VARIATIONS OF LEHMER'S CONJECTURE FOR RAMANUJAN'S TAU-FUNCTION

JENNIFER S. BALAKRISHNAN, WILLIAM CRAIG AND KEN ONO

Abstract. We consider natural variants of Lehmer's unresolved conjecture that Ramanujan's tau-function never vanishes. Namely, for $n > 1$ we prove that

$$\tau(n) \notin \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 691\}.$$

This result is an example of general theorems (see Theorems 1.2 and 1.3 of [2]) for newforms with trivial mod 2 residual Galois representation. Ramanujan's well-known congruences for $\tau(n)$ allow for the simplified proof in these special cases. We make use of the theory of Lucas sequences, the Chabauty–Coleman method for hyperelliptic curves, and facts about certain Thue equations.

1. Introduction and statement of results

In his famous paper "On certain arithmetical functions," Ramanujan introduced $\tau(n)$, the Fourier coefficients of (note: $q := e^{2\pi iz}$ throughout)

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

the normalized weight 12 cusp form for $\mathrm{SL}_2(\mathbb{Z})$. The tau-function has been a remarkable testing ground for the theory of modular forms. Its multiplicative properties foreshadowed the theory of Hecke operators. Ramanujan conjectured bounds that are now celebrated corollaries of Deligne's proof of the Weil Conjectures. Furthermore, Serre [24] viewed its exceptional congruences [5, 22]

$$\tau(n) \equiv \begin{cases} n^2\sigma_1(n) \pmod 9, \\ n\sigma_1(n) \pmod 5, \\ n\sigma_3(n) \pmod 7, \\ \sigma_{11}(n) \pmod{691}, \end{cases} \tag{1.2}$$

where $\sigma_\nu(n) := \sum_{d|n} d^\nu$, as hints of a theory of modular ℓ-adic Galois representations, which are now ubiquitous in number theory.

Surprisingly, Lehmer's Conjecture [17] that $\tau(n)$ never vanishes remains open.[1] We investigate a variation of the original speculation that has been previously considered. For odd α, Murty, Murty and Saradha [20] proved that $\tau(n) \neq \alpha$ for sufficiently large n. Due to the gigantic bounds that arise when applying the theory of linear forms in logarithms, which is the main technique

Key words and phrases. 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).

[1]Recent work by Calegari and Sardari [11] considers a different aspect. They prove that at most finitely many non-CM newforms with fixed tame p level N have vanishing pth Fourier coefficient.

of their proof, the classification of such n has not been carried out for any $\alpha \neq \pm 1$. We prove the following theorem.

Theorem 1.1. *If $n > 1$, then we have that*

$$\tau(n) \notin \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 691\}.$$

Remark. *The authors and Tsai have obtained more general (and stronger) results [2] for newforms with trivial mod 2 residual Galois representations. For $\tau(n)$ with $n > 1$, we have proved (see Theorem 1.2 of [2]) that*

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

Assuming GRH, we also show that

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

The proof of Theorem 1.1 here is simplified by the knowledge of Ramanujan's congruences (1.2).

The proof of Theorem 1.1 makes use of a number of important tools in concert with (1.2). The deep work of Bilu, Hanrot, and Voutier [7] on primitive prime divisors of Lucas sequences forms the primary framework for the proof. Suppose that $\ell \in \{3, 5, 7, 691\}$ and that $\tau(n) = \pm \ell$. Their theory, combined with (1.2) and the multiplicativity of $\tau(n)$, implies that $n = p^{d-1}$, where p is an odd prime, and $d \mid \ell(\ell^2 - 1)$ are certain odd primes. For $\ell \in \{3, 5, 7\}$, it turns out that one must have $d = \ell$. The condition that

$$\tau(p^{d-1}) = \pm \ell$$

implies the existence of a specific integer point on one of two algebraic curves determined by d. These curves are of hyperelliptic and Thue-type. The proof of Theorem 1.1 follows from the explicit determination of the integer points on these curves. This classification is achieved using the Chabauty–Coleman method [14] and the Bilu–Hanrot algorithm [6] for solving Thue equations.

Acknowledgements

The authors thank the referees, Matthew Bisatt, Michael Griffin, Guillaume Hanrot, Sachi Hashimoto, Céline Maistret, Drew Sutherland, Wei-Lun Tsai, and Charlotte Ure for their helpful comments during the preparation of this paper and [2]. The authors are particularly grateful to Guillaume Hanrot and Wei-Lun Tsai who offered assistance with various computer calculations. The third author thanks the Centre di Ricerca Matematica Ennio De Giorgi (Pisa, Italy) and the organizers of the 2018 conference on modular forms and Drinfeld modules for their kind hospitality.

2. Nuts and bolts

The proof of Theorem 1.1 requires facts about primitive prime divisors of Lucas sequences, the Hecke multiplicative properties of $\tau(n)$, and certain arithmetic facts about specific hyperelliptic curves and Thue equations. We record these facts in this section.

2.1. **Lucas sequences and their prime divisors.** We recall the important work of Bilu, Hanrot, and Voutier [7] on Lucas sequences. Suppose that α and β are algebraic integers for which $\alpha+\beta$ and $\alpha\beta$ are relatively prime integers, where α/β is not a root of unity. These algebraic integers generate a *Lucas sequence* $\{u_n(\alpha,\beta)\} = \{u_1 = 1, u_2 = \alpha+\beta, \dots\}$, 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 $\ell \nmid (\alpha-\beta)^2 u_1(\alpha,\beta)\cdots u_{n-1}(\alpha,\beta)$. Those $u_n(\alpha,\beta)$, where $n>2$, without a primitive prime divisor are called *defective*[2] . In the most famous Lucas sequence, the Fibonacci numbers, the following underlined terms are defective:

$$1, 1, 2, 3, 5, \underline{8}, 13, 21, 34, 55, 89, \underline{144}, 233, 377, \dots$$

(note. The terms $F_1 = 1$ and $F_2 = 1$ are not defective as their indices do not exceed 2.) In 1913 Carmichael [12] proved that 144 is the largest defective Fibonacci number. Bilu, Hanrot, and Voutier [7] proved the definitive result for all Lucas sequences. They proved that every Lucas number $u_n(\alpha,\beta)$, with $n>30$, has a primitive prime divisor. Their work is even more impressive; it is sharp and comprehensive. There are sequences for which $u_{30}(\alpha,\beta)$ is defective. Their work, combined with a subsequent paper[3] by Abouzaid [1], gives the *complete classification* of defective Lucas numbers. Tables 1-4 in Section 1 of [7] and Theorem 4.1 of [1] offer this classification. Every defective Lucas number either belongs to a finite list of sporadic examples, or a finite list of parameterized infinite families.

To study $\tau(n)$, we make use of the following consequence of their classification.

Lemma 2.1. *Suppose that α and β are roots of the monic quadratic integral polynomial*

$$F(X) = X^2 - AX + p^{11} = (X-\alpha)(X-\beta),$$

where p is an odd prime, $|A| = |\alpha+\beta| \le 2p^{\frac{11}{2}}$, and $\gcd(\alpha+\beta, p) = 1$. Then there are no defective Lucas numbers $\{u_n(\alpha,\beta)\} \in \{\pm 1, \pm\ell\}$, where ℓ is prime.

Proof. The proof uses Tables 1-4 of [7] and Theorem 4.1 of [1]. Using the assumption that $\alpha\beta$ is the 11th power of an odd prime, one finds that these Lucas numbers are not among the sporadic defective examples.

A straightforward case-by-case analysis of the parameterized infinite families, using elementary congruences and the truth of Catalan's conjecture [18], that 2^3 and 3^2 are the only consecutive perfect powers, leaves one type of possibility. If $|u_n(\alpha,\beta)| = \ell$, where ℓ is prime, then $n = \ell = 3$, and $\alpha+\beta = \pm m$, where $(p, \pm m)$ is an integer point on one of the hyperelliptic curves

$$Y^2 = X^{11} + 3 \quad \text{or} \quad Y^2 = X^{11} - 3. \tag{2.2}$$

The integer points on these curves are known (for example, see [10, 13]). The second curve has none, while the only integer points on the first are $(1, \pm 2)$, which is not of the form $(p, \pm m)$. □

We require the following fundamental divisibility property for Lucas numbers.

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

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

[3]This paper includes a few cases which were omitted in Tables 3 and 4 of [7].

2.2. **Properties of $\tau(n)$.** Here we record properties enjoyed by Ramanujan's tau-function. These include the Hecke multiplicativity established by Mordell [19], and the deep theorem of Deligne [15, 16] that bounds $|\tau(p)|$.

Theorem 2.2. *The following are true:*

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

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

$$\tau(p^m) = \tau(p)\tau(p^{m-1}) - p^{11}\tau(p^{m-2}).$$

(3) If p *is prime and* α_p *and* β_p *are roots of* $F_p(X) := X^2 - \tau(p)X + p^{11}$, *then*

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

Moreover, we have $|\tau(p)| \leq 2p^{\frac{11}{2}}$, *and* α_p *and* β_p *are complex conjugates.*

2.3. **Integer Points on certain hyperelliptic curves and Thue curves.** To prove Theorem 1.1, we require knowledge of the integer points on certain hyperelliptic curves and Thue equations. Here we include the information we require in the following two subsections.

2.3.1. *Some hyperelliptic curves.* For $d \geq 2$, we define the hyperelliptic curves

$$H_{d,\ell}^{\pm}: \ Y^2 = 5X^{2d} \pm 4\ell \quad \text{and} \quad C_{d,\ell}^{\pm}: \ Y^2 = X^{2d-1} \pm \ell. \tag{2.3}$$

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

Lemma 2.2. *The folllowing 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 $n \geq 0$. Bugeaud, Mignotte, and Siksek [9] proved 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

$$Y^2 = 5X^2 + 20 \quad \text{and} \quad Y^2 = 5X^2 - 20,$$

namely $\{L_1 = 1, L_3 = 4, L_5 = 11, L_7 = 29, \dots\}$ and $\{L_0 = 2, L_2 = 3, L_4 = 7, L_6 = 18, \dots\}$ respectively, split the Lucas numbers. The three claims follow immediately. □

The following satisfying lemma classifies the integer points on $H_{11,691}^{+}$ and $C_{6,691}^{+}$.

Lemma 2.3. *There are no integer points on* $C_{6,691}^{+}$ *and* $H_{11,691}^{+}$.

Proof. We carry out the Chabauty–Coleman method [14] to determine the integral points on these curves.

The genus 5 curve $C_{6,691}^{+}$ has Jacobian with Mordell-Weil rank 0, as can be found using the implementation of 2-descent in `Magma` [8]. Since the rank is less than the genus, we may apply the Chabauty–Coleman method, 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[4] using `SageMath` [23]. This set, by construction, contains the set of 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 of $(2, 0)$. (Indeed, the power series corresponding to the expansion of the integral of ω_0 has each of these points occurring as simple zeros.) We conclude that are no integral points on $C^+_{6,691}$.

To compute integral points on $H^+_{11,691}$, we reduce to considering 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 run 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 of $(2, 0)$. As before, the power series 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, and thus we conclude that there are no integral points on $H^+_{11,691}$. □

In contrast to the algebraic method used to establish Lemma 2.3, we show that there are no integer points on $H^-_{11,691}$ and $C^-_{6,691}$ using the classical analytic method of Thue equations.[5] We use the classical fact that these hyperelliptic equations can be reduced to the setting of Thue equations. A *Thue equation* is an equation of the form

$$F(X, Y) = m,$$

where $F(X, Y) \in \mathbb{Z}[X, Y]$ is homogeneous and m is a non-zero integer. Thanks to work of Bilu and Hanrot [6], many of these equations can be effectively solved using software packages such as `PARI/GP` [21] and `Magma`.

Lemma 2.4. *There are no integer points on $C^-_{6,691}$ and $H^-_{11,691}$.*

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

$$x^2 + D = Cy^n, \tag{2.4}$$

where D and C are non-zero integers. An integer point on (2.4) 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 [4] (also see Proposition 3.1 of [10]) gives a step-by-step algorithm that takes alleged solutions of (2.4) and produces integer points on one of finitely many Thue equations constructed from

[4] `SageMath` code used in this paper can be found in [3].

[5] We could have used the Thue method to provide an alternate proof of Lemma 2.3.

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.

The hyperelliptic curve $C^-_{6,691}$ corresponds to (2.4) 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

$$\begin{aligned}2 \times 5^{55} = {} & (99107717427209 0396)x^{11} + (11970001843922078 9119)x^{10}y - (88315992210028361 72345)x^9y^2 \\ & - (33711634551278645628 0840)x^8y^3 + (84929673003753710343324 30)x^7y^4 \\ & + (17518931198691927887 0504298)x^6y^5 - (18818073681639955856448 10248)x^5y^6 \\ & - (22992541672786450593030038430)x^4y^7 + (10477254155373935910225361 3965)x^3y^8 \\ & + (69787579874992244513311731 2720)x^2y^9 - (10688014861698094526193682 18519)xy^{10} \\ & - (22923003748106478231113842 94421)y^{11}.\end{aligned}$$

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.

We now turn our attention to 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 (2.4), 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

$$\begin{aligned}2^2 \times 5^{110} = {} & -(20587212586465949627980680671826599752)x^{22} \\ & + (11332743968358276586138027492273109223 94)x^{21}y \\ & + \cdots \\ & - (79670423145107301772779399379735976309907264511718034789276856)xy^{21} \\ & + (71809437208138431262783549625248617351731199323326115439324273)y^{22}.\end{aligned}$$

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

□

2.3.2. *Some Thue equations.* We require Thue equations that arise from the generating function

$$\frac{1}{1 - \sqrt{Y}T + XT^2} = \sum_{m=0}^{\infty} F_m(X, Y) \cdot T^m = 1 + \sqrt{Y} \cdot T + (Y - X)T^2 + \cdots . \tag{2.5}$$

For every positive integer m, it is simple to verify that

$$F_{2m}(X, Y) = \prod_{k=1}^{m} \left(Y - 4X \cos^2 \left(\frac{\pi k}{2m + 1} \right) \right). \tag{2.6}$$

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

$$\begin{aligned}F_2(X, Y) &= Y - X, \\ F_4(X, Y) &= Y^2 - 3XY + X^2 \\ F_6(X, Y) &= Y^3 - 5XY^2 + 6X^2Y - X^3.\end{aligned}$$

We require the following lemma about six Thue equations arising from these polynomials.

Lemma 2.5. *The following are true.*

(1) The points $(\pm 1, \pm 4), (\pm 2, \pm 1), (\mp 3, \mp 5)$ *are the only integer solutions to*

$$F_6(X, Y) = \pm 7.$$

(2) There are no integer solutions to

$$F_{22}(X, Y) = \pm 691.$$

(3) The points $(\pm 1, \pm 4)$ *are the only integer solutions to*

$$F_{690}(X, Y) = \pm 691.$$

Proof. Claims (1) and (2) are easily obtained using the Thue solver in `PARI/GP`.

At first glance, the proof of (3) seems far more formidable, as $F_{690}(X, Y)$ is a degree 345 homogeneous polynomial. However, for odd primes p, the Thue equations $F_{p-1}(X, Y) = \pm p$ are essentially the well-studied equations

$$\widehat{F}_p(X, Y) = \prod_{k=1}^{\frac{p-1}{2}} \left(Y - 2X \cos\left(\frac{2\pi k}{p}\right)\right) = \pm p \tag{2.7}$$

that starred in the work of Bilu, Hanrot, and Voutier on primitive prime divisors of Lucas sequences. Indeed, we have that $F_{p-1}(X, Y) = \widehat{F}_p(X, Y - 2X)$. A key step (see Cor. 6.6 of [7]) in their work is that there are no integer solutions to (2.7) with $|X| > e^8$ when $31 \le p \le 787$. By a standard lemma (for example, see Lemma 1.1 of [25] and Proposition 2.2.1 of [6])), 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 simple calculation rules out this possibility, leaving only potential small solutions, those with $|X| \le 4$. For these X we find the solutions $(\pm 1, \pm 2)$, which implies that $(\pm 1, \pm 4)$ are indeed the only integral solutions to $F_{690}(X, Y) = \pm 691$. □

3. Proof of Theorem 1.1

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

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

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

$$\{\tau(p), \tau(p^2), \tau(p^3), \dots\}. \tag{3.1}$$

By Theorem 2.2 (2), if $p \mid \tau(p)$ is prime, then $p^m \mid \tau(p^m)$ for every $m \ge 1$, and so $|\tau(p^m)| \ne 1$. For primes $p \nmid \tau(p)$, Theorem 2.2 (3) gives a Lucas sequence satisfying Lemma 2.1, which in turn implies that there are no defective terms with $u_{m+1}(\alpha_p, \beta_p) = \tau(p^m) = \pm 1$. Therefore, all of the values in (3.1) always have a prime divisor, and so cannot have absolute value 1.

We now turn to the primality of absolute values of $\tau(n)$. Thanks to Hecke multiplicativity (i.e. Theorem 2.2 (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 2.1, which guarantees relative divisibility between Lucas numbers, and Lemma 2.1, which guarantees the absence of defective terms in (3.1), 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

$$m_\ell(p) := \min\{n \geq 1 \ : \ \tau(p^n) \equiv 0 \pmod{\ell}\}. \tag{3.2}$$

For $|\tau(p^d)| = \ell$, we must have $m_\ell(p) = d$, where $d+1$ is also an odd prime.

Thanks to the mod 3 congruence in (1.2), we find that

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

Therefore, $d = 2$ is the only possibility. By Theorem 2.2 (2), if $\tau(p^2) = \pm 3$, then $(p, \tau(p)) \in C^{\pm}_{6,3}(\mathbb{Z})$. However, recall that in (2.2) we used the fact that there are no such integer points.

Thanks to the mod 5 congruence in (1.2), we find that

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

and so we only need to consider $d = 4$. By Theorem 2.2 (2), if $\tau(p^4) = \pm 5$, then $(p, 2\tau(p)^2 - 3p^{11}) \in H^{\pm}_{11,5}(\mathbb{Z})$. Lemma 2.2 (2) and (3) show that no such points exist.

Thanks to the mod 7 congruence in (1.2), 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 $\tau(p^6) = \pm 7$. Thanks to (2.5) and Theorem 2.2 (3), for every $m \geq 1$ we have

$$F_{2m}(p^{11}, \tau(p)^2) = \tau(p^{2m}).$$

Lemma 2.5 (1) shows that there are no such solutions to $F_6(X, Y) = \pm 7$.

Thanks to the mod 691 congruence in (1.2), 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. By Lemma 2.5 (2) and (3), the latter two cases, which correspond to

$$\tau(p^{22}) = F_{22}(p^{11}, \tau(p)^2) = \pm 691 \quad \text{and} \quad \tau(p^{690}) = F_{690}(p^{11}, \tau(p)^2) = \pm 691,$$

have no such solutions. If $\tau(p^2) = \pm 691$, then $(p, \tau(p)) \in C^{\pm}_{6,691}(\mathbb{Z})$. If $\tau(p^4) = \pm 691$, then $(p, 2\tau(p)^2 - 3p^{11}) \in H^{\pm}_{11,691}(\mathbb{Z})$. Lemmas 2.3 and 2.4 show that no such integer points exist. $\square$

References

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

[2] J. S. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai, *Variants of Lehmer's speculation for newforms*, submitted.

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

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

[5] 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.

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

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

[8] 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

[9] 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.

[10] 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.

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

[12] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. Math. **15** (1913), 30-70.

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

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

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

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

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

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

[19] L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions*, Proc. Cambridge Phil. Soc. **19** (1917), 117-124.

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

[21] The PARI Group, PARI/GP version `2.11.1`, Univ. Bordeaux, 2019, http://pari.math.u-bordeaux.fr/.

[22] S. Ramanujan, *On certain arithmetical functions*, Trans. Camb. Philos. Soc. **22** no. 9 (1916), 159-184.

[23] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. `https://www.sagemath.org`.

[24] J.-P. Serre, *Une interprétation des congruences relatives à la fonction* τ *de Ramanujan*, Sem. Delange-Pisot-Poitou **14** no. 1 (1968), 1-17.

[25] 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
E-mail address: `jbala@bu.edu`

Department of Mathematics, University of Virginia, Charlottesville, VA 22904
E-mail address: `wlc3vf@virginia.edu`
E-mail address: `ken.ono691@virginia.edu`