VARIANTS OF LEHMER'S SPECULATION FOR NEWFORMS

JENNIFER S. BALAKRISHNAN, WILLIAM CRAIG, KEN ONO, AND WEI-LUN TSAI

Abstract. In the spirit of Lehmer's unresolved speculation on the nonvanishing of Ramanujan's tau-function, it is natural to ask whether a fixed integer α is a value of $\tau(n)$ or is a Fourier coefficient $a_f(n)$ of any given newform $f(z)$. We offer a method, which applies to newforms with integer coefficients and trivial residual mod 2 Galois representation, that answers this question for odd α. We determine infinitely many spaces for which the ordinary primes $3 \leq \ell \leq 37$ are not absolute values of coefficients of newforms with integer coefficients, and we obtain many explicit examples for $\tau(n)$. We also obtain sharp lower bounds for the number of prime factors of such newform coefficients. In the weight aspect, for powers of odd ordinary primes ℓ, we prove that $\pm\ell^m$ is not a coefficient of any such newform f with weight $2k > M^{\pm}(\ell, m)$ and even level coprime to ℓ, where $M^{\pm}(\ell, m)$ are effectively computable constants that are $O_\ell(m)$.

1. Introduction and statement of results

In a paper innocently entitled "On certain arithmetical functions," Ramanujan introduced his tau-function, whose values are the coefficients of the weight 12 modular form (note: $q := e^{2\pi iz}$ where $\mathrm{Im}(z) > 0$)

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n := q \prod_{n=1}^{\infty} (1-q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - \cdots . \tag{1.1}$$

These coefficients have served as a prototype and testing ground for important phenomena in the theory of modular forms. Their multiplicative properties offered hints of the theory of Hecke operators. Ramanujan's conjectured bounds on their size are famous corollaries of Deligne's proof of the Weil Conjectures. Furthermore, Ramanujan offered congruences [11, 33, 35], such as

$$\tau(n) \equiv \sum_{1 \leq d \mid n} d^{11} \pmod{691}, \tag{1.2}$$

that Serre [35] later viewed as glimpses of the theory of modular ℓ-adic Galois representations.

Despite these important roles, some of the function's most basic properties remain unknown. For example, Lehmer's speculation[1] that $\tau(n)$ never vanishes remains open. Lehmer proved [24] that if $\tau(n)$ ever vanishes, then there is a prime p for which $\tau(p) = 0$. Using the Chebotarev Density Theorem, Serre [36] established a quantitative result that implies that the set of such primes p (if any) has density zero within the primes. Serre's estimate, which holds for weight

Key words and phrases. Modular forms, Lehmer's Conjecture.

The first author acknowledges the support of the NSF (DMS-1702196), the Clare Boothe Luce Professorship (Henry Luce Foundation), a Simons Foundation grant (Grant #550023), and a Sloan Research Fellowship. The third author thanks the support of the Thomas Jefferson Fund and the NSF (DMS-1601306 and DMS-2055118).

[1] "Lehmer's Conjecture" is the assertion that $\tau(n)$ never vanishes. To our knowledge, he never formulated such a conjecture, and so we refer to his question as his speculation.

≥ 2 newforms without complex multiplication, has been improved several times, and thanks to work by Thorner and Zaman [37] it is now known that

$$\#\{p \leq X \text{ prime } : \tau(p) = 0\} \ll \pi(X) \cdot \frac{(\log\log X)^2}{\log X},$$

where $\pi(X)$ is the usual prime counting function. Recent work by Calegari and Sardari [17] considers a different aspect; they establish that at most finitely many non-CM newforms with fixed tame p level N have vanishing pth Fourier coefficient.

We consider a variation of Lehmer's original speculation that has also been the focus of study. For an odd integer α, Murty, Murty, and Shorey [29] proved (see [30] for a generalization) that $\tau(n) = \alpha$ for at most finitely many n. Due to the enormous bounds that arise in the theory of linear forms in logarithms (the crux of their method), the classification of such n has not been carried out for any $\alpha \neq \pm 1$. For $\alpha = \pm\ell$, where ℓ is almost any odd prime, it is widely believed that there are no solutions. However, there are counterexamples, such as Lehmer's prime value example [25]

$$\tau(251^2) = -8056166352780240625732174 7. \tag{1.3}$$

Lygeros and Rozier [26] have subsequently discovered further prime values.

We investigate these questions for even weight newforms with integer coefficients and trivial mod 2 residual Galois representation (i.e. even Hecke eigenvalues for $T(p)$ for primes $p \nmid 2N$, where N is the level). We obtain a general theorem (see Theorem 3.2) that theoretically locates those coefficients that are odd prime powers in absolute value for such newforms. For $\tau(n)$, this theorem gives the following criterion, which restricts arguments to explicit finite sets.

Theorem 1.1. *Suppose that ℓ is an odd prime for which $\ell \nmid \tau(\ell)$. If $\tau(n) = \pm\ell^m$, with $m \in \mathbb{Z}^+$, then $n = p^{d-1}$, where p and $d \mid \ell(\ell^2 - 1)$ are odd primes. Furthermore, $\tau(n) = \pm\ell^m$ for at most finitely many n.*

Theorem 1.1 offers a method for determining whether $|\tau(n)| = \ell^m$ has any solutions, which reduces the problem to the determination of certain integer points on finitely many algebraic curves. For $\ell \in \{3, 5, 7\}$, examples of these curves include

$$Y^2 - X^{11} = \pm 3^m, \qquad Y^2 - 5X^{22} = \pm 4 \cdot 5^m \quad \text{and} \quad Y^3 - 5XY^2 + 6X^2Y - X^3 = \pm 7^m. \tag{1.4}$$

By classifying such points when $m = 1$, we obtain the following theorem.[2]

Theorem 1.2. *For every $n > 1$, the following are true.*
(1) We have that

$$\tau(n) \notin \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 13, \pm 17, -19, \pm 23, \pm 37, \pm 691\}.$$

(2) Assuming the Generalized Riemann Hypothesis, we have that

$$\tau(n) \notin \left\{\pm\ell \ : \ 41 \leq \ell \leq 97 \text{ with } \left(\frac{\ell}{5}\right) = -1\right\} \cup \{-11, -29, -31, -41, -59, -61, -71, -79, -89\}.$$

[2]The *Journal of Number Theory* published the proceedings of the conference "Modular forms and Drinfeld Modules" held in 2018 in Pisa, Italy. Paper [6] is an exposition of the third author's lecture at the conference, and pertains to some of the cases of Theorem 1.2 (1). All of the other results in the present paper have not appeared elsewhere. This article is the main reference for the authors' work on variants of Lehmer's speculation.

Remark. *This paper*[3] *has stimulated a number of recent works on variants of Lehmer's speculation. Many authors have made use of its contents and strategy to obtain further results extending and generalizing Theorem 1.2. To be precise, Amir and Hatziiliou* [2]*, Amir and Hong* [3]*, Bennett, Gherga, Patel and Siksek* [10]*, Dembner and Jain* [22]*, Hanada and Madhukara* [23]*, and the authors* [6, 8] *have made use of Theorem 1.1 to obtain explicit extensions and further generalizations of Theorem 1.2. Most notably, Bennett, Gherga, Patel and Siksek (see Theorem 6 of* [10]*) proved the striking fact that* $|\tau(n)| \neq \ell^m$ *for every prime* $3 \leq \ell < 100$ *and every positive integer* m*.*

There are infinite families of newforms with even level for which these methods apply for ordinary primes ℓ (i.e. $\ell \nmid a_f(\ell)$). The next theorem offers unconditional results for $3 \leq \ell \leq 37$, when $2k \in \{4, 6, 8, 10\}$ or $\gcd(3 \cdot 5 \cdot 7, 2k-1) \neq 1$. It also gives further results conditional on the Generalized Riemann Hypothesis (GRH).

Theorem 1.3. *If* $f(z) = q + \sum_{n=2}^{\infty} a_f(n)q^n \in S_{2k}(\Gamma_0(2N)) \cap \mathbb{Z}[[q]]$ *is an even weight* $2k \geq 4$ *newform with trivial mod 2 residual Galois representation, then the following are true for ordinary primes* ℓ*.*

(1) For every $n > 1$ *we have* $a_f(n) \notin \{\pm 1\}$*.*

(2) If $2k = 4$*, then for every* n *we have*

$$a_f(n) \notin \{\pm \ell \ : \ 3 \leq \ell \leq 37 \text{ prime}\} \setminus \{\pm 11, -13, 17, \pm 19, -23, 37\}.$$

Assuming GRH, for every n *we have*

$$a_f(n) \notin \{\pm \ell \ : \ 41 \leq \ell \leq 97 \text{ prime}\} \setminus \{-41, -53, -61, -67, \pm 71, 73, -89\}.$$

(3) If $2k = 6$*, then for every* n *we have*

$$a_f(n) \notin \{\pm \ell \ : \ 3 \leq \ell \leq 37 \text{ prime}\} \setminus \{11, 13\}.$$

Assuming GRH, for every n *we have*

$$a_f(n) \notin \{\pm \ell \ : \ 41 \leq \ell \leq 97 \text{ prime}\} \setminus \{-47\}.$$

(4) If $2k = 8$*, then for every* n *we have*

$$a_f(n) \notin \{\pm \ell \ : \ 3 \leq \ell \leq 37 \text{ prime}\}.$$

Assuming GRH, for every n *we have*

$$a_f(n) \notin \{\pm \ell \ : \ 41 \leq \ell \leq 97 \text{ prime}\} \setminus \{-71\}.$$

(5) If $2k = 10$*, then for every* n *we have*

$$a_f(n) \notin \{\pm \ell \ : \ 3 \leq \ell \leq 37 \text{ prime}\}.$$

Assuming GRH, for every n *we have*

$$a_f(n) \notin \{\pm \ell \ : \ 41 \leq \ell \leq 97 \text{ prime}\} \setminus \{-83\}.$$

[3]This paper was first posted to the arXiv on May 20, 2020.

(6) *If* $\gcd(3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 2k-1) \neq 1$ *and* $2k \geq 12$, *then for every* n *we have*

$$a_f(n) \notin \left\{ \pm \ell \ : \ 3 \leq \ell < 37 \text{ prime with } \left(\frac{\ell}{5}\right) = -1 \right\} \cup \{-37\}.$$

Moreover, if $2k \neq 16$, *then* $a_f(n) \neq 37$. *Assuming GRH, for every* n *we have*

$$a_f(n) \notin \left\{ \pm \ell \ : \ 41 \leq \ell \leq 97 \text{ prime with } \left(\frac{\ell}{5}\right) = -1 \right\}.$$

(7) *If* $\gcd(3 \cdot 5, 2k-1) \neq 1$ *and* $2k \geq 12$, *then for every* n *we have*

$$a_f(n) \notin \left\{ \pm \ell \ : \ 11 \leq \ell \leq 31 \ \text{ prime with } \left(\frac{\ell}{5}\right) = 1 \right\}.$$

Assuming GRH, the range of this set can be expanded to include $\ell \leq 89$.

(8) *If* $7 \mid (2k-1)$ *and* $2k \geq 12$, *then for every* n *we have*

$$a_f(n) \notin \left\{ \pm \ell \ : \ 11 \leq \ell \leq 31 \ \text{ prime with } \left(\frac{\ell}{5}\right) = 1 \right\}.$$

Assuming GRH, for every n *we have*

$$a_f(n) \notin \{\pm 41, \pm 59, \pm 61, -71, \pm 79, \pm 89\}.$$

(9) *If* $11 \mid (2k-1)$, *then for every* n *we have* $a_f(n) \neq -19$, *and assuming GRH we have*

$$a_f(n) \notin \{-11, -29, -31, -41, -59, -61, -71, -79, -89\}.$$

(10) *If* $13 \mid (2k-1)$, *then for every* n *we have* $a_f(n) \neq -11$, *and assuming GRH we have*

$$a_f(n) \notin \{-19, -29, -31, -41, -59, -61, -71, -79\}.$$

Five Remarks.

(i) Theorem 1.3 applies to all newforms [31] with integer coefficients with level $2^a N$, *where* $a \geq 0$ *and* $N \in \{1, 3, 5, 15, 17\}$. *Moreover, the result holds for all odd levels when* $a_f(2)$ *is even.*

(ii) These results follow from Theorem 3.2, which constrains coefficients that are odd prime powers in absolute value. This method extends to arbitrary odd integers by Hecke multiplicativity, thereby giving an algorithm for determining whether a given odd integer is a newform coefficient.

(iii) The proof of Theorem 1.3 (2-6) locates values $\pm\ell$ *that are possible coefficients. For example, Theorem 1.3 (2) allows weight 4 coefficients to be in the set* $\{\pm 11, -13, 17, \pm 19, -23, 37\}$. *The proof shows that these values can only occur as one of the following coefficients:*

$$a_f(3^2) = 37, \quad a_f(3^2) = -11, \quad a_f(3^2) = -23, \quad a_f(3^4) = 19, \quad a_f(5^2) = 19,$$
$$a_f(7^2) = -19, \quad a_f(7^4) = 11, \quad a_f(17^2) = -13, \quad a_f(43^2) = 17.$$

Similarly, Theorem 1.3 (6) allows a coefficient of 37 for weight 16, *which must be* $a_f(3^2) = 37$.

(iv) The assumption that $2k \geq 4$ *guarantees that certain algebraic curves have positive genus, and so have finitely many integer points by Siegel's Theorem. Moreover, we do not believe that conclusions analogous to those obtained in Theorem 1.3 hold for weight 2 newforms.*

(v) Some of the results in Theorem 1.3 rely on the GRH. These cases pertain to situations where GRH was required to reduce the running time of certain computational number theoretic algorithms. The unconditional bounds lead to infeasible computer calculations.

Example. *By Theorem 1.3, the coefficients of the Hecke eigenform $E_4(z)\Delta(z)$ never belong to*

$$\{-1\} \cup \{\pm \ell \ : \ 3 \le \ell \le 37 \text{ prime}\}.$$

Moreover, under GRH the range of the second set can be extended to the odd primes $\ell \le 97$.

Theorems 1.2 and 1.3 offer variants of Lehmer's speculation for individual newforms. It is natural to consider an aspect of these questions where the newforms f vary. Namely, can a fixed odd α be a Fourier coefficient of newforms with arbitrarily large weight? We effectively show that this is generically not the case. To ease notation, if ℓ is an odd prime, then let $\mathbb{S}_\ell$ denote the set of even weight newforms with integer coefficients, trivial residual mod 2 Galois representation, and even level that is coprime to ℓ.

Theorem 1.4. *If $m \in \mathbb{Z}^+$, then there are effectively computable constants $M^{\pm}(\ell, m) = O_\ell(m)$ for which $\pm\ell^m$ is not a coefficient of any $f \in \mathbb{S}_\ell$ with weight $2k > M^{\pm}(\ell, m)$ with ℓ ordinary for f. In particular,[4] for $\ell \in \{3, 5\}$, we have*

$$M^{\pm}(\ell, m) := \begin{cases} 2m + 10^{23}\sqrt{m} & \text{if } \varepsilon = +, m \text{ odd, and } \ell = 3, \\ 2m + 10^{13}\sqrt{m} & \text{if } \varepsilon = +, m \text{ even, and } \ell = 3, \\ 2m + 10^{32}\sqrt{m} & \text{if } \varepsilon = - \text{ and } \ell = 3, \\ 3m + 10^{24}\sqrt{m} & \text{if } \varepsilon = \pm, m \text{ odd, and } \ell = 5, \\ 3m + 10^{13}\sqrt{m} & \text{if } \varepsilon = +, m \text{ even, and } \ell = 5, \\ 3m + 10^{30}\sqrt{m} & \text{if } \varepsilon = -, m \text{ even, and } \ell = 5. \end{cases}$$

Three Remarks.

(i) The condition that the level of f is even is not crucial for the proof of Theorem 1.4. If the level is odd, then the proof implies that $a_f(2n+1) \neq \pm\ell^m$ for all n provided that f has large weight. Furthermore, if $a_f(2)$ is even, then the stronger claim that $\pm\ell^m$ is not a Fourier coefficient holds.

(ii) The condition that the level of f is coprime to ℓ also is not crucial. If ℓ exactly divides the level, then there is at most one counterexample, and it will be a Fourier coefficient of the form $a_f(\ell^r)$ (see Theorem 2.6 (4)). Otherwise, the stronger claim holds.

(iii) Using the methods in this paper, one can obtain a generalization of Theorem 1.4 for all odd α, as well as analogous results for odd weights and forms with real Nebentypus.

These results are related to lower bounds for the number of prime divisors of coefficients of newforms. We obtain a general theorem (see Theorem 2.5) which implies the following lower bound for $\Omega(\tau(n))$, the number of prime divisors (counted with multiplicity) of $\tau(n)$. As usual, we let $\omega(n)$ denote the number of distinct prime divisors of n, and we let $\mathrm{ord}_p(n)$ denote the power of p dividing n.

Theorem 1.5. *If $n > 1$ is divisible by only ordinary primes, then*

$$\Omega(\tau(n)) \ge \sum_{\substack{p \mid n \\ \text{prime}}} (\sigma_0(\mathrm{ord}_p(n) + 1) - 1) \ge \omega(n).$$

Remark. *Theorem 1.5 is sharp, as the prime in (1.3) satisfies $\Omega(\tau(251^2)) = \sigma_0(3) - 1 = 1$.*

[4]We offer these values to indicate that one can easily work out explicit constants.

The proofs of these results make use of a number of important tools. The deep work of Bilu, Hanrot, and Voutier [13] on primitive prime divisors of Lucas sequences forms the primary framework for these results. The theory for Lucas sequences applies to the recursion relations given by Hecke operators in the theory of modular forms. Their work, combined with some combinatorial facts and properties of 2-adic modular Galois representations, leads to Theorems 1.5 and 2.5. Theorems 1.1 and 3.2 follow easily from these results, and they offer an algorithm for locating $\pm\ell^m$, for odd primes ℓ, in Fourier expansions in suitable newforms. Such occurrences correspond to special integer points (if any) on elliptic curves, hyperelliptic curves, and certain Thue equations. In Section 4 we classify the integer points on the six curves in (1.4) when $m = 1$ (among others), using facts about the classical Lucas sequence, the Chabauty–Coleman method, and results on Thue equations. We rely heavily on previous work of Barros [9], Cohn [18], Bugeaud, Mignotte, and Siksek [16]. With some assistance from Ramanujan's congruences for $\tau(n)$, this classification gives Theorem 1.2. In general, this classification leads to the proof of Theorem 1.3. Finally, in the last section we prove Theorem 1.4 on variants of Lehmer's speculation for large weight newforms.

Acknowledgements

The authors thank Malik Amir, Matthew Bisatt, Michael Griffin, Guillaume Hanrot, Vanshika Jain, Sachi Hashimoto, Céline Maistret, Drew Sutherland, and Charlotte Ure for their helpful comments during the preparation of this paper. The authors are particularly grateful to Guillaume Hanrot, who offered assistance with various computer calculations. Finally, we thank the referees for offering further suggestions that improved this paper.

2. Lucas sequences and the proof of Theorem 1.5

We recall work of Bilu, Hanrot, and Voutier [13] on Lucas sequences. Combining their results with facts about newforms gives Theorem 2.5, which in turn implies Theorem 1.5.

2.1. **Lucas sequences and their prime divisors.** Suppose that α and β are algebraic integers for which $\alpha+\beta$ and $\alpha\beta$ are relatively prime non-zero integers, where α/β is not a root of unity. Their *Lucas numbers* $\{u_n(\alpha,\beta)\} = \{u_1 = 1, u_2 = \alpha+\beta, \dots\}$ are the integers

$$u_n(\alpha,\beta) := \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{2.1}$$

A prime $\ell \mid u_n(\alpha,\beta)$ is a *primitive prime divisor of* $u_n(\alpha,\beta)$ if $\ell \nmid (\alpha-\beta)^2 u_1(\alpha,\beta)\cdots u_{n-1}(\alpha,\beta)$. Bilu, Hanrot, and Voutier [13] proved the following definitive theorem.

Theorem 2.1. *Every Lucas number $u_n(\alpha,\beta)$, with $n > 30$, has a primitive prime divisor.*

This theorem is sharp; there are sequences for which $u_{30}(\alpha,\beta)$ does not have a primitive prime divisor. We call a Lucas number $u_n(\alpha,\beta)$, with $n > 2$, *defective*[5] if $u_n(\alpha,\beta)$ does not have a primitive prime divisor. Bilu, Hanrot and Voutier essentially complete the theory; they basically characterized all of the defective Lucas numbers. Their work, combined with a subsequent paper[6] by Abouzaid [1], gives the *complete classification* of defective Lucas numbers. Tables 1-4 in Section 1 of [13] and Theorem 4.1 of [1] offer this classification. Every defective

[5]We do not consider the absence of a primitive prime divisor for $u_2(\alpha,\beta) = \alpha+\beta$ to be a defect.

[6]This paper included a few cases which were omitted in [13].

Lucas number either belongs to a finite list of sporadic examples or a finite list of parameterized infinite families.

We consider Lucas sequences arising from those quadratic integral polynomials

$$F(X) = X^2 - AX + B = (X-\alpha)(X-\beta), \tag{2.2}$$

where $B = \alpha\beta = p^{2k-1}$ is an odd power of a prime p, and $|A| = |\alpha+\beta| \leq 2\sqrt{B} = 2p^{\frac{2k-1}{2}}$. A straightforward analysis of these tables of defective Lucas numbers reveals a list of sporadic examples, and several potentially infinite families of examples. A straightforward case-by-case analysis using elementary congruences, divisibilities, and the truth of Catalan's conjecture [27], that 2^3 and 3^2 are the only consecutive perfect powers, yields the following characterization.

Theorem 2.2. *Tables 1 and 2 in the Appendix list the defective $u_n(\alpha,\beta)$ satisfying (2.2).*

To identify the cases where $|u_n(\alpha,\beta)| = 1$ and $|u_n(\alpha,\beta)| = \ell$ is prime, we require the curves

$$B_{1,k}^{r,\pm} : Y^2 = X^{2k-1} \pm 3^r, \quad \text{and} \quad B_{2,k} : Y^2 = 2X^{2k-1} - 1. \tag{2.3}$$

Lemma 2.1. *Suppose that $u_n(\alpha,\beta)$ is a defective Lucas number from Table 1 or Table 2.*

(1) We have that $|u_n(\alpha,\beta)| = 1$ if and only if

$$(A,B,n) \in \big\{(\pm 1,2,5),(\pm 1,2,13),(\pm 1,3,5),(\pm 1,5,7),(\pm 2,3,3),(\pm 3,2^3,3)\big\},$$

or $(A,B,n) = (\pm m, p, 3)$, where $p = m^2+1$ is prime with $m > 1$.

(2) If $|u_n(\alpha,\beta)| = \ell$ is prime, then $(A,B,\ell,n) \in \big\{(\pm 1,2,7,7),(\pm 1,2,3,8),(\pm 2,11,5,5)\big\}$, or $(A,B,\ell,n) = (\pm m, p^{2k-1}, 3, 3)$, where $(p,\pm m) \in B_{1,k}^{1,\pm}$ and $3 \nmid m$, or $(A,B,\ell,n) = (\pm m, p^{2k-1}, m, 4)$, where $(p,\pm m) \in B_{2,k}$.

Proof. The proof of both (1) and (2) follow by a simple (and tedious) case-by-case analysis. □

In addition to this classification, we recall several vital facts about Lucas numbers (see Section 2 of [13]). It is important to know about their relative divisibility properties.

Proposition 2.3 (Prop. 2.1 (ii) of [13])**.** *If $d \mid n$, then $u_d(\alpha,\beta) | u_n(\alpha,\beta)$.*

To keep track of the first occurrence of prime divisors, we let $m_\ell(\alpha,\beta)$ be the smallest $n \geq 2$ for which $\ell \mid u_n(\alpha,\beta)$. We note that $m_\ell(\alpha,\beta) = 2$ if and only if $\alpha+\beta \equiv 0 \pmod{\ell}$.

Proposition 2.4 (Cor. 2.2[7] of [13])**.** *If $\ell \nmid \alpha\beta$ is an odd prime with $m_\ell(\alpha,\beta) > 2$, then the following are true.*

(1) If $\ell \mid (\alpha-\beta)^2$, then $m_\ell(\alpha,\beta) = \ell$.
(2) If $\ell \nmid (\alpha-\beta)^2$, then $m_\ell(\alpha,\beta) \mid (\ell-1)$ or $m_\ell(\alpha,\beta) \mid (\ell+1)$.

Remark. *If $\ell \mid \alpha\beta$, then either $\ell \mid u_n(\alpha,\beta)$ for all n, or $\ell \nmid u_n(\alpha,\beta)$ for all n.*

[7]This corollary is stated for Lehmer numbers. The conclusions hold for Lucas numbers because $\ell \nmid (\alpha+\beta)$.

2.2. **Prime divisors of newform coefficients.** Throughout this paper we suppose that

$$f(z) = q + \sum_{n=2}^{\infty} a_f(n) q^n \in S_{2k}(\Gamma_0(N)) \cap \mathbb{Z}[[q]] \tag{2.4}$$

is an even weight $2k$ newform. Let S_f be the finite (generally empty) set of primes p for which $(A, B) = (a_f(p), p^{2k-1})$ appears in Tables 1 or 2. For primes $p \notin S_f$ and $m \geq 1$, we let

$$\widehat{\sigma}(p; m) := \sigma_0(m+1) - 1, \tag{2.5}$$

while for $p \in S_f$ we define $\widehat{\sigma}(p; m)$ in Table 3 in the Appendix. We have the following theorem.

Theorem 2.5. *Assume the notation and hypotheses above. If $n > 1$ is only divisble by ordinary primes, then*

$$\Omega(a_f(n)) \geq \sum_{p \mid N} (k-1)\mathrm{ord}_p(n) + \sum_{\substack{p \nmid N \\ \mathrm{ord}_p(n) \geq 2}} \widehat{\sigma}(p; \mathrm{ord}_p(n)).$$

Remark. *Theorem 2.5 does not take into account those primes $p \nmid N$ which exactly divide n because it can happen that $|a_f(p)| = 1$. However, if the mod 2 residual Galois representation is trivial, then $a_f(p)$ is even for every prime $p \nmid 2N$. In such cases, we get*

$$\Omega(a_f(n)) \geq \sum_{p \mid N} (k-1)\mathrm{ord}_p(n) + \sum_{p \nmid 2N} \widehat{\sigma}(p; \mathrm{ord}_p(n)).$$

This applies to $\Delta(z)$, by the congruence $\Delta(z) \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod 2$. Since $(A, B) = (\tau(p), p^{11})$ does not appear in Lemma 2.1 (1), the proof of Theorem 2.5 gives Theorem 1.5.

2.3. **Proof of Theorem 2.5.** We recall some basic facts about *Atkin-Lehner newforms* (see [4, 28]), along with the deep theorem of Deligne [20, 21] that bounds their Fourier coefficients.

Theorem 2.6. *Suppose that $f(z) = q + \sum_{n=2}^{\infty} a_f(n) q^n \in S_{2k}(\Gamma_0(N))$ is a newform with integer coefficients. Then the following are true:*

(1) If $\gcd(n_1, n_2) = 1$, then $a_f(n_1 n_2) = a_f(n_1) a_f(n_2)$.

(2) If $p \nmid N$ is prime and $m \geq 2$, then

$$a_f(p^m) = a_f(p) a_f(p^{m-1}) - p^{2k-1} a_f(p^{m-2}).$$

(3) If $p \nmid N$ is prime and α_p and β_p are roots of $F_p(x) := x^2 - a_f(p)x + p^{2k-1}$, then

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

Moreover, we have $|a_f(p)| \leq 2p^{\frac{2k-1}{2}}$, and α_p and β_p are complex conjugates.

(4) If $p \mid N$ is prime, then $f|U(p) := \sum_{n=1}^{\infty} a_f(np) q^n = a_f(p) f(\tau)$. Moreover, we have

$$a_f(p^m) = \begin{cases} (\pm 1)^m p^{(k-1)m} & \text{if } \mathrm{ord}_p(N) = 1, \\ 0 & \text{if } \mathrm{ord}_p(N) \geq 2. \end{cases}$$

Theorem 2.6 leads to lower bounds for the number of prime divisors (counted with multiplicity) of the coefficients in the sequence $\{a_f(p^2), a_f(p^3), \dots\}$, where p is prime.

Proposition 2.7. *Assuming the notation in Theorem 2.6, the following are true for $m \geq 2$.*

(1) *If $p \mid N$ is prime, then* $\mathrm{ord}_p(a_f(p^m)) \geq (k-1)m$.
(2) *Suppose that $p \nmid N$ is prime. If $(A, B) = (a_f(p), p^{2k-1})$ does not appear in Tables 1 or 2, then*
$$\Omega(a_f(p^m)) \geq \sigma_0(m+1) - 1.$$
(3) *Suppose that $p \nmid N$ is prime. If $(A, B) = (a_f(p), p^{2k-1})$ appears in Tables 1 or 2, then Table 3 of the Appendix contains a lower bound for $\Omega(a_f(p^m))$.*

Proof of Proposition 2.7. The first claim follows from Theorem 2.6 (4). The second claim follows from Theorem 2.6 (3), Proposition 2.3 and Theorem 2.1 in a case-by-case analysis. The point is that at least one new prime divisor is accumulated with each subsequent step in a Lucas sequence. In other words, the relative divisibility of Lucas numbers and the presence of primitive prime divisors guarantees the lower bound. The only divisor of $m+1$ which does not contribute is $u_1 = 1$. The third claim follows similarly by taking into account the defective Lucas numbers that appear in Tables 1 and 2. □

Proof of Theorem 2.5. The theorem follows from Theorem 2.6 (1) and Proposition 2.7. □

3. Variations of Lehmer's Speculation

Regarding coefficients of newforms satisfying (2.4), we classify those n for which $|a_f(n)| = \ell$ is an odd prime. For the remainder of the paper, we assume that all newforms have weight $2k \geq 4$. We first determine when $|a_f(n)| = 1$. Define the set

$$\mathcal{U}_f := \begin{cases} \{1, 4\} & \text{if } a_f(2) = \pm 3,\ 2k = 4, \text{and } N \text{ odd}\}, \\ \{1\} & \text{otherwise.} \end{cases} \tag{3.1}$$

Proposition 3.1. *Suppose that the mod 2 residual Galois representation for $f(z)$ is trivial. Then we have $|a_f(n)| = 1$ if and only if $n \in \mathcal{U}_f$.*

Proof. By multiplicativity (i.e. Theorem 2.6 (1)), it suffices to determine when $|a_f(p^m)| = 1$, where p is prime. By Proposition 2.7 (1), we have $p \nmid N$. By Theorem 2.6 (3), it suffices to determine when the $|u_{m+1}(\alpha_p, \beta_p)| = 1$, where $m \geq 2$. Indeed, $a_f(p) = u_2(\alpha_p, \beta_p)$ is even for $p \nmid 2N$. By Theorem 2.1, this reduces to Lemma 2.1 (1). The defective cases $(A, B, n) = (\pm 3, 2^3, 3)$ correspond to potential weight 4 newforms, while the remaining possibilities are for weight 2. In the weight 4 cases we have $a_f(2) = \pm 3$, which gives $a_f(4) = a_f(2)^2 - 2^3 = 1$. □

Theorem 3.2. *Suppose that the mod 2 residual Galois representation for $f(z)$ is trivial, and that $\ell \nmid a_f(\ell)$. If $|a_f(n)| = \ell^m$, with $m \in \mathbb{Z}^+$ and ℓ is an odd prime, then $n = m_0 p^{d-1}$, where $m_0 \in \mathcal{U}_f$, $p \nmid N$ is prime, and $d \mid \ell(\ell^2 - 1)$ is an odd prime. Moreover, $|a_f(n)| = \ell^m$ for finitely many (if any) n.*

Proof of Theorem 1.1 and 3.2. By Proposition 3.1 and Theorem 2.6 (1) and (4), it suffices to determine when $|a_f(p^{d-1})| = |u_d(\alpha_p, \beta_p)| = \ell$, where $p \nmid N$ is prime. Since $2k \geq 4$, ℓ is odd, and $A = a_f(p)$ is even, Lemma 2.1 (2) leaves the defective possibilities $(A, B, \ell, n) = (\pm m, p^{2k-1}, 3, 3)$, which by Theorem 2.6 (2), implies that $(p, a_f(p))$ is an integer point on $Y^2 = X^{2k-1} \pm 3$. This means that $u_3(\alpha_p, \beta_p) = a_f(p^2) = \pm 3$, which is the claimed conclusion with $d = \ell = 3$.

Now we consider whether a prime power can be a nondefective Lucas number $u_d(\alpha_p, \beta_p) = a_f(p^{d-1})$, for primes $p \nmid 2N$. Since $a_f(p)$ is even, we may assume that $\ell \nmid \alpha_p \beta_p$ and $m_\ell(\alpha_p, \beta_p) > 2$.

Moreover, Theorem 2.6 (2) implies that $a_f(p^b)$ is odd if and only if b is even, and so we may assume that d is odd. Proposition 2.4 implies that $m_\ell(\alpha_p, \beta_p) = \ell$ or $m_\ell(\alpha_p, \beta_p)|(\ell - 1)$ or $m_\ell(\alpha_p, \beta_p)|(\ell + 1)$.

Due to the generic presence of primitive prime divisors, a Lucas number that is a prime power ℓ^m in absolute value is the first multiple of ℓ in the sequence. By Theorem 2.1, Proposition 2.3, and Lemma 2.1 (2), this holds for every sequence satisfying (2.2) for weights $2k \geq 4$. In particular, d is an odd prime. The finiteness of the number of p for which $|a_f(p^{d-1})| = \ell$, follows from Siegel's Theorem, that positive genus curves have at most finitely many integer points. These curves are easily assembled using Theorem 2.6 (2) (see Lemma 5.1). □

4. Integral Points on some curves

To prove Theorems 1.2 and 1.3, we require knowledge of the integer points on certain curves.

4.1. **Some Thue equations.** An equation of the form $F(X, Y) = D$, where $F(X, Y) \in \mathbb{Z}[X, Y]$ is homogeneous and D is a non-zero integer, is known as a *Thue equation*. We require such equations that arise from the generating function

$$\frac{1}{1 - \sqrt{Y}T + XT^2} = \sum_{m=0}^{\infty} F_m(X, Y) \cdot T^m = 1 + \sqrt{Y} \cdot T + (Y - X)T^2 + \cdots . \tag{4.1}$$

The first few homogenous polynomials $F_{2m}(X, Y)$ are as follows:

$$\begin{aligned} F_2(X, Y) &= Y - X, \\ F_4(X, Y) &= Y^2 - 3XY + X^2 \\ F_6(X, Y) &= Y^3 - 5XY^2 + 6X^2Y - X^3. \\ F_{10}(X, Y) &= Y^5 - 9XY^4 + 28X^2Y^3 - 35X^3Y^2 + 15X^4Y - X^5. \end{aligned}$$

For every positive integer m, we consider the degree m Thue equations of the form

$$F_{2m}(X, Y) = \prod_{k=1}^{m} \left(Y - 4X \cos^2 \left(\frac{\pi k}{2m + 1} \right) \right) = D. \tag{4.2}$$

The next lemma gives integer points on several Thue equations that we shall require.

Lemma 4.1. *The following are true.*

(1) Table 4 in the Appendix lists all of the integer solutions to

$$F_{d-1}(X, Y) = \pm\ell$$

for every pair of odd primes (d, ℓ) for which $7 \leq d \mid \ell(\ell^2 - 1)$ and $\ell \in \{7 \leq \ell \leq 37\}$.

(2) Conditional on GRH, Table 5 in the Appendix lists all of the integer solutions to

$$F_{d-1}(X, Y) = \pm\ell$$

for every pair of odd primes (d, ℓ) for which $7 \leq d \mid \ell(\ell^2 - 1)$ and $41 \leq \ell \leq 97$.

(3) There are no integer solutions to $F_{22}(X, Y) = \pm 691$.

(4) The points $(\pm 1, \pm 4)$ are the only integer solutions to $F_{690}(X, Y) = \pm 691$.

Proof. Claims (1), (2) and (3) are easily obtained using the Thue solver in `PARI/GP` [32] (see [7] for all of the code required for this paper).

The proof of (4) is more formidable, as $F_{690}(X,Y)$ has degree 345. However, for odd primes p, the Thue equations $F_{p-1}(X,Y) = \pm p$ are equivalent to the well-studied equations

$$\widehat{F}_p(X,Y) = \prod_{k=1}^{\frac{p-1}{2}} \left(Y - 2X\cos\left(\frac{2\pi k}{p}\right)\right) = \pm p \tag{4.3}$$

that were prominent in the work of Bilu, Hanrot, and Voutier on primitive prime divisors of Lucas sequences. Indeed, we have $F_{p-1}(X,Y) = \widehat{F}_p(X, Y-2X)$. They prove the important fact (see Cor. 6.6 of [13]) that there are no integer solutions to (4.3) with $|X| > e^8$ when $31 \leq p \leq 787$. By a well-known criterion (for example, see Lemma 1.1 of [38] and Proposition 2.2.1 of [12])), midsize solutions of $\widehat{F}_{691}(X,Y) = \pm 691$ correspond to convergents of the continued fraction expansion of some $2\cos(2\pi k/691)$. A short calculation rules this out, possibly leaving some small solutions, those with $|X| \leq 4$. For these X, we find $(\pm 1, \pm 2)$, which implies that $(\pm 1, \pm 4)$ are the only integral solutions to $F_{690}(X,Y) = \pm 691$. □

4.2. **The elliptic and hyperelliptic curves $Y^2 = X^{2d-1} \pm \ell$.** For $d \in \{2,3,4,6,7\}$ and odd primes $\ell \leq 97$, we list all of the integer points on

$$C^{\pm}_{d,\ell} : Y^2 = X^{2d-1} \pm \ell. \tag{4.4}$$

Lemma 4.2. *If $3 \leq \ell \leq 97$ is prime and $d \in \{2,3,4,6,7\}$, then the following are true:*

(1) Table 6 in the Appendix lists the integer points on $C^{+}_{d,\ell}$.
(2) Table 7 in the Appendix lists the integer points on $C^{-}_{d,\ell}$.

Proof. Work by Barros [9], Cohn [18] and Bugeaud, Mignotte and Siksek [16] establish these claims. Table 6 is assembled from the Appendix of [9], and Table 7 is assembled from the Appendix of [16]. □

4.3. **The hyperelliptic curves $Y^2 = 5X^{2d} \pm 4\ell$.** For $d \geq 2$, we define the hyperelliptic curves

$$H^{\pm}_{d,\ell} : Y^2 = 5X^{2d} \pm 4\ell. \tag{4.5}$$

The following satisfying lemma classifies the integer points on $H^{\pm}_{d,5}$.

Lemma 4.3. *If $\ell = 5$, then the following are true.*

(1) If $d = 2$ and $\ell = 5$, then the only integer points on $H^{+}_{2,5}$ are $(\pm 1, \pm 5)$ and $(\pm 2, \pm 10)$.
(2) If $d > 2$, then the only integer points on $H^{+}_{d,5}$ are $(\pm 1, \pm 5)$.
(3) If $d \geq 2$, then $H^{-}_{d,5}$ has no integer points.

Proof. We recall the classical Lucas sequence

$$\{L_n\} = \{2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, \dots\},$$

defined by $L_0 := 2$ and $L_1 := 1$ and the recurrence $L_{n+2} := L_{n+1} + L_n$ for $n \geq 0$. A theorem of Bugeaud, Mignotte, and Siksek [15] asserts that $L_1 = 1$ and $L_3 = 4$ are the only perfect power Lucas numbers. By the theory of Pell's equations, the positive integer X-coordinate solutions to $H^{+}_{1,5}$ and $H^{-}_{1,5}$, namely $\{L_1 = 1, L_3 = 4, L_5 = 11, \dots\}$ and $\{L_0 = 2, L_2 = 3, L_4 = 7, \dots\}$ respectively, split the Lucas numbers. The three claims follow immediately. □

For primes $\ell \in \{691\} \cup \left\{11 \leq \ell \leq 89 \ : \ \text{prime with } \left(\frac{\ell}{5}\right) = 1\right\}$, we have the following lemma.

Lemma 4.4. *The following are true.*

(1) For most[8] $d \in \{3, 5, 7, 11, 13\}$ *and primes* $\ell \in \left\{11 \leq \ell \leq 89 \ : \ \left(\frac{\ell}{5}\right) = 1\right\}$, *Table 8 in the Appendix lists (some cases conditional on GRH) the integer points on* $H^{\pm}_{d,\ell}$.

(2) There are no integer points on $C^{-}_{6,691}$.

(3) There are no integer points on $H^{-}_{11,691}$.

Proof. Generalized Lebesgue–Ramanujan–Nagell equations are equations of the form

$$x^2 + D = Cy^n, \tag{4.6}$$

where D and C are non-zero integers. An integer point on (4.6) can be studied in the ring of integers of $\mathbb{Q}(\sqrt{-D})$ using the factorization

$$(x + \sqrt{-D})(x - \sqrt{-D}) = Cy^n.$$

This observation is a standard tool in the study of Thue equations. In particular, Theorem 2.1 of [9] (also see Proposition 3.1 of [16]) gives a step-by-step algorithm that takes alleged solutions of (4.6) and produces integer points on one of finitely many Thue equations constructed from C, D and n via the algebraic number theory of $\mathbb{Q}(\sqrt{-D})$. These equations are assembled from the knowledge of the group of units and the ideal class group.

To prove all three parts of the lemma (apart from $H^{+}_{7,89}$), we implemented this algorithm in `SageMath` (see [7] for all `SageMath` code required for this paper). Some cases required GRH as a simplifying assumption. As the curves in (2) and (3) are the most complicated, we offer brief details in these two cases.

To prove (2), we consider the hyperelliptic curve $C^{-}_{6,691}$, which corresponds to (4.6) for the class number 5 imaginary quadratic field $\mathbb{Q}(\sqrt{-691})$, where $x = Y, y = X, C = 1, D = 691$, and $n = 11$. In this case the algorithm gives exactly one Thue equation, which after clearing denominators can be rewritten as

$$\begin{aligned}
2 \times 5^{55} = {} & (99107717427209 0396)x^{11} + (11970001843922078 9119)x^{10}y - (88315992210028361 72345)x^9y^2 \\
& - (33711634551278645628 0840)x^8y^3 + (84929673003753710343324 30)x^7y^4 \\
& + (17518931198691927887050 4298)x^6y^5 - (18818073681639955856448 10248)x^5y^6 \\
& - (22992541672786450593030038430)x^4y^7 + (10477254155373935910225 3613965)x^3y^8 \\
& + (69787579874992244513311 7312720)x^2y^9 - (10688014861698094526193 68218519)xy^{10} \\
& - (22923003748106478231113842 94421)y^{11}.
\end{aligned}$$

The Thue equation solver in `PARI/GP`, which implements the Bilu–Hanrot algorithm, establishes that there are no integer solutions, and so $C^{-}_{6,691}$ has no integer points.

Claim (3) is about the hyperelliptic curve $H^{-}_{11,691}$. Its integer points (X, Y) satisfy

$$(Y + 2\sqrt{-691})(Y - 2\sqrt{-691}) = 5X^{22}.$$

Therefore, we again employ the imaginary quadratic field $\mathbb{Q}(\sqrt{-691})$. In particular, we have (4.6), where $x = Y, y = X, C = 5, D = 4 \cdot 691$ and $n = 22$. The algorithm again gives one Thue equation, which after clearing denominators can be rewritten as

[8] We were unable to obtain results for $H^{+}_{7,71}$, $H^{-}_{13,89}$, and any $H^{+}_{11,\ell}$ and $H^{+}_{13,\ell}$.

$$\begin{aligned}2^2 \times 5^{110} = &-(20587212586465949627980680671826599752)x^{22}\\ &+(1133274396835827658613802749227310922394)x^{21}y\\ &+\cdots\\ &-(796704231451073017727793993797359763099072645117180347892768 56)xy^{21}\\ &+(7180943720813843126278354962524861735173119932332611543932427 3)y^{22}.\end{aligned}$$

The Thue solver in `PARI/GP` establishes that there are no integer solutions, and so $H^-_{11,691}$ has no integer points. □

We use the Chabauty–Coleman method[9], which employs p-adic integration to determine the rational points on suitable curves of genus $g \geq 2$, to determine the integer points on $C^+_{6,691}$, $H^+_{7,89}$, and $H^+_{11,691}$.

Lemma 4.5. *The following are true.*

(1) There are no integer points on $C^+_{6,691}$.
(2) There are no integer points on $H^+_{11,691}$.
(3) Assuming GRH, the only integer points on $H^+_{7,89}$ have $(|X|, |Y|) = (1, 19)$.

Proof. We employ the Chabauty–Coleman method [19] to determine the integral points on these curves.

We first prove (1). The genus 5 curve $C^+_{6,691}$ has Jacobian with Mordell-Weil rank 0. This can be determined using the implementation of 2-descent in `Magma` [14]. Since the rank is less than the genus, the Chabauty–Coleman method applies, which, in this case, gives a 5-dimensional space of regular 1-forms vanishing on rational points. We take as our basis for the space of annihilating differentials the set $\{\omega_i := X^i \frac{dX}{2Y}\}_{i=0,1,\ldots,4}$. The prime $p = 3$ is a prime of good reduction for $C^+_{6,691}$, and taking the point at infinity ∞ as our basepoint, we compute the set of points

$$\left\{ z \in C^+_{6,691}(\mathbb{Z}_3) : \int_\infty^z \omega_i = 0 \text{ for all } i = 0, 1, \ldots, 4 \right\},$$

where the integrals are Coleman integrals computed using `SageMath` [34]. By construction, this set contains the integral points on the working affine model of $C^+_{6,691}$.

The computation gives three points: two points with X-coordinate 0 and a third point with Y-coordinate 0 in the residue disk corresponding to $(2, 0) \in C^+_{6,691}(\mathbb{F}_3)$. (Indeed, the power series corresponding to the expansion of the integral of ω_0 has each of these points occurring as simple zeros.) Hence, there are no integral points on $C^+_{6,691}$.

Turning to $H^+_{11,691}$, we consider the integral points on the curve $Y^2 = 5X^{11} + 4 \cdot 691$ and then pull back any points found using the map $(X, Y) \to (X^2, Y)$. Using `Magma`, we find that the rank of the Jacobian of this genus 5 curve is 0. We rescale variables to work with the monic model $Y^2 = X^{11} + 4 \cdot 5^{10} \cdot 691$ and we apply the Chabauty–Coleman method using $p = 3$. As before, the computation gives three points with coordinates in $\mathbb{Z}_3$: two points with X-coordinate 0 and a third point with Y-coordinate 0 in the residue disk corresponding to $(2, 0)$. The power series

[9]We could have (in theory) used the Thue method as in the proof of Lemma 4.4. We chose this method as it did not require substantial computer resources.

corresponding to the expansion of the integral of ω_0 has each of these points occurring as simple zeros. None of these points are rational. Therefore, $H^+_{11,691}$ has no integral points. This proves (2).

Now we turn to (3). To compute integral points on $H^+_{7,89}$, we work with the genus 3 curve $Y^2 = 5X^7 + 4 \cdot 89$ and then pull back any integral points found using the map $(X, Y) \to (X^2, Y)$. Using `Magma`, we find that the rank of the Jacobian of this genus 3 curve is 2, under the assumption of GRH[10]. We work with the monic model

$$H_m : Y^2 = X^7 + 4 \cdot 5^6 \cdot 89$$

and run the Chabauty–Coleman method using $p = 3$.

The points

$$P = [x^3 + 14x^2 - 800, 9x^2 + 200x - 4050] \qquad \text{and} \qquad Q = [x - 5, 19 \cdot 5^3]$$

(given in Mumford representation) are independent in the Jacobian of H_m. To simplify the Chabauty–Coleman computation—in particular, so that we carry out all of our computations over $\mathbb{Q}_3$—we replace P with P', a small $\mathbb{Z}$-linear combination of P and Q that is linearly independent from Q, with the property that the first coordinate of the Mumford representation of P' splits over $\mathbb{Q}_3$.

We take $P' := 2P - 5Q$, with Mumford representation of P' given by $[f(x), g(x)]$ where

$$f(x) = x^3 - \frac{57819608106819190393450758001494220029312032281}{24343262587220695977334792112937389448514980 9}x^2 + \frac{30102205702297838355306742898539370800418880 3800}{81144208624068986591115973709791298161716603}x - \frac{49352442278032156366349264656570112208461467631 00}{24343262587220695977334792112937389448514980 9},$$

$$g(x) = \frac{13467788979408324218581419111573847035681150845619031139253274307312471}{37981155721946187641366914767773231499005562696462193735136892103 77}x^2 - \frac{73837091689655128840131596065726589815272462202819205672839132728899500}{12660385240648729213788971589257743833001854232154064578378964034 59}x + \frac{12499832471053603339430709386527094765975931482170643513178700161693548 50}{37981155721946187641366914767773231499005562696462193735136892103 77}.$$

To compute an annihilating differential, we compute the 3×2 matrix of Coleman integrals $(\int_{P'} \omega_i, \int_Q \omega_i)_{i=0,1,2}$, where $\omega_i = X^i \frac{dX}{2Y}$, in `Sage`:

$$\begin{pmatrix} 2 \cdot 3 + 2 \cdot 3^2 + 3^4 + 2 \cdot 3^6 + 3^8 + 2 \cdot 3^9 + O(3^{10}) & 3^3 + 2 \cdot 3^4 + 3^7 + 2 \cdot 3^8 + 3^9 + O(3^{10}) \\ 2 \cdot 3 + 3^2 + 3^3 + 2 \cdot 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 + O(3^{10}) & 2 \cdot 3 + 3^2 + 3^3 + 2 \cdot 3^7 + 2 \cdot 3^8 + 3^9 + O(3^{10}) \\ 3 + 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^5 + 3^6 + 3^7 + 2 \cdot 3^9 + O(3^{10}) & 2 \cdot 3 + 3^2 + 3^3 + 2 \cdot 3^4 + 3^5 + 3^7 + 2 \cdot 3^8 + 2 \cdot 3^9 + O(3^{10}) \end{pmatrix}.$$

We then compute a basis of the kernel of this matrix, which gives us our annihilating differential

$$\omega = \omega_0 + (1 + 2 \cdot 3^2 + 2 \cdot 3^4 + 3^5 + 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + 2 \cdot 3^9 + O(3^{10}))\omega_1 + (2 + 2 \cdot 3 + 3^2 + 3^3 + 2 \cdot 3^4 + 3^5 + 2 \cdot 3^6 + 3^9 + O(3^{10}))\omega_2.$$

Finally, we have three residue disks to consider, corresponding to $(1, 0)$ and $(2, \pm 1) \in H_m(\mathbb{F}_3)$. We compute the set of points $z \in H_m(\mathbb{Z}_3)$ in these residue disks such that $\int_\infty^z \omega = 0$. This produces three points, each occurring as simple zeros of the corresponding 3-adic power series: a Weierstrass point and the points $(5, \pm 2375)$. The Weierstrass point is not rational, while the points $(5, \pm 2375)$ correspond to the points $(\pm 1, \pm 19)$ on $H^+_{7,89}$. □

[10]The `Magma` procedure that computes ranks requires GRH in this case to be computationally feasible.

5. Proofs of Theorems 1.2 and 1.3

We combine results from the previous section with Theorem 3.2 to prove Theorems 1.2 and 1.3. The following lemma, which relates Fourier coefficients to special integer points on algebraic curves, is a straightforward consequence of Theorem 2.6 (2) and (3).

Lemma 5.1. *Assuming the notation in Theorem 2.6, if $p \nmid N$ is prime, then we have the following:*

(1) If $a_f(p^2) = \alpha$, then $(p, a_f(p))$ is an integer point on

$$Y^2 = X^{2k-1} + \alpha.$$

(2) If $a_f(p^4) = \alpha$, then $(p, 2a_f(p)^2 - 3p^{2k-1})$ is an integer point on

$$Y^2 = 5X^{2(2k-1)} + 4\alpha.$$

(3) For every positive integer m we have that $F_{2m}(p^{2k-1}, a_f(p)^2) = a_f(p^{2m})$.

Proof of Theorem 1.2. It is well-known that $\tau(n)$ is odd if and only if n is an odd square. To see this, we employ the Jacobi Triple Product identity to obtain the congruence

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

We consider the possibility that ± 1 appear in sequences of the form

$$\{\tau(p), \tau(p^2), \tau(p^3), \dots\}. \tag{5.1}$$

By Theorem 2.6 (2), if p is prime and $p \mid \tau(p)$, then $p^m \mid \tau(p^m)$ for every $m \geq 1$, and so $|\tau(p^m)| \neq 1$. Moreover, $|\tau(p)| \neq p$, where p is an odd prime, because $\tau(p)$ is even. Therefore, such sequences may be completely ignored for the remainder of the proof.

For primes $p \nmid \tau(p)$, Theorem 2.6 (3) gives a Lucas sequence with $A = \tau(p)$ and $B = p^{11}$. Lemma 2.1 shows that there are no defective terms with $u_{m+1}(\alpha_p, \beta_p) = \tau(p^m) \neq \pm 1$ or $\pm\ell$, where ℓ is an odd prime. To see this, we note that $A = \tau(p)$ is even. Lemma 2.1 (2) does not allow for A to be even with one exception, the possibility that $(A, B, \ell, n) = (\pm m, p^{11}, 3, 3)$, where $(p, \pm m) \in B_{1,6}^{1,\pm}$. However, these curves are the same as $C_{6,3}^{\pm}$, and Lemma 4.2 shows that there are no such points. Therefore, we may assume that all of the values in (5.1) have a primitive prime divisor, and never have absolute value 1.

We now turn to the primality of absolute values of $\tau(n)$. Thanks to Hecke multiplicativity (i.e. Theorem 2.6 (1)) and the discussion above, if ℓ is an odd prime and $|\tau(n)| = \ell$, then $n = p^d$, where p is an odd prime for which $p \nmid \tau(p)$. The fact that $\tau(p^d) = u_{d+1}(\alpha_p, \beta_p)$ leads to a further constraint on d (i.e. refining the fact that d is even). By Proposition 2.3, which guarantees relative divisibility between Lucas numbers, and Lemma 2.2, which guarantees the absence of defective terms in (5.1), it follows that $d+1$ must be an odd prime, and $\tau(p^d)$ is the very first term that is divisble by ℓ.

To make use of this observation, for odd primes p and ℓ we define

$$m_\ell(p) := \min\{n \geq 1 \ : \ \tau(p^n) \equiv 0 \pmod \ell\}. \tag{5.2}$$

For $|\tau(p^d)| = \ell$, we have $m_\ell(p) = d$, where $d+1$ is also an odd prime. The Ramanujan congruences [11, 33, 35]

$$\tau(n) \equiv \begin{cases} n^2\sigma_1(n) \pmod 9, \\ n\sigma_1(n) \pmod 5, \\ n\sigma_3(n) \pmod 7, \\ \sigma_{11}(n) \pmod{691}, \end{cases}$$

where $\sigma_\nu(n) := \sum_{1\le d|n} d^\nu$, make it simple to compute $m_\ell(p)$ for the primes $\ell \in \{3, 5, 7, 691\}$.

Thanks to the mod 9 congruence, we find that

$$m_3(p) = \begin{cases} 1 & \text{if } p \equiv 0, 2 \pmod 3, \\ 2 & \text{if } p \equiv 1 \pmod 3. \end{cases}$$

Therefore, $d = 2$ is the only possibility. If $\tau(p^2) = \pm 3$, then Lemma 5.1 (1) implies that $(p, \tau(p))$ is a point on $C^{\pm}_{6,3}$, which were considered immediately above. Again, Lemma 4.2 (1) implies that there are no such integer points.

Thanks to the mod 5 congruence, we find that

$$m_5(p) = \begin{cases} 1 & \text{if } p \equiv 0, 4 \pmod 5, \\ 3 & \text{if } p \equiv 2, 3 \pmod 5, \\ 4 & \text{if } p \equiv 1 \pmod 5. \end{cases}$$

Therefore, $d = 4$ is the only possibility. If $\tau(p^4) = \pm 5$, then Lemma 5.1 (2) implies that $(p, 2\tau(p)^2 - 3p^{11})$ is an integer point on $H^{\pm}_{11,5}$. Lemma 4.3 shows that no such points exist on these hyperelliptic curves.

Thanks to the mod 7 congruence, we find that

$$m_7(p) = \begin{cases} 1 & \text{if } p \equiv 0, 3, 5, 6 \pmod 7, \\ 6 & \text{if } p \equiv 1, 2, 4 \pmod 7. \end{cases}$$

Hence, $d = 6$ is the only possibility, and so we must rule out the possibility that $\tau(p^6) = \pm 7$. If there are such primes p, then Lemma 5.1 (3) implies that $F_6(p^{11}, \tau(p)^2) = \pm 7$. Lemma 4.1 (1) shows that there are no such solutions to $F_6(X, Y) = \pm 7$.

Thanks to the mod 691 congruence, we find that the only cases where $m_{691}(p) = d$ where $d+1$ is an odd prime are $d = 2, 4, 22$, and 690. For the cases where $d = 2$ and 4 respectively, Lemma 5.1 (1-2) implies that $(p, \tau(p))$ would be an integral point on $C^{\pm}_{6,691}$, and that $(p, 2\tau(p)^2 - 3p^{11})$ would be an integral point on $H^{\pm}_{11,691}$. Lemma 4.4 (2-3) and Lemma 4.5 show that no such points exist. By Lemma 5.1 (3), the remaining cases (i.e. $d = 22$ and 690) correspond to the Thue equations $F_{22}(p^{11}, \tau(p)^2) = \pm 691$ and $F_{690}(p^{11}, \tau(p)^2) = \pm 691$. Lemma 4.1 (3) and (4) show that there are no such integer solutions.

The arguments above show that $\tau(n) \notin \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 691\}$. The remaining cases are special cases of Theorem 1.3 (6) and (9) and are proved below. □

Proof of Theorem 1.3. By hypothesis, for primes $p \nmid 2N$ we have that $a_f(p)$ is even. For such primes, Theorem 2.6 (2) implies that $a_f(p^m)$ is odd if and only if m is even. Suppose that p is a prime for which $p \mid a_f(p)$, which includes those primes $p \mid 2N$ by Theorem 2.6 (4). Theorem 2.6

(2) and (4) imply that $p^m \mid a_f(p^m)$. Therefore, we do not need to consider these coefficients in the remainder of the proof.

It suffices to consider the Lucas sequences corresponding to $A = a_f(p)$ and $B = p^{2k-1}$, when $p \nmid a_f(p)$. By applying Lemma 2.1 (2) (as above in the proof of Theorem 1.2), we may assume that $\{1, a_f(p), a_f(p^2), \dots\}$ is a Lucas sequence without any defective terms. To establish this, we must show that $B_{1,k}^{1,\pm}$, which are the same as $C_{k,3}^{\pm}$, have no suitable integer points. Since we only consider weights for which $\gcd(3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 2k-1) \neq 1$, it suffices to show that $C_{d,3}^{\pm}$ has no such points for $d \in \{2, 3, 4, 6, 7\}$. Lemma 4.2 confirms this requirement for these ten curves.

The first claim of the theorem now follows from Proposition 3.1. To prove the remaining claims we apply Theorem 3.2. Namely, if $|a_f(n)| = \ell$, then $n = p^{d-1}$, where $d \mid \ell(\ell^2 - 1)$ is an odd prime. The existence of such coefficients can be ruled out with Lemma 5.1, which reduces the proof to a case-by-case search for suitable integral points on hyperelliptic curves and solutions to Thue equations which were considered in the previous section. If $a_f(p^2) = \pm\ell$, then $(p, a_f(p)) \in C_{k,\ell}^{\pm}$. If $a_f(p^4) = \pm\ell$, then $(p, 2_f(p)^2 - 3p^{2k-1}) \in H_{2k-1,\ell}^{\pm}$. Obviously, it suffices to study curves $C_{d,\ell}^{\pm}$ (resp. $H_{2d-1,\ell}^{\pm}$) with $d \mid (2k-1)$. Finally, if $a_f(p^{d-1}) = \pm\ell$ with $d \geq 7$, then $(p^{2k-1}, a_f(p)^2)$ is a solution to $F_{d-1}(X, Y) = \pm\ell$. By Lemmas 4.1, 4.2, 4.3, and 4.4 (i.e. inspecting the tables in the Appendix), there are no such integral points (sometimes under GRH) in the cases claimed by the theorem. □

6. Lehmer's speculation for large weight newforms

We conclude this paper with the proof of Theorem 1.4. To prove this result, we make use of Theorem 3.2, which in turn reduces the problem to a search for integer points on suitable curves by Lemma 5.1. Namely, we show, for each ℓ^m, that the finitely many Diophantine conditions have no integer solutions when the newform weights are (effectively) sufficiently large. To derive these conclusions, we employ a deep theorem of Baker and Wüstholz [5] in the theory of linear forms in logarithms, and work of Tzanakis and de Weger [38] on Thue equations.

6.1. **Some Diophantine equations.**

Here we prove some Diophantine results concerning families of Lebesgue–Ramanujan–Nagell type equations which are of independent interest. To make them precise, for $\ell \in \{3, 5\}, \varepsilon \in \{\pm\}$, and $m \in \mathbb{Z}^+$, we define

$$T^{\varepsilon}(\ell, m) := \begin{cases} 2m + 10^{32}\sqrt{m} & \text{if } \varepsilon = + \text{ and } \ell = 3, \\ 2m + 10^{23}\sqrt{m} & \text{if } \varepsilon = -, m \text{ odd, and } \ell = 3, \\ 2m + 10^{13}\sqrt{m} & \text{if } \varepsilon = -, m \text{ even, and } \ell = 3, \\ 3m + 10^{24}\sqrt{m} & \text{if } \varepsilon = \pm, m \text{ odd, and } \ell = 5, \\ 3m + 10^{30}\sqrt{m} & \text{if } \varepsilon = +, m \text{ even, and } \ell = 5, \\ 3m + 10^{13}\sqrt{m} & \text{if } \varepsilon = -, m \text{ even, and } \ell = 5. \end{cases} \tag{6.1}$$

Furthermore, we define $U^{\varepsilon}(m)$ by

$$U^{\varepsilon}(m) := \begin{cases} 3m + 10^{24}\sqrt{m} & \text{if } \varepsilon = \pm \text{ and } m \text{ odd}, \\ 3m + 10^{30}\sqrt{m} & \text{if } \varepsilon = + \text{ and } m \text{ even}, \\ 3m + 10^{13}\sqrt{m} & \text{if } \varepsilon = - \text{ and } m \text{ even}. \end{cases} \tag{6.2}$$

Theorem 6.1. *If $\ell \in \{3,5\}$, $\varepsilon \in \{\pm\}$, and $m \in \mathbb{Z}^+$, then the following are true.*
(1) If $n > T^{\varepsilon}(\ell, m) = O_\ell(m)$, then there are no integer points[11] (X, Y), with $Y \notin \{0, \pm 1\}$, on

$$X^2 + \varepsilon \ell^m = Y^n. \tag{6.3}$$

(2) If $n > U^{\varepsilon}(m) = O_\ell(m)$, then there are no integer points (X, Y), with $Y \neq 0$, on

$$X^2 + \varepsilon 4 \cdot 5^m = Y^n. \tag{6.4}$$

6.2. **A theorem of Baker and Wüstholz.** To prove Theorem 6.1, we make use of the following classical result of Baker and Wüstholz [5] on linear forms in logarithms.

Theorem 6.2 (p. 20 of [5])**.** *Let $\alpha_1, \dots, \alpha_r$ be algebraic numbers and $b_1, \dots, b_r$ be rational integers. If $\Lambda := b_1 \log \alpha_1 + \cdots + b_r \log \alpha_r$ (note. where the logarithms have their principal values such that $-\pi < \mathrm{Im}(\log \alpha) \leq \pi$) is nonzero, then we have*

$$\log |\Lambda| > -C(r,d) \log(\max\{e, B\}) \prod_{i=1}^{r} h'(\alpha_i),$$

where $d := [\mathbb{Q}(\alpha_1, \dots, \alpha_r) : \mathbb{Q}]$, $B := \max\{|b_1|, \dots, |b_r|\}$,

$$C(r,d) := 18(r+1)!\ r^{r+1}(32d)^{r+2} \log(2rd),$$

and $h'(\alpha) := \max\{h(\alpha)/d, |\log \alpha|/d, 1/d\}$, where $h(\alpha)$ is the logarithmic Weil height of α.

This deep theorem can be applied to the Diophantine equations in (6.3) and (6.4). We shall now assume that n is fixed for the remainder of this discussion. Namely, we view potential integer points as factorizations, in the ring of integers of the quadratic fields $K = \mathbb{Q}(\sqrt{-\varepsilon \ell^m})$, given by

$$(X + \sqrt{-\varepsilon \ell^m})(X - \sqrt{-\varepsilon \ell^m}) = Y^n \quad \text{and} \quad (X + 2\sqrt{-\varepsilon \ell^m})(X - 2\sqrt{-\varepsilon \ell^m}) = Y^n.$$

Namely, if $[K : \mathbb{Q}] = 2$ and $h_K = 1$, then we have $\beta \in \mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\beta) = Y$ and

$$(X + \sqrt{-\varepsilon \ell^m}) = \beta^n \pmod{\mathcal{O}_K^\times} \quad \text{and} \quad (X + 2\sqrt{-\varepsilon \ell^m}) = \beta^n \pmod{\mathcal{O}_K^\times}.$$

If K does not have class number one, then we may pick $\beta \in \mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\beta) = Y^{h_K}$ and consider β^{n/h_K} instead. This only applies when $\varepsilon = 1, \ell = 5$ and m is odd, in which case $h_{\mathbb{Q}(\sqrt{-5})} = 2$. In these cases we let $\overline{\beta}$ denote the Galois conjugate of β. Finally, if $K = \mathbb{Q}$, then we may pick $\beta, \overline{\beta} \in \mathbb{Z}$ (abusing notation) such that $\beta\overline{\beta} = Y$ and $|\beta| \leq \sqrt{|Y|}$. In each case, the algebraic integer β is uniquely determined up to unit.

Given such a β, we construct a corresponding linear form in logarithms arising from $\beta/\overline{\beta}$. For convenience, we denote the relevant fundamental units by $w_3 := 2 + \sqrt{3}$ and $w_5 := 1/2 + \sqrt{5}/2$, and we denote the 6th root of unity by $w_{-3} := 1/2 + \sqrt{-3}/2$. By taking logarithms, we obtain a triple of integers $0 \leq j_4 \leq 3, 0 \leq j_6 \leq 5$, and $0 \leq j_n < n - 1$, for which one of the corresponding

[11] We switch X and Y here to be consistent with the literature on Lebesgue–Ramanujan–Nagell equations.

forms (depending on ε, ℓ and the parity of m), say $\Lambda_{T^\varepsilon(\ell,m)}$ and $\Lambda_{U^\varepsilon(m)}$, is given by

$$\Lambda_{T^\varepsilon(\ell,m)} := \begin{cases} j_6 \log(\overline{w}_{-3}/w_{-3}) - n\log(\overline{\beta}/\beta) + ki\pi & \text{if } \varepsilon = +, m \text{ odd, and } \ell = 3, \\ j_4 \log(\overline{i}/i) - n\log(\overline{\beta}/\beta) + ki\pi & \text{if } \varepsilon = +, m \text{ even, and } \ell = 3, \\ -(n/2)\log(\overline{\beta}/\beta) + ki\pi & \text{if } \varepsilon = +, m \text{ odd, and } \ell = 5, \\ j_4 \log(\overline{i}/i) - n\log(\overline{\beta}/\beta) + ki\pi & \text{if } \varepsilon = +, m \text{ even, and } \ell = 5, \\ j_n \log(\overline{w}_3/w_3) - n\log(\overline{\beta}/\beta) & \text{if } \varepsilon = -, m \text{ odd, and } \ell = 3, \\ -n\log(\overline{\beta}/\beta) & \text{if } \varepsilon = -, m \text{ even, and } \ell = 3, \\ j_n \log(\overline{w}_5/w_5) - n\log(\overline{\beta}/\beta) & \text{if } \varepsilon = -, m \text{ odd, and } \ell = 5, \\ -n\log(\overline{\beta}/\beta) & \text{if } \varepsilon = -, m \text{ even, and } \ell = 5, \end{cases} \tag{6.5}$$

and

$$\Lambda_{U^\varepsilon(m)} := \begin{cases} -(n/2)\log(\overline{\beta}/\beta) + ki\pi & \text{if } \varepsilon = + \text{ and } m \text{ odd}, \\ j_4 \log(\overline{i}/i) - n\log(\overline{\beta}/\beta) + ki\pi & \text{if } \varepsilon = + \text{ and } m \text{ even}, \\ j_n \log(\overline{w}_5/w_5) - n\log(\overline{\beta}/\beta) & \text{if } \varepsilon = - \text{ and } m \text{ odd}, \\ -n\log(\overline{\beta}/\beta) & \text{if } \varepsilon = - \text{ and } m \text{ even}, \end{cases} \tag{6.6}$$

where $k \in \mathbb{Z}$ with $|\Lambda_{T^+(\ell,m)}|,\ |\Lambda_{U^+(m)}| < \pi$. The next lemma bounds these quantities.

Lemma 6.1. *Assuming the notation and hypotheses above, the following are true.*
(1) If $n > 2\log(4\sqrt{\ell^m})/\log|Y|$ and (X,Y) is an integer point on (6.3), with $Y \notin \{0, \pm 1\}$, then

$$|\Lambda_{T^\varepsilon(\ell,m)}| \le 2.78 \cdot \frac{\sqrt{\ell^m}}{|Y|^{\frac{n}{2}}}.$$

(2) If $n > 2\log(8\sqrt{5^m})/\log|Y|$, and (X,Y) is an integer point on (6.4), with $Y \neq 0$, then

$$|\Lambda_{U^\varepsilon(m)}| \le 5.56 \cdot \frac{\sqrt{5^m}}{|Y|^{\frac{n}{2}}}.$$

Proof. By the definition of $\Lambda_{T^\varepsilon(\ell,m)}$, we directly find that

$$|e^{\Lambda_{T^\varepsilon(\ell,m)}} - 1| = \left| \frac{X + \sqrt{\pm\ell^m}}{X - \sqrt{\pm\ell^m}} - 1 \right| \le \frac{2\sqrt{\ell^m}}{|Y|^{\frac{n}{2}}}. \tag{6.7}$$

For $|z| < 1/2$, we note that $|\log(1+z)| \le 1.39 \cdot |z|$. Also, we note that the hypothesis on n gives $|e^{\Lambda_{T^\varepsilon(\ell,m)}} - 1| < 1/2$. Hence, we obtain (1), the claimed inequality

$$|\Lambda_{T^\varepsilon(\ell,m)}| \le 1.39 \cdot |e^{\Lambda_{T^\varepsilon(\ell,m)}} - 1| = 2.78 \cdot \frac{\sqrt{\ell^m}}{|Y|^{\frac{n}{2}}}.$$

The same method gives (2), after noting that $Y = \pm 1$ has no integer point on (6.4). □

6.3. **Proof of Theorem 6.1.** For brevity, we only consider when $\ell = 3$ and $\varepsilon = -$, as the same method applies to all of the cases. Suppose that there is an integer point (X,Y) on

$X^2+3^m=Y^n$. Therefore, there is an integer $0\le j_6\le 5$ and an algebraic integer $\beta\in\mathbb{Q}(\sqrt{-3})$ for which $N_{K/\mathbb{Q}}(\beta)=Y$ and

$$(X+\sqrt{-3^m})=\frac{\beta^n}{w_{-3}^{j_6}}.$$

In particular, if m is odd, then we have

$$\Lambda_{T^\varepsilon(\ell,m)}=j_6\log(\overline{w}_{-3}/w_{-3})-n\log(\overline{\beta}/\beta)+ki\pi=j_6\log(\overline{w}_{-3}/w_{-3})-n\log(\overline{\beta}/\beta)+k\log(-1).$$

Since $\Lambda_{T^\varepsilon(\ell,m)}\neq 0$, Theorem 6.2 implies that

$$\log|\Lambda_{T^\varepsilon(\ell,m)}|>-C(3,2)h'(\overline{w}_{-3}/w_{-3})h'(\overline{\beta}/\beta)h'(-1)\log(\max\{e,j_6,n,|k|\}.$$

Furthermore, by a short calculation, we get

$$\begin{aligned}&h'(\overline{w}_{-3}/w_{-3})\le\frac{\pi}{3},\\ &h'(\overline{\beta}/\beta)\le\max\{\log|Y|,\pi\}\\ &h'(-1)\le\frac{\pi}{2},\ \max\{e,j_6,n,|k|\})\le n+5.\end{aligned}$$

Therefore, Theorem 6.2 implies that

$$\log|\Lambda_{T^\varepsilon(\ell,m)}|>-\frac{\pi^2}{6}C(3,2)\max\{\log|Y|,\pi\}\log(n+5).$$

However, Lemma 6.1 (1) gives

$$\log(2.78\cdot\sqrt{3^m})-\frac{n}{2}\cdot\log|Y|>\log|\Lambda_{T^\varepsilon(\ell,m)}|>-\frac{\pi^3}{6}C(3,2)\log(n+5)\cdot\log|Y|,$$

which in turn implies that

$$\log(2.78\cdot\sqrt{3^m})-\frac{n}{2}\log 2>-\frac{\pi^3}{6}C(3,2)\sqrt{n+4}.$$

Since we have $C(3,2)=18(4)!\,3^4(64)^5\log(12)$, a direct calculation shows that we must have

$$n\le 1.6m+(60\sqrt{m}+5.9)\cdot 10^{30},$$

which gives a constant that is smaller than the claimed $M^-(3,m)$. Taking into account even m, a similar calculation gives $n<1.6m+(9.4\sqrt{m}+1.4)\cdot 10^{31}$. The claimed $M^-(3,m)$ is a "rounded up" version of the maximum of these two constants.

6.4. **Proof of Theorem 1.4.** Suppose that ℓ^m is a power of an odd prime. Thanks to Theorem 3.2, if $a_f(n)=\pm\ell^m$, then $n=p^{d-1}$, where p and $d\mid\ell(\ell^2-1)$ are odd primes. For each d, Lemma 5.1 gives an integer point on an elliptic or hyperelliptic curve, or gives an integer solution to a Thue equation.

If $\ell=3$ (resp. $\ell=5$), then we find that the only possibility is $d=3$ (resp. $d=3,5$). This leads to the equations in Theorem 6.1, which in turn gives the claimed bounds in these cases. Turning to $\ell\ge 7$, we note for $d=3$ (resp. 5) that one can argue again as in the proof of Theorem 6.1 to conclude that $a_f(p^2)\neq\pm\ell^m$ (resp. $a_f(p^4)\neq\pm\ell^m$) for f with (effectively)

sufficiently large weight $2k$. For any $d \geq 7$, Lemma 5.1 (3) gives the integer solution $(X, Y) = (p^{2k-1}, a_f(p^2))$ to the Thue equation

$$F_{d-1}(X, Y) = \pm \ell^m.$$

As an implementation of Baker's theory of linear forms in logarithms, a well-known paper of Tzanakis and de Weger (see p. 103 of [38]) on Thue equations gives a method for effectively determining an upper bound[12] for $|X|$ of any integer point satisfying $F_{d-1}(X, Y) = \pm \ell^m$, which in turn leads to an upper bound for the weight $2k$. The linearity of these constants in m aspect follows from the formal taking of a logarithm in these Diophantine equations.

[12]The reader should switch the roles of X and Y when applying the discussion in [38].

7. Appendix

(A, B)	Defective $u_n(\alpha, \beta)$
$(\pm 1, 2^1)$	$u_5 = -1$, $u_7 = 7$, $u_8 = \mp 3$, $u_{12} = \pm 45$, $u_{13} = -1$, $u_{18} = \pm 85$, $u_{30} = \mp 24475$
$(\pm 1, 3^1)$	$u_5 = 1$, $u_{12} = \pm 160$
$(\pm 1, 5^1)$	$u_7 = 1$, $u_{12} = \mp 3024$
$(\pm 2, 3^1)$	$u_3 = 1$, $u_{10} = \mp 22$
$(\pm 2, 7^1)$	$u_8 = \mp 40$
$(\pm 2, 11^1)$	$u_5 = 5$
$(\pm 4, 5^1)$	$u_6 = \pm 44$
$(\pm 5, 7^1)$	$u_{10} = \mp 3725$
$(\pm 3, 2^3)$	$u_3 = 1$
$(\pm 5, 2^3)$	$u_6 = \pm 85$

Table 1. *Sporadic examples of defective $u_n(\alpha, \beta)$ satisfying (2.2)*

The families of defective Lucas numbers satisfying (2.2) are given by the following curves.

(7.1)

$$B_{1,k}^{r,\pm} : Y^2 = X^{2k-1} \pm 3^r, \quad B_{2,k} : Y^2 = 2X^{2k-1} - 1, \quad B_{3,k}^{\pm} : Y^2 = 2X^{2k-1} \pm 2,$$
$$B_{4,k}^{r} : Y^2 = 3X^{2k-1} + (-2)^{r+2}, \quad B_{5,k}^{\pm} : Y^2 = 3X^{2k-1} \pm 3, \quad B_{6,k}^{r,\pm} : Y^2 = 3X^{2k-1} \pm 3 \cdot 2^r.$$

(A,B)	Defective $u_n(\alpha,\beta)$	Constraints on parameters
$(\pm m,p)$	$u_3=-1$	$m>1$ and $p=m^2+1$
$(\pm m,p^{2k-1})$	$u_3=\varepsilon 3^r$	$(p,\pm m)\in B_{1,k}^{r,\varepsilon}$ with $3\nmid m$, $(\varepsilon,r,m)\neq(1,1,2)$, and $m^2\geq 4\varepsilon 3^{r-1}$
$(\pm m,p^{2k-1})$	$u_4=\mp m$	$(p,\pm m)\in B_{2,k}$ with $m>1$ odd
$(\pm m,p^{2k-1})$	$u_4=\pm 2\varepsilon m$	$(p,\pm m)\in B_{3,k}^{\varepsilon}$ with $(\varepsilon,m)\neq(1,2)$ and $m>2$ even
$(\pm m,p^{2k-1})$	$u_6=\pm(-2)^r m(2m^2+(-2)^r)/3$	$(p,\pm m)\in B_{4,k}^{r}$ with $\gcd(m,6)=1$, $(r,m)\neq(1,1)$, and $m^2\geq(-2)^{r+2}$
$(\pm m,p^{2k-1})$	$u_6=\pm\varepsilon m(2m^2+3\varepsilon)$	$(p,\pm m)\in B_{5,k}^{\varepsilon}$ with $3\mid m$ and $m>3$
$(\pm m,p^{2k-1})$	$u_6=\pm 2^{r+1}\varepsilon m(m^2+3\varepsilon\cdot 2^{r-1})$	$(p,\pm m)\in B_{6,k}^{r,\varepsilon}$ with $m\equiv 3 \bmod 6$ and $m^2\geq 3\varepsilon\cdot 2^{r+2}$

TABLE 2. Parameterized families of defective $u_n(\alpha,\beta)$ satisfying (2.2)
Notation: $m,k,r\in\mathbb{Z}^+$, $\varepsilon=\pm 1$, p *is a prime number.*

$(a_f(p),p^{2k-1})$	$\widehat{\sigma}(p,m)$
$(\pm 3,2^3)$	$\sigma_0(m+1)-2$ when $3\mid(m+1)$, $\sigma_0(m+1)-1$ otherwise.
$(\pm 5,2^3)$	$\sigma_0(m+1)-2$ if $6\mid(m+1)$, $\sigma_0(m+1)-1$ otherwise.
$(\pm m,p^{2k-1})$	$\sigma_0(m+1)-4$ if $(p,\pm m)\in S$, $\sigma_0(m+1)-1$ otherwise.

TABLE 3. *Lower bounds on* $\Omega(a_f(p^m))$ *in defective cases for weights* $2k\geq 4$.
Notation: S *is the collection of all points on any of* $B_{1,k}^{r,\pm}, B_{2,k}, B_{3,k}^{r}, B_{4,k}, B_{5,k}^{r}$.

(d, D)	Integer Solutions to $F_{d-1}(X, Y) = D$
$(7, \pm 7)$	$(\pm 1, \pm 4), (\pm 2, \pm 1), (\mp 3, \mp 5)$
$(7, \pm 13)$	$(\pm 3, \pm 10), (\pm 2, \pm 7), (\pm 3, \pm 4), (\pm 4, \pm 1),$ $(\pm 3, \pm 1), (\mp 1, \pm 1), (\mp 2, \mp 5), (\mp 5, \mp 8), (\mp 7, \mp 11)$
$(7, \pm 29)$	$(\mp 6, \mp 1), (\mp 5, \mp 16), (\mp 4, \mp 7), (\pm 1, \pm 5),$ $(\pm 3, \pm 2), (\pm 11, \pm 17)$
$(11, \pm 11), (19, \pm 19),$ $(23, \pm 23), (31, \pm 31)$	$(\pm 1, \pm 4)$
$(11, \pm 23)$	$(\pm 3, \pm 2), (\pm 2, \pm 1), (\mp 2, \mp 3)$
$(13, 13), (17, 17), (29, 29), (37, 37)$	$(-1, -4), (1, 4)$
$(13, -13), (17, -17),$ $(29, -29), (37, -37)$	$\varnothing$
$(19, \pm 37)$	$(\mp 2, \mp 5)$

TABLE 4. *Solutions for the Thue equations where* $D = \pm \ell$ *and* $7 \leq \ell \leq 37$

(d, D)	Integer Solutions to $F_{d-1}(X, Y) = D$
$(7, \pm 41)$	$(\mp 3, \mp 7), (\mp 1, \pm 2), (\pm 4, \pm 5)$
$(41, 41), (53, 53), (61, 61),$ $(73, 73), (89, 89), (97, 97)$	$(-1, -4), (1, 4)$
$(41, -41), (23, \pm 47), (13, 53), (53, -53), (29, \pm 59),$ $(31, \pm 61), (61, -61), (17, -67), (37, \pm 73), (73, -73),$ $(13, -79), (41, \pm 83), (89, -89), (97, -97)$	$\varnothing$
$(7, \pm 43)$	$(\mp 3, \mp 8), (\mp 2, \pm 1), (\pm 5, \pm 7)$
$(11, \pm 43)$	$(\mp 3, \mp 5), (\pm 2, \pm 5)$
$(43, \pm 43), (47, \pm 47), (59, \pm 59), (67, \pm 67),$ $(71, \pm 71), (79, \pm 79), (83, \pm 83)$	$(\pm 1, \pm 4)$
$(13, -53), (17, 67)$	$(-2, -3), (2, 3)$
$(11, \pm 67)$	$(\mp 7, \mp 12), (\mp 3, \mp 11), (\mp 2, \mp 7)$
$(7, \pm 71)$	$(\mp 16, \mp 25), (\mp 5, \mp 9), (\pm 1, \pm 6),$ $(\pm 4, \pm 3), (\pm 7, \pm 23), (\pm 9, \pm 2)$
$(13, 79)$	$(-2, -5), (2, 5)$
$(7, \pm 83)$	$(\mp 8, \mp 13), (\mp 7, \mp 1), (\mp 6, \mp 19),$ $(\pm 3, \pm 11), (\pm 5, \pm 2), (\pm 13, \pm 20)$
$(11, \pm 89)$	$(\mp 1, \pm 1)$
$(7, \pm 97)$	$(\mp 4, \mp 11), (\mp 3, \pm 1), (\pm 7, \pm 10)$

TABLE 5. *Solutions (with GRH) to the Thue equations where* $D = \pm \ell$ *and* $41 \leq \ell \leq 97$

ℓ	$C^+_{2,\ell}$	$C^+_{3,\ell}$	$C^+_{4,\ell}$	$C^+_{6,\ell}$	$C^+_{7,\ell}$
3	$(1, \pm 2)$	$(1, \pm 2)$	$(1, \pm 2)$	$(1, \pm 2)$	$(1, \pm 2)$
5	$(-1, \pm 2)$	$(-1, \pm 2)$	$(-1, \pm 2)$	$(-1, \pm 2)$	$(-1. \pm 2)$
7,23, 29, 47, 53, 59, 61, 67, 83	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
11	$\varnothing$	$(5, \pm 56)$	$\varnothing$	$\varnothing$	$\varnothing$
13	$\varnothing$	$(3, \pm 16)$	$\varnothing$	$\varnothing$	$\varnothing$
17	$(-2, \pm 3), (-1, \pm 4), (2, \pm 5), (4, \pm 9), (8, \pm 23)(43, \pm 282), (52, \pm 375), (5234, \pm 378661)$	$(-1, \pm 4)$	$(-1, \pm 4)$	$(-1, \pm 4)$	$(-1, \pm 4)$
19	$(5, \pm 12)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
31	$(-3, \pm 2)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
37	$(-1, \pm 6), (3, \pm 8), (243, \pm 3788)$	$(-1, \pm 6), (27, \pm 3788)$	$(-1, \pm 6)$	$(-1, \pm 6)$	$(-1, \pm 6)$
41	$(2, \pm 7)$	$(-2, \pm 3)$	$(2, \pm 13)$	$\varnothing$	$\varnothing$
43	$(-3, \pm 4)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
71	$(5, \pm 14)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
73	$(-4, \pm 3), (2, \pm 9), (3, \pm 10), (6, \pm 17), (72, \pm 611), (356, \pm 6717)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
79	$(45, \pm 302)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
89	$(-4, \pm 5), (-2, \pm 9), (10, \pm 33), (55, \pm 408)$	$(2, \pm 11)$	$\varnothing$	$\varnothing$	$\varnothing$
97	$\varnothing$	$\varnothing$	$(2, \pm 15)$	$\varnothing$	$\varnothing$

TABLE 6. *Integer points on* $C^+_{d,\ell}$

ℓ	$C^-_{2,\ell}$	$C^-_{3,\ell}$	$C^-_{4,\ell}$	$C^-_{6,\ell}$	$C^-_{7,\ell}$
$3, 5, 17, 29, 37,$ $41, 43, 59, 73, 97$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
7	$(2, \pm 1),\ (32, \pm 181)$	$(2, \pm 5),\ (8, \pm 181)$	$(2, \pm 11)$	$\varnothing$	$\varnothing$
11	$(3, \pm 4),\ (15, \pm 58)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
13	$(17, \pm 70)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
19	$(7, \pm 18)$	$(55, \pm 22434)$	$\varnothing$	$\varnothing$	$\varnothing$
23	$(3, \pm 2)$	$(2, \pm 3)$	$\varnothing$	$(2, \pm 45)$	$\varnothing$
31	$\varnothing$	$(2, \pm 1)$	$\varnothing$	$\varnothing$	$\varnothing$
47	$(6, \pm 13), (12, \pm 41), (63, \pm 500)$	$(3, \pm 14)$	$(2, \pm 9)$	$\varnothing$	$\varnothing$
53	$(9, \pm 26), (29, \pm 156)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
61	$(5, \pm 8)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
67	$(23, \pm 110)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
71	$(8, \pm 21)$	$\varnothing$	$(3, \pm 46)$	$\varnothing$	$\varnothing$
79	$(20, \pm 89)$	$\varnothing$	$(2, \pm 7)$	$\varnothing$	$\varnothing$
83	$(27, \pm 140)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
89	$(5, \pm 6)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$

TABLE 7. *Integer points on* $C^-_{d,\ell}$

ℓ	$H^-_{3,\ell}$	$H^+_{3,\ell}$	$H^-_{5,\ell}$	$H^+_{5,\ell}$	$H^-_{7,\ell}$	$H^+_{7,\ell}$	$H^-_{11,\ell}$	$H^-_{13,\ell}$
11	$\varnothing$	$(1,7),(7,767)$	$\varnothing$	$(1,7)$	$\varnothing$	$(1,7)$	$\varnothing_*$	$\varnothing$
19	$\varnothing$	$(1,9),(3,61)$	$\varnothing$	$(1,9)$	$\varnothing$	$(1,9)$	$\varnothing$	$\varnothing_*$
29	$\varnothing$	$(1,11)$	$\varnothing$	$(1,11)$	$\varnothing$	$(1,11)$	$\varnothing_*$	$\varnothing_*$
31	$(2,14)$	$\varnothing$	$\varnothing$	$\varnothing$	$(2,286)$	$\varnothing$	$\varnothing_*$	$\varnothing_*$
41	$(3,59)$	$(1,13),(2,22)$	$\varnothing$	$(1,13)$	$\varnothing$	$(1,13)_*$	$\varnothing_*$	$\varnothing_*$
59	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing_*$	$\varnothing$	$\varnothing_*$	$\varnothing_*$	$\varnothing_*$
61	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing_*$	$\varnothing_*$	$\varnothing_*$
71	$(2,6),(5,279)$	$(1,17)$	$\varnothing$	$(1,17)$	$\varnothing$	**?**	$\varnothing_*$	$\varnothing_*$
79	$(2,2),(4,142)$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing_*$	$\varnothing_*$	$\varnothing_*$
89	$\varnothing$	$(1,19),(2,26)$	$\varnothing$	$(1,19)_*,\ (2,74)_*$	$\varnothing$	$(1,19)_*$	$\varnothing_*$	**?**

TABLE 8. $(|X|,|Y|)$ *for integer points on* $H^{\pm}_{d,\ell}$ *with* $\left(\frac{\ell}{5}\right)=1$. *(note. GRH assumption indicated by* $_*$*.)*

References

[1] M. Abouzaid, *Les nombres de Lucas et Lehmer sans diviseur primitif*, J. Th. Nomb. Bordeaux **18** (2006), 299-313.

[2] M. Amir and A. Hatziiliou, *A short note on inadmissible coefficients of weight 2 and* $2k+1$ *newforms*, (arXiv preprint https://arxiv.org/abs/2102.03912).

[3] M. Amir and L. Hong, *On L-functions of modular elliptic curves and certain* $K3$ *surfaces*, (arXiv preprint https://arxiv.org/abs/2007.09803, Ramanujan Journal, accepted for publication.

[4] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134-160.

[5] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **441** (1993), 19-62.

[6] J. S. Balakrishnan, W. Craig, and K. Ono, *Variations of Lehmer's conjecture for Ramanujan's tau-function*, J. Number Theory (Prime), accepted for publication (arXiv preprint https://arxiv.org/abs/2005.10345).

[7] J. S. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai, *Sage code*, https://github.com/jbalakrishnan/Lehmer.

[8] J. S. Balakrishnan, K. Ono, and W.-L. Tsai, *Even values of Ramanujan's tau-function*, La Matematica, accepted for publication, (arXiv preprint https://arxiv.org/abs/2102.00111).

[9] C. Barros, *On the Lebesgue-Nagell equation and related subjects*, Univ. Warwick Ph.D. Thesis, 2010.

[10] M. A. Bennett, A. Gherga, V. Patel, and S. Siksek, *Odd values of the Ramanujan tau function*, (arXiv preprint https://arxiv.org/abs/2101.02933).

[11] B. C. Berndt and K. Ono, *Ramanujan's unpublished manuscript on the partition and tau functions with proofs and commentary*, Sém. Lothar. Combin. **42** (1999), Art. B42c.

[12] Y. Bilu and G. Hanrot, *Solving the Thue equations of high degree*, J. Numb. Th. **60** (1996), 373-392.

[13] Y. Bilu, G. Hanrot, P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75-122.

[14] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1 484-478.

[15] Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Ann. Math. **163** (2006), 969-1018.

[16] Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue-Nagell equation,* Compositio Math. **142** (2006), 31-62.

[17] F. Calegari and N. Sardari, *Vanishing Fourier coefficients of Hecke eigenforms*, arXiv preprint, https://arxiv.org/abs/2003.07570.

[18] J. Cohn, *The Diophantine equation* $x^2 + C = y^n$, Acta Arith. **55** (1993), 367-381.

[19] R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770.

[20] P. Deligne, *La conjecture de Weil. I*, Publ. Math. de IHES **43** (1974), 273-307.

[21] P. Deligne, *La conjecture de Weil. II*, Publ. Math. de IHES **52** (1980), 137-252.

[22] S. Dembner and V. Jain, *Hyperelliptic curves and newform coefficients*, J. Number Th., accepted for publication (arXiv preprint https://arxiv.org/abs/2007.08358).

[23] M. Hanada and R. Madhukara, *Fourier coefficients of Level 1 Hecke eigenforms,* Acta Arithmetica, accepted for publication (arXiv preprint https://arxiv.org/abs/2007.08683).

[24] D. H. Lehmer, *The vanishing of Ramanujan's* $\tau(n)$, Duke Math. J. **14** (1947), 429-433.

[25] D. H. Lehmer, *The primality of Ramanujan's Tau-function*, Amer. Math. Monthly **72** (1965), 15-18.

[26] N. Lygeros and O. Rozier, *Odd prime values of the Ramanujan tau function*, Ramanujan J. **32** (2013), 269-280.

[27] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine. Angew. Math. **572** (2004), 167-195.

[28] T. Miyake, *Modular forms*, Springer-Verlag, Berlin, 2006.

[29] V. K. Murty, M. R. Murty, T. N. Shorey, *Odd values of the Ramanujan tau function*, Bull. Soc. Math. France **115** (1987), 391-395.

[30] V. K. Murty and M. R. Murty, *Odd values of Fourier coefficients of certain modular forms*, Int. J. Numb. Th. **3** (2007), 455-470.
[31] K. Ono and Y. Taguchi, 2-*adic properties of certain modular forms and their applications to arithmetic functions,* Int. J. Numb. Th. **1** (2005), 75-101.
[32] The PARI Group, PARI/GP version `2.11.1`, Univ. Bordeaux, 2019, `http://pari.math.u-bordeaux.fr/`.
[33] S. Ramanujan, *On certain arithmetical functions*, Trans. Camb. Philos. Soc. **22** no. 9 (1916), 159-184.
[34] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. `https://www.sagemath.org`.
[35] J.-P. Serre, *Une interprétation des congruences relatives à la fonction τ de Ramanujan*, Sem. Delange-Pisot-Poitou **14** no. 1 (1968), 1-17.
[36] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. de IHES **54** (1981), 323-401.
[37] J. Thorner and A. Zaman, *A Chebotarev variant of the Brun-Titchmarsh Theorem and bounds for the Lang-Trotter conjectures,* Int. Math. Research Notices (2018) No. 16, 4991-5027.
[38] N. Tzanakis and B. de Weger *On the practical solution of the Thue equation*, J. Number Th. **31** (1989), 99-132.

Department of Mathematics and Statistics, Boston University, Boston, MA 02215
Email address: `jbala@bu.edu`

Department of Mathematics, University of Virginia, Charlottesville, VA 22904
Email address: `wlc3vf@virginia.edu`
Email address: `ken.ono691@virginia.edu`
Email address: `tsaiwlun@gmail.com`