}.$$

Fix ρ_i such that

$$\mathfrak{p}_i^h = (\rho_i).$$

Then,

$$(\lambda_f(p^m))^h = (\alpha'),$$

where

$$\alpha' = \rho_1^{f_1} \cdots \rho_t^{f_t}.$$

Thus,

$$\lambda_f(p^m)^h = \epsilon \alpha',$$

for some unit ϵ. We write

$$\epsilon = \epsilon_1^{a_1} \cdots \epsilon_t^{a_t},$$

for a fundamental system of units $\epsilon_1, \ldots, \epsilon_r$ of $\mathcal{O}_f$. We write

$$a_i = t_i(mh/2) + \delta_i, \quad 0 \leq \delta_i < mh/2,$$

so that δ_i is bounded. Thus, for some unit u, we can write

$$\lambda_f(p^m)^h = \epsilon_0 u^{mh/2} \alpha',$$

from which we get

$$\lambda_f(p^m) = u^{m/2} (\epsilon_0 \alpha')^{1/h}.$$

As noted earlier, the left-hand side is a binary form of degree $m/2$. The $u^{m/2}$ can be absorbed into the binary form of degree $m/2$ given by $\lambda_f(p^m)$. Thus, with earlier

notation, we have

$$f_m(\lambda_f(p)^2/u, p^{k-1}/u) = (\epsilon_0\alpha')^{1/h}.$$

There are only a finite number of possible values of ϵ_0. We therefore deduce in this case that for $m \geq 6$, the equation has only finitely many solutions. In particular, p^{k-1}/u has bounded norm and so there are only finitely many possibilities for p. These primes can be effectively bounded using Proposition 2.3.

This leaves the case $m = 2, 4$ for discussion. Let us consider the case $m = 2$. In this case, we have the equation

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

as is easily verified. Thus, for a specified value β of $\lambda_f(p^2)$, the equation gives an integral point $(p, \lambda_f(p))$ on the elliptic curve

$$y^2 = x^3 + \beta,$$

if $k = 4$. If $k \geq 5$, we have the integral point $(p, \lambda_f(p))$ on the hyperelliptic curve

$$y^2 = x^{k-1} + \beta.$$

In any case, there are only finitely many $\mathcal{O}_f$ integral solutions. Note that $\lambda_f(p^2)$ can range over a finite collection of values (upto associates). We treat this difficulty, as before, by writing

$$\lambda_f(p^2) = \epsilon\alpha',$$

and $\epsilon = \epsilon_0 u^{2(k-1)}$, with u a unit, using the Dirichlet unit theorem. For $m = 4$, we proceed similarly. We have

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

so that for a fixed value β of $\lambda_f(p^4)$, we have an integral point $(p, 2\lambda_f(p)^2 - 3p^{k-1})$ on the curve

$$y^2 = 5x^{2(k-1)} + 4\beta.$$

This case is now handled in an identical fashion as the case $m = 2$. Thus, the equation

$$\lambda_f(n) = \alpha$$

has only finitely many solutions. Moreover, Proposition 2.2 can be used to bound these solutions and this completes the proof of Theorem 1.1.

We now make some remarks on the size of the solutions. It is clear from the preceding argument that for m sufficiently large,

$$\lambda_f(p^m) = \alpha'$$

implies that p^m is itself bounded by an absolute constant. As the number of prime ideal divisors of α are bounded by $\log|N(\alpha)|$, this would give us a bound of

$$C^{\log|N(\alpha)|} = |N(\alpha)|^{c_1},$$

for the size of any solution.

For $m \geq 6$, m bounded, the results of Sprindzuk (Proposition 2.3) alluded to earlier give an absolute constant c_2 such that

$$\max(\lambda_f(p)^2, p^{k-1}) \leq |N(\alpha)|^{c_2}.$$

It will be noted that the cases $m = 2$ and $m = 4$ led to poor bounds above arising from Proposition 2.2. One can obtain better results assuming the *abc* conjecture for number fields. We recall the formulation of this conjecture. 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 $\mathfrak{p}$ for which the numbers

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

are unequal. Then, 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 take replace $C_{K,\epsilon}$ by

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

where C_ϵ depends only on ϵ. We refer the reader to Vojta [22] for further details. But we do not need the stronger version of the *abc* conjecture here. We will simply use the weaker version to treat the equation

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

Using the *abc* conjecture for number fields, we easily see that any solution of the equations treated in the cases $m = 2$ and $m = 4$ has height bounded by

$$C_{K,\epsilon} N(\alpha)^{1+\epsilon}.$$

In this way, we deduce the estimates of Theorem 1.4. We emphasize that the *abc* conjecture is only needed in the estimation of size of solutions in the $m = 2$ and $m = 4$ cases.

3. Proof of Theorem 1.3

We want to show that the Lang–Trotter conjecture implies the strong Lang–Trotter conjecture. We proceed as in the previous section. From the equation

$$\lambda_f(n) = \alpha,$$

we proceed to the ideal equation

$$\prod_{p^\beta || n} (\lambda_f(p^\beta)) = (\alpha) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

from which we deduce that

$$(\lambda_f(p^\beta)) = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_g^{f_g},$$

for some $f_i \leq e_i$. As before, taking hth powers, we get

$$\lambda_f(p^\beta)^h = \epsilon\alpha',$$

for some unit ϵ and we deduce analogously the equation

$$\lambda_f(p^\beta) = \alpha'',$$

with α'' ranging over a *finite* set of algebraic integers. In the earlier discussion, we assumed β even but now we must consider β odd too. In this situation, $\lambda_f(p^\beta)/\lambda_f(p)$ is a binary form of degree $(\beta-1)/2$. If $\beta \geq 5$, the preceding discussion applies and we deduce a finite set of possible values of p^β. If $\beta = 1$, the Lang–Trotter conjecture implies only finitely many values of p exist for which the equation holds. If $\beta = 3$, we note the identity

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

Arguing as before, we get the equation

$$\lambda_f(p)^2 - 2p^{k-1} = \alpha''',$$

where α''' ranges over a finite set of algebraic integers. This means that $(p, \lambda_f(p))$ lies on the curve

$$y^2 = 2x^{k-1} + \alpha'''.$$

This is a hyperelliptic curve if $k \geq 4$ and there are only finitely many possible values of p. This completes the proof of Theorem 1.3.

4. An Example

In this section, we will give an example of an eigenform of weight k and level $N > 1$ to which our Theorem 1.1 applies.

This is provided by the Calabi–Yau three-fold which has an affine model given by

$$x + x^{-1} + y + y^{-1} + z + z^{-1} + w + w^{-1} = 0.$$

If we let N_p^* be the number of solutions over $\mathbb{F}_p$, with $xyzw \neq 0$, then one can show [6] for $p \neq 2, 3$

$$N_p^* = p^3 - 2p^2 - a_p - 7,$$

where a_n is the nth Fourier coefficient of the weight 4 cusp form of level 8 given by

$$\eta(2z)^4\eta(4z)^4,$$

with $\eta(z)$ the Dedekind η-function. It is easy to see that by pairing up (x, y, z, w) with $(x^{-1}, y^{-1}, z^{-1}, w^{-1})$ in the affine model, N_p^* is even for $p \neq 2, 3$. By direct checking, we see $a_2 = 0$, and $a_3 = -4$. Thus, a_p is even for every prime p. Hence Theorem 1.1 applies to this eigenform of weight 4 and level 8.

Another way of seeing this suggested by the referee is by noting that the form in question is

$$\begin{aligned} & q\prod_{n=1}^{\infty}(1-q^{2n})^4(1-q^{4n})^4 \\ & \quad \equiv q\prod_{n=1}^{\infty}(1-q^{8n})(1-q^{16n}) \\ & \quad \equiv q\prod_{n=1}^{\infty}(1-q^{n})^{24} \\ & \quad \equiv \Delta \pmod 2. \end{aligned}$$

Here, q denotes as usual $e^{2\pi iz}$.

This particular eigenform has an interesting connection to Apéry numbers, defined as

$$A_n := \sum_{j=0}^{n}\binom{n+j}{j}^2\binom{n}{j}^2.$$

These numbers were used by Roger Apéry in his famous 1978 proof that $\zeta(3)$ is irrational. In 1987, Beukers [3] proved that for every odd prime p, we have

$$a_p \equiv A_{(p-1)/2} \pmod p.$$

Extending the work of Ishikawa, Ahlgren and Ono [1] showed the stronger congruence

$$a_p \equiv A_{(p-1)/2} \pmod{p^2}.$$

5. Concluding Remarks

To apply Theorem 1.1 to any specific eigenform, it suffices to verify that $\lambda_f(p)$ is even for a finite number of primes to ensure that it is the case for all primes sufficiently large. If the level is coprime to 2, then there is an effectively computable constant $c > 0$ such that $\lambda_f(p) \equiv 0 \pmod 2$ for all $p < N^c$ implies that this holds for all p. This follows from the effective version of the Chebotarev density theorem (see, for example, [12]).

An important question is whether one can obtain uniform bounds for the solutions in Theorem 1.1. This is indeed possible and our methods can be fine tuned to obtain such results. However, the bounds are again exponential and these poor estimates arise from the fact that we do not have good estimates for integral points on hyperelliptic curves. Again, strong versions of the *abc* conjecture for number fields can be invoked to improve these bounds.

These methods are versatile to deal with other related questions. For example, one can study the growth of the largest prime ideal factor of $\lambda_f(p^n)$ for fixed prime p and varying n, as is done in [13]. They can also be combined with the method

of Dirichlet series and employed in the study of the number of solutions of the equation $|N(\lambda_f(\alpha))| = a$ for a fixed positive integer a as in [14]. In both instances, transcendental number theory plays a fundamental role as it did in this paper.

Acknowledgments

We would like to thank the referee for useful remarks on an earlier version of this paper. The research was partially supported by an NSERC grant.

References

[1] S. Ahlgren and K. Ono, Modularity of a certain Calabi–Yau threefold, *Monatsh. Math.* **129**(3) (2000) 177–190.
[2] A. Baker and G. Wusthölz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993) 19–62.
[3] F. Beukers, Another congruence for the Apéry numbers, *J. Number Theory* **25**(2) (1987) 201–210.
[4] P. Deligne, *Formes Modulaires et Représentations ℓ-Adiques*, Sém. Bourbaki, 1968–1969, No. 355, Lecture Notes in Mathematics, Vol. 179 (Springer-Verlag, 1971), pp. 139–172.
[5] P. Deligne, La conjecture de Weil I, *Inst. Hautes Études Sci. Publ. Math.* **43** (1974) 273–307.
[6] B. van Gemeen and N. Nygaard, On the geometry and arithmetic of some Siegel modular three-folds, *J. Number Theory* **53** (1995) 45–87.
[7] E. Hecke, Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktenwicklung, *Math. Ann.* **114** (1937) 1–28.
[8] S. Lang and H. Trotter, *Frobenius Distributions in GL_2 Extensions*, Lecture Notes in Mathematics, Vol. 504 (Springer-Verlag, 1976), 274 pp.
[9] D. H. Lehmer, The vanishing of Ramanujan's function $\tau(n)$, *Duke Math. J.* **14** (1947) 429–433.
[10] V. Kumar Murty, Frobenius distributions and Galois representations, in *Automorphic Forms, Automorphic Representations, and Arithmetic*, eds. R. Doran, Z.-L. Dou and G. Gilbert, Proc. Symp. Pure Math., Vol. 66, Part 1 (American Mathematical Society, Providence, RI, 1999), pp. 193–212.
[11] M. Ram Murty, The Ramanujan τ-function, in *Ramanujan Revisited (Urbana-Champaign, Ill., 1987)* (Academic Press, Boston, MA, 1988), pp. 269–288.
[12] M. Ram Murty, V. Kumar Murty and N. Saradha, Modular forms and the Chebotarev density theorem, *Amer. J. Math.* **110**(2) (1988) 253–281.
[13] M. Ram Murty and V. Kumar Murty, On a conjecture of Shorey, to appear in *Proceedings in Honour of T.N. Shorey* (Tata Institute for Fundamental Research, 2007).
[14] M. Ram Murty and V. Kumar Murty, A variant of the Lang–Trotter conjecture, to appear in *Lang Memorial Volume* (Springer, 2007).
[15] M. Ram Murty, V. Kumar Murty and T. N. Shorey, Odd values of the Ramanujan τ-function, *Bulletin Soc. Math. France* **115**(3) (1987) 391–395.
[16] K. Ono and Y. Taguchi, 2-adic properties of certain modular forms and their applications to arithmetic functions, *Int. J. Number Theory* **1**(1) (2005) 75–101.
[17] R. A. Rankin, Newforms for the modular group on spaces of dimension 2, in *Number Theory in Progress*, eds. K. Győry, H. Iwaniec and J. Urbanowicz, Vol. 2 (de Gruyter, 1999), pp. 1065–1070.

[18] J.-P. Serre, Valeurs propres des opérateurs de Hecke modulo ℓ, *Astérisque* **24–25** (1975) 109–117.
[19] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics, Vol. 87 (Cambridge University Press, 1986).
[20] V. G. Sprindzuk, *Classical Diophantine Equations*, Lecture Notes in Mathematics, Vol. 1559 (Springer-Verlag, 1993).
[21] J. Tate, *The Non-Existence of Certain Galois Extensions of* $\mathbb{Q}$ *Unramified Outside* 2, Contemporary Mathematics, Vol. 174 (American Mathematical Society, Providence, RI, 1994), pp. 153–156.
[22] P. Vojta, *Diophantine Approximations and Value Distribution Theory*, Lecture Notes in Mathematics, Vol. 1239 (Springer-Verlag, 1987).
[23] P. M. Voutier, An upper bound for the size of integral solutions to $y^m = f(x)$, *J. Number Theory* **53** (1995) 247–271.