Annales mathématiques du Québec (2023) 47:389–402
https://doi.org/10.1007/s40316-021-00168-4

A short note on inadmissible coefficients of weight 2 and $2k+1$ newforms

Malik Amir[1] · **Andreas Hatziiliou**[2]

Received: 28 February 2021 / Accepted: 27 May 2021 / Published online: 16 June 2021

Abstract
Let $f(z) = q + \sum_{n\geq 2} a(n)q^n$ be a weight k normalized newform with integer coefficients and trivial residual mod 2 Galois representation. We extend the results of Amir and Hong in Amir and Hong (On L-functions of modular elliptic curves and certain K3 surfaces, Ramanujan J, 2021) for $k = 2$ by ruling out or locating all odd prime values $|\ell| < 100$ of their Fourier coefficients $a(n)$ when n satisfies some congruences. We also study the case of odd weights $k \geq 1$ newforms where the nebentypus is given by a quadratic Dirichlet character.

Résumé
Soit $f(z) = q + \sum_{n\geq 2} a(n)q^n$ une forme de Hecke normalisée de poids k à coefficients entiers possédant une représentation galoisienne modulo 2 triviale. On généralise les résultats de Amir et Hong présentés dans Amir and Hong (On L-functions of modular elliptic curves and certain K3 surfaces,, Ramanujan J, 2021) pour le poids $k = 2$ en éliminant ou en localisant toutes les valeurs impaires $|\ell| < 100$ des coefficients de Fourier $a(n)$ pour n respectant certaines congruences. On étudie aussi le cas des poids impairs $k \geq 1$ de formes de Hecke dont le caractère est donné par un caractère quadratique de Dirichlet.

Keywords Lucas sequences · Lehmer's conjecture · Modular forms · L-Functions · Elliptic curves

1 Introduction and statement of the results

In an article entitled *"On certain arithmetical functions"* [17], Ramanujan introduced the τ-function in 1916, known as the Fourier coefficients of the weight 12 modular form

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

✉ Malik Amir
malik.amir.math@gmail.com

Andreas Hatziiliou
andreas.hatziiliou@mail.mcgill.ca

[1] Department of Mathematics, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland

[2] Department of Mathematics and Statistics, McGill University, Montreal, Canada

where throughout $q{:=}e^{2\pi iz}$. It was conjectured by Ramanujan that the τ-function is multiplicative and this offered a glimpse into a much more general theory known today as the theory of Hecke operators. Despite its importance in the large web of mathematics and physics, basic properties of $\tau(n)$ are still unknown. The most famous example is Lehmer's conjecture about the nonvanishing of $\tau(n)$. Lehmer proved that if $\tau(n) = 0$, then n must be a prime [12]. One may be interested in studying odd values taken by $\tau(n)$ or, more generally, the coefficients of any newform. This is the question we consider as a variation of Lehmer's original speculation.

For an odd number α, Murty, Murty and Shorey [14] proved using linear forms in logarithms that $\tau(n) \neq \alpha$ for all n sufficiently large. However, the bounds that they obtained are huge and computationally impractical. Recently, using the theory of Lucas sequences, Balakrishnan, Craig, Ono and Tsai proved in [3] and [4], together with work of Dembner and Jain in [10], that $\tau(n) = \ell$ has no solution for $|\ell| < 100$ an odd prime. In addition, Hanada and Madhukara proved in [11] that $\tau(n) = \alpha$ has no solution for $|\alpha| < 100$ an odd integer. Following these ideas, Amir and Hong investigated weight 2 and 3 newforms corresponding to modular elliptic curves and a special family of $K3$ surfaces in [2].

In this paper, we extend slightly the results of [2] on inadmissible coefficients for L-functions of modular elliptic curves and give a procedure to rule out odd prime values ℓ, positive or negative, as coefficients of any normalized newform of odd weight $k \geq 1$ with integer coefficients having trivial residual mod 2 Galois representation and a quadratic Dirichlet character. For the rest of this paper, whenever we say newform of weight k, we talk about a newform with the aforementioned properties. In the case of weight 2 newforms, we have the following results.

Theorem 1.1 *Suppose* $f(z) = q + \sum_{n\geq 2} a(n)q^n \in S_2^{new}(\Gamma_0(N)) \cap \mathbb{Z}[[q]]$ *has trivial residual mod 2 Galois representation, namely,* $E/\mathbb{Q}$ *is an elliptic curve of conductor N with a rational* 2*-torsion point. Then the following are true.*
If $E/\mathbb{Q}$ *has a rational* 3*-torsion point, then for* $n > 1$ *and* $\gcd(n, 2 \cdot 3 \cdot N) = 1$*, we have*

1. *If* $a(n) = 7, 13, 19, 31, 37$*, then* $n = p^2$ *and* $p = 2 \pmod 3$.
2. *If* $a(n) = 29$ *then* $n = p^{d-1} = 13^4$ *and* $a(p) = \pm 2$.
3. *If* $a(n) = 41$ *then* $n = p^{d-1} = 43^4$ *and* $a(p) = \pm 4$.
4. *If* $a(n) = -19$ *then* $n = p^{d-1} = 7^4$ *and* $a(p) = \pm 2$.
5. *If* $a(n) = -31$ *then* $n = p^{d-1} = 7^4$ *and* $a(p) = \pm 4$.
6. *If* $a(n) = -79$ *then* $n = p^{d-1} = 167^4$ *and* $a(p) = \pm 8$.

Furthermore,

$$a(n) \notin \{-1, 1, 5, -7, 11, -13, 17, 23, -37, -43, 47, 53, 59, -61, -67, 71, -73, 83, 89, -97\}.$$

If $E/\mathbb{Q}$ *has a rational* 5*-torsion point, then for* $n > 1$ *and* $\gcd(n, 2 \cdot 5 \cdot N) = 1$*, we have*

1. *If* $\ell \equiv 1 \pmod 5$ *and* $a(n) = \ell$*, then* $n = p^2$ *and* $p \equiv 4 \pmod 5$.
2. *If* $\ell \equiv 2 \pmod 5$*,* $\ell \neq -3$ *and* $a(n) = \ell$*, then* $n = p^2$ *and* $p \equiv 2 \pmod 5$.
3. *If* $\ell \equiv 3 \pmod 5$*,* $\ell \neq 3$ *and* $a(n) = \ell$*, then* $n = p^2$ *and* $p \equiv 1, 3 \pmod 5$.

Furthermore,

$$a(n) \notin \{-1, 1, -11, 19, 29, -31, -41, 59, -61, -71, 79, 89, -691\}.$$

Theorem 1.2 *Let* $E/\mathbb{Q}$ *be an elliptic curve of conductor N with a* 2 *and* 3*-torsion point. Let* $n > 1$ *and* $gcd(n, 2 \cdot 3 \cdot N) = 1$*. If* $\ell \equiv 2 \pmod 3$*,* $\ell \neq 5$ *and the odd prime divisors d of* $|\ell|(|\ell| - 1)(|\ell| + 1)$ *are not congruent to* 2 $\pmod 3$*, then* $a(n) \neq \ell$.

Theorem 1.3 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N with a 2 and 5-torsion point. Let $n > 1$ and $\gcd(n, 2 \cdot 5 \cdot N) = 1$.*

1. *If $\ell \equiv 1 \pmod 5$ and the odd prime divisors d of $|\ell|(|\ell| - 1)(|\ell| + 1)$ are not congruent to $1, 3 \pmod 5$, then $a(n) \neq \ell$.*
2. *If $\ell \equiv 2 \pmod 5$, $\ell \neq -3$ and the odd prime divisors d of $|\ell|(|\ell| - 1)(|\ell| + 1)$ are not congruent to $2, 3 \pmod 5$, then $a(n) \neq \ell$.*
3. *If $\ell \equiv 3 \pmod 5$, $\ell \neq 3$ and the odd prime divisors d of $|\ell|(|\ell| - 1)(|\ell| + 1)$ are not congruent to $2, 3 \pmod 5$, then $a(n) \neq \ell$.*
4. *If $\ell \equiv 4 \pmod 5$ and the odd prime divisors d of $|\ell|(|\ell| - 1)(|\ell| + 1)$ are not congruent to $2, 4 \pmod 5$, then $a(n) \neq \ell$.*

Theorem 1.4 *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and f the corresponding newform with Fourier coefficients $a(n)$. For $r = 3, 5$, suppose that $2 \cdot r$ divides $|E_{\text{tor}}(\mathbb{Q})|$. Then $a(p^{d-1}) \neq r^v$ unless $d = r$ for some $v \in \mathbb{N}$.*

For odd weights $k \geq 3$ newforms, we have the following result.

Theorem 1.5 *Let $\gcd(n, 2 \cdot N) = 1$. Then $a(p^{d-1}) \neq \pm 1$ and for $n > 1$, we also have $a(n) \neq \pm 1$. Furthermore, if $a(n) = \pm\ell$ for some prime ℓ, then $n = p^{d-1}$ where $d | \ell(\ell^2 - 1)$ is odd. If $\pm\ell$ is not defective, then d is an odd prime.*

In Sects. 3.2 and 4, we give results allowing us to state the above theorems independently of the level.

2 Preliminaries

2.1 Lucas sequences and their primitive prime divisors

We recall the deep work of Bilu, Hanrot and Voutier [7] on Lucas sequences which is central to this note.

A *Lucas pair* (α, β) is a pair of algebraic integers, roots of a monic quadratic polynomial $F(x) = (x - \alpha)(x - \beta) \in \mathbb{Z}[x]$ where $\alpha + \beta, \alpha\beta$ are coprime non-zero integers and such that α/β is not a root of unity. To any Lucas pair (α, β) we can associate a sequence of integers $\{u_n(\alpha, \beta)\} = \{u_1 = 1, u_2 = \alpha + \beta, \dots\}$ called *Lucas numbers* defined by the following formula

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

We call a prime $\ell \mid u_n(\alpha, \beta)$ a *primitive prime divisor of* $u_n(\alpha, \beta)$ if $\ell \nmid (\alpha - \beta)^2 u_1(\alpha, \beta) \cdots u_{n-1}(\alpha, \beta)$. We call a Lucas number $u_n(\alpha, \beta)$ with $n > 2$ *defective*[1] if $u_n(\alpha, \beta)$ does not have a primitive prime divisor. Bilu, Hanrot, and Voutier [7] proved the following theorem for all Lucas sequences.

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

This theorem is sharp in the sense that there are sequences for which $u_{30}(\alpha, \beta)$ does not have a primitive prime divisor. Their work, combined with a subsequent paper[2] of Abouzaid

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

[2] This paper included a few cases which were omitted in [7].

[1], gives the *complete classification* of defective Lucas numbers in two categories; a sporadic family of examples and a set of infinite parametrized families, as can be seen from Tables 1–4 in Sect. 1 of [7] and Theorem 4.1 of [1]. The main arguments in our proofs will largely rely on relative divisibility properties of Lucas numbers. We now recall some of these facts[3].

Proposition 2.2 (Prop. 2.1 (ii) of [7]) *If $d \mid n$, then $u_d(\alpha, \beta) | u_n(\alpha, \beta)$.*

In order to keep track of the first occurrence of a prime divisor, we define $m_\ell(\alpha, \beta)$ to 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 2.3 *(Cor. 2.2[4] of [7]) 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 $\ell | \alpha\beta$, then either $\ell | u_n(\alpha, \beta)$ for all n or $\ell \nmid u_n(\alpha, \beta)$ for all n.

We now recall the following facts about newforms of weight $k \in \mathbb{N}$ and character χ that we will denote by $S_k^{new}(\Gamma_0(N), \chi)$. We suggest that the reader take a look at the book of Cohen and Strömberg [9] for a thorough introduction to the theory of modular forms and to and the book of Ono [16] for a clear and concise exposition of more advanced topics.

Proposition 2.4 *Suppose that $f(z) = q + \sum_{n \geq 2} a(n) q^n \in S_k(\Gamma_0(N), \chi)$ is a normalized newform with nebentypus χ. Then the following are true.*

1. *If $\gcd(n_1, n_2) = 1$, then $a(n_1 n_2) = a(n_1) a(n_2)$.*
2. *If $p \nmid N$ is prime and $m \geq 2$, then*
$$a(p^m) = a(p) a(p^{m-1}) - \chi(p) p^{k-1} a(p^{m-2}).$$
3. *If $p \nmid N$ is prime and α_p and β_p are roots of $F_p(x) := x^2 - a(p)x + \chi(p)p^{k-1}$, then*
$$a(p^m) = u_{m+1}(\alpha_p, \beta_p) = \frac{\alpha_p^{m+1} - \beta_p^{m+1}}{\alpha_p - \beta_p}.$$

Moreover, we have the Deligne's bound $|a(p)| \leq 2p^{\frac{k-1}{2}}$.

In this note, we consider Lucas sequences arising from the roots of the Frobenius polynomial

$$F_p(x) := x^2 - Ax + B := x^2 - a(p)x + \chi(p)p^{k-1} = (x - \alpha_p)(x - \beta_p), \tag{2.2}$$

for a fixed prime $p \nmid N$ where

$$u_n(\alpha_p, \beta_p) := a(p^{n-1}) = \frac{\alpha_p^n - \beta_p^n}{\alpha_p - \beta_p},$$

and $|a(p)| \leq 2p^{\frac{k-1}{2}}$.

[3] See Sect. 2 of [7].

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

Table 1 Sporadic family of defective $u_n(\alpha, \beta)$ satisfying equation 2.2 in even weight $2k$ including $2k = 2$ [4]

(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 2 Sporadic family of defective $u_n(\alpha, \beta)$ satisfying Eq. 2.2 *in odd weight* $k \geq 1$

(A, B)	Defective $u_n(\alpha, \beta)$
$(\pm 1, -1)$	$u_5 = 5, u_{12} = \pm 144$
$(\pm 1, 2^1)$	$u_5 = -1, u_7 = 7, u_8 = \mp 3, u_{12} = \pm 45,$ $u_{13} = -1, u_{18} = \pm 85, u_{30} = \mp 24475$
$(\pm 1, 2^2)$	$u_5 = 5, u_{12} = \mp 231$
$(\pm 1, 3^1)$	$u_5 = 1, u_{12} = \pm 160$
$(\pm 1, 5^1)$	$u_7 = 1, u_{12} = \mp 3024$
$(\pm 2, 3^1)$	$u_{10} = \mp 22$
$(\pm 2, 7^1)$	$u_8 = \mp 40$
$(\pm 2, 11^1)$	$u_5 = 5$
$(\pm 5, 7^1)$	$u_{10} = \mp 3725$

2.2 Modular forms and their Galois representation

Definition 2.5 We say that a newform $f \in S_k^{new}(\Gamma_0(N), \chi)$ has trivial residual mod 2 Galois representation if $a(p)$ is even for all $p \nmid 2 \cdot N$.

Remark The condition $p \neq 2$ comes from the fact that the determinant of the representation of the Galois group evaluated at the Frobenius element needs to be nonzero in order to be invertible. Using Proposition 2.4-*(2)*, this implies that we can derive $a(p^d)$ to be odd if and only if d is even. Similarly, we get that $a(p^d)$ is even if and only if d is odd. It follows that $a(n)$ is odd if and only if n is an odd square. Furthermore, requiring $f \in S_2^{new}(\Gamma_0(N))$ to have trivial residual mod 2 Galois representation is equivalent to asking that the associated modular elliptic curve has a rational 2-torsion point.

Table 3 Parameterized family of defective $u_n(\alpha, \beta)$ satisfying Eq. 2.2 in even weight $2k \geq 2$ [4]. Notation: $m, k, r \in \mathbb{Z}^+$, $\varepsilon = \pm 1$, p is a prime number

(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 4 Parameterized family of defective $u_n(\alpha, \beta)$ satisfying Eq. 2.2 in odd weight. Notation: $m, k, r \in \mathbb{Z}^+$, $\varepsilon = \pm 1$, p is a prime number

(A, B)	Defective $u_n(\alpha, \beta)$	Constraints on parameters
$(\pm m, \chi(p)p^{k-1})$	$u_3 = -1$	$\chi(p)p^{k-1} = m^2 + 1$
$(\pm m, \chi(p)p^{k-1})$	$u_3 = 1$	$\chi(p)p^{k-1} = m^2 - 1$ with $m > 1$
$(\pm m, \chi(p)p^{k-1})$	$u_3 = \varepsilon 3^r$	$\chi(p)p^{k-1} = m^2 - \varepsilon 3^r$ with $3 \nmid m$, $(\varepsilon, r, m) \neq (1, 1, 2)$, and $r > 0$
$(\pm m, \chi(p)p^{k-1})$	$u_4 = \pm \varepsilon m$	$2\chi(p)p^{k-1} = m^2 - \varepsilon$ with $2 \nmid m, m \neq 1$
$(\pm m, \chi(p)p^{k-1})$	$u_4 = \pm 2\varepsilon m$	$2\chi(p)p^{k-1} = m^2 - 2\varepsilon$ with $2 \mid m, (\varepsilon, m) \neq (1, 2)$
$(\pm m, \chi(p)p^{k-1})$	$u_6 = (\pm 2m^3 \pm m)/3$	$3\chi(p)p^{k-1} = m^2 - 1$ with $3 \nmid m > 3$
$(\pm m, \chi(p)p^{k-1})$	$u_6 = \pm 2\varepsilon m^3 \pm 3m$	$3\chi(p)p^{k-1} = m^2 - 3\varepsilon$ with $3 \mid m$
$(\pm m, \chi(p)p^{k-1})$	$u_6 = (\pm 2m^3(-2)^r \pm m((-2)^r)^2)/3$	$12\chi(p)p^{k-1} = 4m^2 - (-2)^{r+2}$ $r > 0, m \equiv \pm 1[6], (r, m) \neq (1, 1)$
$(\pm m, \chi(p)p^{k-1})$	$u_6 = \pm 2m^3\varepsilon \cdot 2^r \pm 3m(2^r)^2$	$12\chi(p)p^{k-1} = 4m^2 - 3 \cdot 2^{r+2}\varepsilon, r > 0, m \equiv 3[6]$

3 Newforms of weight $k = 2$

We begin by studying newforms of weight $k = 2$, level N and trivial character χ with integer coefficients. These modular forms are interesting by themselves as they correspond to modular elliptic curves. For completeness, we recall some facts from the weight 2 case presented in [2].

Lemma 3.1 (Lemma 2.1 [2]) *Assume $a(p)$ is even for primes $p \nmid 2 \cdot N$. The only defective odd values $u_d(\alpha_p, \beta_p)$ are given in Table 1 by*

$$(d, A, B, k) \in \{(3, 2, 3, 2), (5, 2, 11, 2)\},$$

and in rows 1 and 2 of Table 2.

Remark For $u_3(\alpha_p, \beta_p) = \varepsilon 3^r$, we have $3 \nmid a(p)$ and so $u_3(\alpha, \beta)$ is the first occurrence of 3 in the sequence. If $3|a(p)$ however, then $\varepsilon 3^r$ is no longer a defective value.

We will make use of the two following fundamental results.

Theorem 3.1 (Modularity Theorem [8]) *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and a rational 2-torsion point. Denote the associated newform with trivial residual mod 2 Galois representation by $f_E(z) = \sum_{n\geq 1} a(n)q^n \in S_2^{New}(\Gamma_0(N)) \cap \mathbb{Z}[[q]]$. Then for all primes $p \nmid 2 \cdot N$ of good reduction, we have*

$$a(p) = p + 1 - \#E(\mathbb{F}_p),$$

where $\#E(\mathbb{F}_p)$ denotes the number of $\mathbb{F}_p$-points of the elliptic curve reduced mod p.

The following theorem of Mazur classifies the possible torsion groups of ellitpic curves of $E/\mathbb{Q}$.

Theorem 3.2 (Mazur's Theorem [15]) *If $E/\mathbb{Q}$ is an elliptic curve, then*

$$E_{\text{tor}}(\mathbb{Q}) \in \{\mathbb{Z}/N\mathbb{Z} \mid 1 \leq N \leq 10 \text{ or } N = 12\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \mid N = 2, 4, 6, 8\}.$$

Furthermore, recall that if $E/\mathbb{Q}$ has good reduction at $p \nmid m$ for some $m \in \mathbb{N}$, then the reduction map

$$\pi : E(\mathbb{Q}) \to E(\mathbb{F}_p), \tag{3.1}$$

is injective when restricted to m-torsion [19]. As a consequence, we get the following result.

Lemma 3.2 (Lemma 3.1 [2]) *Suppose that $E/\mathbb{Q}$ is an elliptic curve and that $r \mid \#E_{\text{tor}}(\mathbb{Q})$. Then for all primes $p \nmid 2 \cdot r \cdot N$, we have*

$$a(p^d) \equiv 1 + p + p^2 + \cdots + p^d \mod r.$$

Lemma 3.3 (Lemma 3.2 [2]) *If $E/\mathbb{Q}$ has a rational 2 and r-torsion point where $r = 3, 5$, then for all $\gcd(n, 2 \cdot r \cdot N) = 1$, we have $|a(n)| \neq 1$.*

3.1 Integer points on Thue equations

We discuss the general approach to solve the equation $a(n) = \ell$ for some prime ℓ, positive or negative, where $a(n)$ is the Fourier coefficient of $f \in S_k^{new}(\Gamma_0(N), \chi) \cap \mathbb{Z}[[q]]$. Assume that $|a(n)| \neq 1$ for some given values of n. Using Proposition 2.4 *(1)-(2)*, we can see that studying $a(n) = \ell$ is equivalent to studying $a(p^{d-1}) = \ell$ for $d \big| |\ell|(|\ell| - 1)(|\ell| + 1)$. From the two-term recurrence relation satisfied by $a(p^{d-1})$, $a(p^{d-1}) = \ell$ reduces to the search of integer points on special curves. We make this statement precise now.

Let D be a non-zero integer. A polynomial equation of the form $F(X, Y) = D$, where $F(X, Y) \in \mathbb{Z}[X, Y]$ is a homogeneous polynomial, is called a *Thue* equation. We will consider those equations arising from the series expansion of

$$\frac{1}{1 - \sqrt{Y}T + XT^2} = \sum_{m=0}^{\infty} F_m(X, Y) \cdot T^m = 1 + \sqrt{Y} \cdot T + (Y - X) \cdot T^2 + \dots \tag{3.2}$$

Lemma 3.4 *If $a(n)$ satisfies Proposition 2.4, and $p \nmid N$ is a prime, then*

$$F_{2m}\left(\chi(p)p^{k-1}, a(p)^2\right) = a(p^{2m}).$$

Hence, solving $a(p^{2m}) = q$ boils down to computing integer solutions to the equation

$$F_{2m}(X, Y) = \ell.$$

Methods for solving Thue equations are implemented in Sage [5], Magma, and are best suited for $m \geq 3$. For $m = 1, 2$, these equations often have infinitely many solutions as they do not represent curves with positive genus when the weight is $k = 1, 2$, hence we require extra information to infer their finiteness. In the case of weight 2 newforms, the idea is to introduce a 3 and 5-torsion point to get additional congruences to avoid having to deal with infinitely many solutions for the equations $a(p^2) = \ell$, $a(p^4) = \ell$. Indeed, note that

$$d \big| |\ell|(|\ell| - 1)(|\ell| + 1) \equiv 0 \pmod 3,$$

for all ℓ and hence $d = 3$ will always have to be checked.

3.2 Some congruences

We now list congruences obtained using Lemma 3.2.

Lemma 3.5 *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N having a rational 2 and 3-torsion point. Consider primes p for which $\gcd(p, 2 \cdot 3 \cdot N) = 1$.*

1. *If $a(p^{d-1}) = \ell = \pm 3$, then*
$$(p, d) \in \{(1, 0), (2, 0), (2, 2) \pmod 3\}.$$
2. *If $a(p^{d-1}) = \ell \equiv 1 \pmod 3$, then*
$$(p, d) \in \{(1, 1), (2, \textit{odd}) \pmod 3\}.$$
3. *If $a(p^{d-1}) = \ell \equiv 2[3]$, then*
$$(p, d) = (1, 2) \pmod 3.$$

Remark In point 2, the last pair is problematic as d is always odd. Hence, it is not possible to provide a general result in this case.

Let $E/\mathbb{Q}$ be an elliptic curve with conductor N having a rational 2 and 5-torsion point. Consider primes p for which $\gcd(p, 2 \cdot 5 \cdot N) = 1$.

1. If $a(p^{d-1}) = \pm 5$, then
$$(p, d) \in \{(1, 0), (3, 0), (3, 4), (4, 0), (4, 4), (4, 2) \pmod 5\}.$$
2. If $a(p^{d-1}) = \ell \equiv 1 \pmod 5$, then
$$(p, d) \in \{(1, 1), (2, 1), (3, 1), (4, 1), (4, 3) \pmod 5\}.$$
3. If $a(p^{d-1}) = \ell \equiv 2 \pmod 5$, then
$$(p, d) \in \{(1, 2), (2, 3) \pmod 5\}.$$
4. If $a(p^{d-1}) = \ell \equiv 3 \pmod 5$, then
$$(p, d) \in \{(1, 3), (3, 3), (2, 2) \pmod 5\}.$$
5. If $a(p^{d-1}) = \ell \equiv 4 \pmod 5$, then
$$(p, d) \in \{(1, 4), (3, 2) \pmod 5\}.$$

Using the above congruences extensively as well as the relative divisibility property of Lucas numbers, we get the following result.

Theorem 3.3 *Suppose* $f(z) = q + \sum_{n \geq 2} a(n)q^n \in S_2^{new}(\Gamma_0(N)) \cap \mathbb{Z}[[q]]$ *has trivial residual mod 2 Galois representation, namely,* $E/\mathbb{Q}$ *is an elliptic curve of conductor N with a rational 2-torsion point. Then the following are true.*
If $E/\mathbb{Q}$ *has a rational 3-torsion point, then for* $n > 1$ *and* $\gcd(n, 2 \cdot 3 \cdot N) = 1$*, we have*

1. *If* $a(n) = 7, 13, 19, 31, 37$*, then* $n = p^2$ *with* $p = 2 \pmod 3$.
2. *If* $a(n) = 29$ *then* $n = p^{d-1} = 13^4$ *and* $a(p) = \pm 2$.
3. *If* $a(n) = 41$ *then* $n = p^{d-1} = 43^4$ *and* $a(p) = \pm 4$.
4. *If* $a(n) = -19$ *then* $n = p^{d-1} = 7^4$ *and* $a(p) = \pm 2$.
5. *If* $a(n) = -31$ *then* $n = p^{d-1} = 7^4$ *and* $a(p) = \pm 4$.
6. *If* $a(n) = -79$ *then* $n = p^{d-1} = 167^4$ *and* $a(p) = \pm 8$.

Furthermore,

$$a(n) \notin \{-1, 1, 5, -7, 11, -13, 17, 23, -37, -43, 47, 53, 59, -61, -67, 71, -73, 83, 89, -97\}.$$

If $E/\mathbb{Q}$ *has a rational 5-torsion point, then for* $n > 1$ *and* $\gcd(n, 2 \cdot 5 \cdot N) = 1$*, we have*

1. *If* $\ell \equiv 1 \pmod 5$ *and* $a(n) = \ell$*, then* $n = p^2$ *and* $p \equiv 4 \pmod 5$.
2. *If* $\ell \equiv 2 \pmod 5$*,* $\ell \neq -3$ *and* $a(n) = \ell$*, then* $n = p^2$ *and* $p \equiv 2 \pmod 5$.
3. *If* $\ell \equiv 3 \pmod 5$*,* $\ell \neq 3$ *and* $a(n) = \ell$*, then* $n = p^2$ *and* $p \equiv 1, 3 \pmod 5$.

Furthermore,

$$a(n) \notin \{-1, 1, -11, 19, 29, -31, -41, 59, -61, -71, 79, 89, -691\}.$$

Remark In the first part of the theorem, we have omitted the primes 43, 61, 67, 73, 79, 97, which are of the form $\ell \equiv 1 \pmod 3$, and the primes $-\ell \equiv 1 \pmod 3$ due to the large number of curves involved. However, following the methods outlined in this text, the interested reader will have no difficulty investigating these cases. In the second part, note that the primes of the form $\ell \equiv 4 \pmod 5$ are those of the outlined list. We've also ruled out -691 simply because it is a pretty number and a nice example of application of Theorem 3.5.

Theorem 3.4 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N with a 2 and 3-torsion point. Let $n > 1$ and $gcd(n, 2 \cdot 3 \cdot N) = 1$. If $\ell \equiv 2 \pmod 3$, $\ell \neq 5$ and the odd prime divisors d of $|\ell|(|\ell| - 1)(|\ell| + 1)$ are not congruent to $2 \pmod 3$, then $a(n) \neq \ell$.*

Theorem 3.5 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N with a 2 and 5-torsion point. Let $n > 1$ and $\gcd(n, 2 \cdot 5 \cdot N) = 1$.*

1. *If $\ell \equiv 1 \pmod 5$ and the odd prime divisors d of $|\ell|(|\ell| - 1)(|\ell| + 1)$ are not congruent to $1, 3 \pmod 5$, then $a(n) \neq \ell$.*
2. *If $\ell \equiv 2 \pmod 5$, $\ell \neq -3$ and the odd prime divisors d of $|\ell|(|\ell| - 1)(|\ell| + 1)$ are not congruent to $2, 3 \pmod 5$, then $a(n) \neq \ell$.*
3. *If $\ell \equiv 3 \pmod 5$, $\ell \neq 3$ and the odd prime divisors d of $|\ell|(|\ell| - 1)(|\ell| + 1)$ are not congruent to $2, 3 \pmod 5$, then $a(n) \neq \ell$.*
4. *If $\ell \equiv 4 \pmod 5$ and the odd prime divisors d of $|\ell|(|\ell| - 1)(|\ell| + 1)$ are not congruent to $2, 4 \pmod 5$, then $a(n) \neq \ell$.*

The above theorems can be made independent of the level using the following lemma.

Lemma 3.6 *Let $p|N$ be a prime and N the level of the newform $f(z)$. Then*

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

Theorem 3.6 *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and $f(z)$ the corresponding newform with Fourier coefficients $a(n)$. For $r = 3, 5$, suppose that $2 \cdot r$ divides $|E_{\text{tor}}(\mathbb{Q})|$. Then $a(p^{d-1}) \neq r^v$ unless $d = r$ for some $v \in \mathbb{N}$.*

Proof Let $r = 3$. Then by Lemma 3.5, $3 \big| |a(p^{d-1})|$ if and only if $3|d$. Indeed, if $p \equiv 0, 2 \pmod 3$, then $a(p^{d-1}) \equiv 1 \pmod 3$ and so $p \equiv 1 \pmod 3$ implies that $3|d$. Suppose that $a(p^{d-1}) = 3^v$ and $d > 3$, then $a(p^{d-4})$ is also a multiple of 3, which contradicts that 3^v is not defective. Thus $d = 3$ is the only solution.

Let $r = 5$. Then by Lemma 3.5, $5 \big| |a(p^{d-1})|$ if and only if $p \equiv 1[5]$ and $5|d$. For $d > 5$, we have $a(p^{d-6})$ is also a multiple of 5, violating that $a(p^{d-1})$ is not defective. Hence $d = 5$. □

4 Newforms of odd weight $k \geq 3$

In this section, we explain the basic framework to rule out odd prime values $\pm\ell$ as Fourier coefficients of odd weight $k \geq 3$ normalized newforms with integer coefficients of level N and nebentypus χ given by a quadratic Dirichlet character and trivial residual mod 2 Galois representation.

Theorem 4.1 *Let $\gcd(n, 2 \cdot N) = 1$. Then $a(p^{d-1}) \neq \pm 1$ and for $n > 1$ we have $a(n) \neq \pm 1$. It follows that if $a(n) = \pm\ell$ for some prime ℓ, then $n = p^{d-1}$ where $d|\ell(\ell^2 - 1)$ is odd. If $\pm\ell$ is not defective, then d is an odd prime.*

Proof Note that ± 1 is a defective value which must be located in the first 2 rows of Table 4. In fact, the table of sporadic values does not have to be considered. In row 1 of Table 4, we have that if $a(p^{d-1}) = -1$, then it must be at $u_3 = a(p^2) = -1$, where the constraints imply that we must satisfy $\chi(p)p^{k-1} = a(p)^2 + 1$. Since $k-1$ is even, let's write $k-1 = 2m$. Then we're left with the equation $\chi(p)x^{2m} = y^2 + 1$ and clearly there are no solutions for $\chi(p) = 0, -1$. If $\chi(p) = 1$ then we obtain $(x^m)^2 - y^2 = 1$ and this gives us the integer solutions $x = \pm 1$, $y = 0$ which aren't allowed. Hence $a(p^{d-1}) \neq -1$ for $\gcd(p, 2 \cdot N) = 1$. Now for row 2, if $a(p^{d-1}) = 1$ then it must happen for $u_3 = a(p^2) = 1$ with constraints given by $\chi(p)p^{k-1} = a(p)^2 - 1, a(p) > 1$. There are no solutions to this equation for $\chi(p) = 0, -1, 1$. Hence $a(p^{d-1}) \neq \pm 1$. □

Lemma 4.1 *The curve $a(p^2) = \pm\ell$ has no solutions if $\chi(p) = 0$. If $\chi(p) = 1$ then the curve has the form $(y - x^m)(y + x^m) = \pm\ell$ which has a unique solution depending on ℓ only. For $\chi(p) = -1$ the curve has the form $y^2 + (x^m)^2 = \pm\ell$ which has no solutions for $-\ell$ and has finitely many solutions for $+\ell$ as it is a sum of squares.*

Hence, to rule out or locate any odd prime value ℓ as a Fourier coefficient of $f(z)$, it suffices to follow the following steps. Let $\gcd(n, 2 \cdot N) = 1$ and ℓ be an odd prime.

1. By multiplicativity of the Fourier coefficients, we have that

$$a(n) = \pm\ell \text{ if and only if } \prod_i a(p_i^{d_i - 1}) = \pm\ell.$$

2. Use Theorem 1.5.
3. Use the Sage Thue solver [5] to solve $a(p^{d-1}) = \pm\ell$ and analyze the solutions.

Lemma 4.2 (Proposition 13.3.14 [9]) *Let $p|N$ and assume that χ can be defined modulo N/p and let $f = \sum a(n)q^n \in S_k^{new}(\Gamma_0(N), \chi)$ be a normalized eigenform. Then*

1. *If $p^2|N$, then $a(p) = 0$.*
2. *If $p^2 \nmid N$, then $a(p)^2 = \chi_1(p)p^{k-2}$ where χ_1 is the character modulo N/p equivalent to χ.*

Using this lemma, we easily obtain the following.

Corollary 4.2 *Suppose that χ can be reduced modulo N/p and call it χ_1. Then $a(p^m) = 0$ for all $m \geq 1$ and $a(n) = 0$ for all $(n, N) \geq p$.*

Proof Recall that $a(p^m) = a(p)a(p^{m-1})$ and if $p^2|N$ the result follows immediately. For $p^2 \nmid N$ we have $a(p)^2 = \chi_1(p)p^{k-2}$. Since k is odd, $k-2$ is odd and if $\chi_1(p) \neq 0$ then $a(p)$ cannot be an integer which is what we require for our newforms. Hence $a(p) = 0$ is the only possibility. □

Lemma 4.3 (Corollary 13.3.17 [9]) *Let $p|N$ and assume that χ cannot be defined modulo N/p. If $f \in S_k^{new}(\Gamma_0(N), \chi)$ is a normalized eigenform, then $|a(p)| = p^{\frac{k-1}{2}}$.*

Corollary 4.3 *Let $p|N$ and assume that χ cannot be defined modulo N/p. Then $a(p^m) = (\pm 1)^m (p^{\frac{k-1}{2}})^m$.*

5 Newforms of weight $k = 1$

In this section, we discuss briefly the problems arising in the case of weight $k = 1$ newforms. Recall that Proposition 2.2 is the main tool to determine if d is prime or not. However, we may have that $n|d$ and $u_n = -1$. From the first row of the defective table, we know that this may happen only if $n = 3$, namely if $u_3 = a(p^2) = -1$. Thus, we would like to avoid $3|d$ but that is not possible as $\ell(\ell-1)(\ell+1)$ is always divisible by 3. This implies that we only have the information that $d|\ell(\ell-1)(\ell+1)$ is odd and no longer an odd prime. First, this leads us to a large amount of equations to verify in order to rule out an odd prime as a Fourier coefficient. Secondly, when $d = 3$, the equation that we obtain is

$$y^2 = \pm\ell + \chi(p)$$

and is incredibly difficult to solve as it is still an open problem to determine if there are infinitely many primes of the form $\ell = y^2 + 1$.

Funding Open Access funding provided by EPFL Lausanne.

References

1. M. Abouzaid, *Les nombres de Lucas et Lehmer sans diviseur primitif*, J. Théor. Nombres Bordeaux **18**, 299-313 (2006).
2. Malik Amir and Letong Hong, *On L-functions of modular elliptic curves and certain K3 surfaces*, https://doi.org/10.1007/s11139-021-00388-w, Ramanujan J. (2021).
3. J. S. Balakrishnan, W. Craig, and K. Ono, *Variations of Lehmer's Conjecture for Ramanujan's tau-function*, ISSN 0022-314X, J Number Theory (2020).
4. J. S. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai, *Variants of Lehmer's speculation for newforms*, arXiv:2005.10354 [math.NT] (2020).
5. J. S. Balakrishnan, W. Craig, and K. Ono, *Sage code*, https://github.com/jbalakrishnan/Lehmer.
6. Y. Bilu and G. Hanrot, *Solving the Thue equations of high degree*, Journal of Number Theory, **60**, 373-392 (1996).
7. Y. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539**, 75-122 (2001).
8. C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises*, Journal of the American Mathematical Society **14** (4): 843–939 (2001).
9. H. Cohen and F. Strömberg, *Modular Forms, A Classical Approach*, American Mathematical Society, Graduate Studies in Mathematics 179 (2017).
10. S. Dembner and V. Jain, *Hyperelliptic curves and newform coefficients*, arXiv:2007.08358 [math.NT] (2020), submitted for publication.
11. M. Hanada and R. Madhukara, *Fourier coefficients of level 1 Hecke eigenforms*, arXiv:2007.08683 [math.NT] (2020), submitted for publication.

12. D. H. Lehmer, *The vanishing of Ramanujan's* $\tau(n)$, Duke Math. J. **14**, 429-433 (1947).
13. The LMFDB Collaboration, The L-functions and Modular Forms Database, http://lmfdb.org/, 2020,[Online, accessed July 2020].
14. V. K. Murty, R. Murty, and N. Shorey, *Odd values of the Ramanujan tau function*, Bull. Soc. Math. France **115** (1987), 391-395.
15. B. Mazur *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math., 44(2) : 129-162 (1978).
16. K. Ono, *The Web of Modularity : Arithmetic of the Coefficients of Modular Forms and q-series*, American Mathematical Society, CBMS regional conference series in mathematics, ISSN 0160-7642; no. 102 (2003).
17. S. Ramanujan, *On certain arithmetical functions*, Trans. Camb. Phil. Soc., 22, 159–184 (1916).
18. K. Ribet, *Galois representations attached to eigenforms with nebentypus*, Lecture Notes in Math., vol. 601, Springer-Verlag, New York, pp.17-51 (1976).
19. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Second Edition, New York: SpringerVerlag (2009).