EVEN VALUES OF RAMANUJAN'S TAU-FUNCTION

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

In celebration of Don Zagier's 70th birthday

Abstract. In the spirit of Lehmer's speculation that Ramanujan's tau-function never vanishes, it is natural to ask whether any given integer α is a value of $\tau(n)$. For any given odd α, Murty, Murty, and Shorey proved that $\tau(n) \neq \alpha$ for sufficiently large n. Several recent papers consider the case of odd α. In this note, we determine examples of even integers that are not tau-values. Namely, for the indicated primes ℓ, we prove that

$$\tau(n) \notin \{\pm 2 \cdot 691\} \cup \{2\ell \ : \ 3 \leq \ell \leq 97 \text{ with } \ell \neq 43, 79\}$$
$$\cup \{-2\ell \ : \ 3 \leq \ell \leq 97 \text{ with } \ell \neq 5, 17, 41, 47, 59, 89\} \cup \{-2\ell^2 \ : \ 3 \leq \ell \leq 23\}.$$

The method of proof applies *mutatis mutandis* to newforms with residually reducible mod 2 Galois representation and is easily adapted to generic newforms with integer coefficients.

1. Introduction and statement of results

Ramanujan's tau-function [9, 20], the coefficients of the unique normalized weight 12 cusp form for $\mathrm{SL}_2(\mathbb{Z})$ (note: $q := e^{2\pi i z}$ throughout)

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

has been a remarkable prototype in the theory of modular forms. Despite many advances that reveal its deep properties, Lehmer's Conjecture [18] that $\tau(n)$ never vanishes remains open.

In the spirit of this conjecture, it is natural to ask whether any given integer α is a value of $\tau(n)$. Much is known for odd α thanks to the convenient fact that

$$\Delta(z) \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod 2. \tag{1.2}$$

Murty, Murty, and Shorey [19] proved that $\tau(n) \neq \alpha$ for sufficiently large n. Craig and the authors [4, 5] proved some effective results concerning potential odd values of $\tau(n)$ and, more generally, coefficients of newforms with residually reducible mod 2 Galois representation. Their methods have been carried further in subsequent work by Amir and Hong [2], Dembner and Jain [16], and Hanada and Madhukara [17]. For example, for $n > 1$, these papers prove that

$$\tau(n) \notin \{\pm 1, \pm 691\} \cup \{\pm \ell \ : \ 3 \leq \ell \leq 97 \text{ prime}\}. \tag{1.3}$$

Key words and phrases. Lehmer's Conjecture, Newforms.

The first author acknowledges the support of NSF grant (DMS-1702196), the Clare Boothe Luce Professorship (Henry Luce Foundation), a Simons Foundation grant (Grant #550023), and a Sloan Research Fellowship. The second author thanks the Thomas Jefferson Fund and the NSF (DMS-1601306 and DMS-2002265).

Recently,[1] Bennett, Gherga, Patel, and Siksek [8] proved a number of spectacular results regarding odd values of $\tau(n)$. If $P(m)$ denotes the largest prime factor of m, they prove the existence of an effectively computable constant κ such that for odd $\tau(n)$ with $n \geq 25$, then either

$$P(\tau(n)) > \kappa \cdot \frac{\log\log\log n}{\log\log\log\log n},$$

or there is a prime $p \mid n$ for which $\tau(p) = 0$. In particular, they prove that $|\tau(n)| \neq \ell^b$, where $\ell < 100$ is prime and b is a positive integer.

Much less is known for even α. In this note, we offer the first examples of even numbers that never arise as tau-values. To this end, we first recall lower bounds for the number of prime divisors of tau-values. Craig and the authors proved (see[2] Theorem 1.5 of [5]) that

$$\Omega(\tau(n)) \geq \sum_{\substack{p \mid n \\ prime}} (\sigma_0(\mathrm{ord}_p(n) + 1) - 1) \geq \omega(n), \tag{1.4}$$

where $\omega(n)$ (resp. $\Omega(\tau(n))$) is the number of distinct prime factors of n (resp. $\tau(n)$ with multiplicity), and $\sigma_0(N)$ is the number of positive divisors of N. For example, if $\tau(n) = \pm 2\ell$, where ℓ is an odd prime, then this inequality implies that n has at most two distinct prime factors. Moreover, if $n = p_1^{m_1} p_2^{m_2}$, where $p_1 \neq p_2$ are prime and $m_1, m_2 \geq 1$, then $m_1 + 1$ and $m_2 + 1$ are both prime.

We show that stronger results can often be obtained, given specific integers α. Namely, we identify some even α that can only arise as tau-values with prime argument.

Theorem 1.1. *If $\tau(n) = \alpha$, where*

$$\alpha \in \{\pm 2, \pm 2 \cdot 691\} \cup \{\pm 2\ell \ : \ 3 \leq \ell \leq 97 \text{ prime}\} \cup \{\pm 2\ell^2 \ : \ 3 \leq \ell \leq 23 \text{ prime}\},$$

then n is prime. Under GRH, the same conclusion holds for

$$\alpha \in \{\pm 2\ell^2 \ : \ 23 < \ell \leq 97 \text{ prime}, \ell \neq 61\}.$$

As a corollary, we rule out many of the even α in Theorem 1.1 as possible tau-values.

Corollary 1.2. *For positive integers n, the following are true.*

(1) We have that $\tau(n) \notin \{\pm 2 \cdot 691\}$.

(2) For odd primes $\ell \leq 97$, we have

$$\tau(n) \notin \{2\ell \ : \ell \neq 43, 79\} \cup \{-2\ell \ : \ell \neq 5, 17, 41, 47, 59, 89\}.$$

(3) For odd primes $\ell \leq 23$, we have $\tau(n) \neq -2\ell^2$.

(4) Under GRH, for primes $23 < \ell \leq 97$, with $\ell \neq 61$, we have $\tau(n) \neq -2\ell^2$.

Remark. *As noted earlier, the present work was nearly finished when preprint [8] was posted on the arXiv. Thanks to their work, we note that the claims in Theorem 1.1 and Corollary 1.2 that rely on GRH are unconditionally true. To see this, one applies Theorem 6 of [8], which implies for odd primes $\ell < 100$ that $|\tau(n)| \neq \ell^2$, in the proof of Case (3) of Theorem 1.1.*

Remark. *The first examples of $\tau(n) = \pm 2\ell$, where ℓ is prime, are*

$$\tau(277) = -2 \cdot 8209466002937 \quad \text{and} \quad \tau(1297) = 2 \cdot 58734858143062873.$$

We note that 277 and 1297 are both prime. Every such value with $n \leq 200,000$ has prime n.

[1] Paper [8] was posted on the arXiv just as the authors were making their final edits to this preprint.

[2] Theorem 2.5 of [5] concerns the case of generic newforms with integer coefficients.

The proof of Theorem 1.1 is a modification of the approach employed in [4, 5]. These tools are based on the observation that integer sequences of the form $\{1, \tau(p), \tau(p^2), \tau(p^3), \dots\}$, where p is prime, are *Lucas sequences*. Deep and beautiful work of Bilu, Hanrot, and Voutier [11] on primitive prime divisors of Lucas sequences applies to α-variants of Lehmer's Conjecture. Loosely speaking, their work implies that each $\tau(p^m)$ is divisible by at least one prime ℓ for which $\ell \nmid \tau(p)\tau(p^2)\cdots\tau(p^{m-1})$. In [4, 5], this property is combined with the theory of newforms to obtain variants of Lehmer's Conjecture. Namely, certain odd integers α are ruled out as tau-values, as well as coefficients of newforms with residually reducible mod 2 Galois representation. Such conclusions follow from the absence of special integer points (X, Y) on specific curves, including hyperelliptic curves and curves defined by Thue equations. These special points (if any) have the property that $X = p$ or p^{2k-1}, where p is prime and $2k$ is the weight of the newform.

In Section 2, we recall the main tools from [5] and essential facts about newform coefficients, such as Ramanujan's tau-function. In Section 3, we characterize certain integer points on special curves, which we then use to prove Theorem 1.1. Some cases of this characterization were obtained by Tengely [21]. Finally, we prove Corollary 1.2 using famous congruences of Ramanujan.

Remark. *The proof of Theorem 1.1 applies mutatis mutandis to integer weight newforms with integer coefficients and residually reducible mod 2 Galois representation. A minor modification holds for arbitrary integer weight newforms $f(z)$ with integer coefficients, regardless of its 2-adic properties. Indeed, suppose that $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$, and let α be any non-zero integer. We consider the "equation" $a_f(n) = \alpha$. Theorem 2.5 of [5] offers the generalization of (1.4) which constrains the possible prime factorizations of n; the number of distinct prime factors of n generally does not exceed $\omega(\alpha)$. By the multiplicativity of newform coefficients, for $d \mid \alpha$, we must solve the equation $a_f(p^m) = d$, where $m \geq 1$, and p is prime. To this end, one applies a generalization of Theorem 2.4, which identifies the finitely many m that must be considered.*[3] *In Section 2 we explain that a solution for p, when $m \geq 2$, requires special integer points on specific curves. In many cases, there are no such points, which leads to restrictions such as those in Theorem 1.1.*

Acknowledgements

We would like to thank Matthew Bisatt for several helpful discussions about root numbers of Jacobians of hyperelliptic curves.

2. Nuts and bolts

Here we recall essential facts about Lucas sequences and properties of newform coefficients.

2.1. Properties of Newforms.

We recall basic facts about even integer weight newforms (see [3]), along with the deep theorem of Deligne [14, 15] that bounds their Fourier coefficients.

Theorem 2.1. *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] Theorem 2.4 can be modified to cases where the mod 2 Galois represention is not residually reducible.

(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

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

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

We require Diophantine criteria for the equations $a_f(p^m) = \alpha$, where $m \geq 2$. We use *Thue equations* defined by the coefficients of the generating function

$$\frac{1}{1 - \sqrt{Y}T + XT^2} =: \sum_{m=0}^{\infty} F_m(X, Y) \cdot T^m = 1 + \sqrt{Y} \cdot T + (Y - X)T^2 + \cdots . \tag{2.1}$$

The degree m Thue equations we require are

$$F_{2m}(X, Y) = \prod_{k=1}^{m} \left(Y - 4X \cos^2 \left(\frac{\pi k}{2m+1} \right) \right) = \alpha. \tag{2.2}$$

The next lemma provides the key Diophantine criteria for the proof of Theorem 1.1.

Lemma 2.1. (Lemma 5.1 of [5]) *Assume the notation and hypotheses in Theorem 2.1. 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

$$C_{2k,\alpha} : \quad Y^2 = X^{2k-1} + \alpha.$$

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

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

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

2.2. **Implications of properties of Lucas sequences for newforms.** 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

$$u_n(\alpha, \beta) := \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{2.3}$$

In particular, in the notation of Theorem 2.1, for primes $p \nmid N$ and $m \geq 1$, we have

$$a_f(p^m) = u_{m+1}(\alpha_p, \beta_p) = \frac{\alpha_p^{m+1} - \beta_p^{m+1}}{\alpha_p - \beta_p}. \tag{2.4}$$

The following well-known relative divisibility propery is important for the proof of Theorem 1.1.

Proposition 2.2 (Prop. 2.1 (ii) of [11]). *If $d \mid n$, then $u_d(\alpha, \beta) | u_n(\alpha, \beta)$.*

To prove Theorem 1.1, we employ bounds on the first occurrence of a multiple of a prime ℓ in a Lucas sequence. 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 $\alpha + \beta \equiv 0 \pmod{\ell}$. The following proposition is well known.

Proposition 2.3 (Corollary[4] 2.2 of [11]). *If $\ell \nmid \alpha\beta$ is an odd prime with $m_\ell(\alpha, \beta) > 2$, then the following are true.*

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

(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.*

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 [11] proved that every Lucas number $u_n(\alpha,\beta)$, with $n>30$, has a primitive prime divisor. Their work is comprehensive; they have classified *defective* terms, the integers $u_n(\alpha,\beta)$, with $n>2$, that do not have a primitive prime divisor. Their work, combined with a subsequent paper[5] by Abouzaid [1], gives the *complete classification* of defective Lucas numbers. In [4, 5], these results were applied to even weight newforms, including $\Delta(z)$. Arguing as in these papers, we obtain the following lemma.

Lemma 2.2. *Suppose $2k \geq 4$ is even, and α and β are roots of the integral polynomial*

$$F(X) = X^2 - AX + p^{2k-1} = (X-\alpha)(X-\beta), \tag{2.5}$$

where p is prime, $|A| = |\alpha+\beta| \leq 2p^{\frac{2k-1}{2}}$, and $\gcd(\alpha+\beta, p) = 1$. Then there are no defective Lucas numbers $\{u_n(\alpha,\beta)\} \in \{\pm 2, \pm 2\ell, \pm 2\ell^2\}$, where ℓ is an odd prime. Also, if $u_n(\alpha,\beta) = \pm\ell$ is a defective Lucas number, then one of the following is true.

(1) We have $(A,\ell,n) = (\pm m, 3, 3)$, where $3 \nmid m$ and $(p, \pm m)$ satisfies $Y^2 = X^{2k-1} \pm 3$.
(2) We have $(A,\ell,n) = (\pm\ell, \ell, 4)$, where $(p, \pm\ell)$ satisfies $Y^2 = 2X^{2k-1} - 1$.

Proof. As mentioned above, [1, 11] classify defective Lucas numbers. This classification includes a finite list of sporadic examples and a list of parameterized infinite families. Theorem 2.2 of [5] uses these results to describe the defective Lucas numbers that can arise as newform coefficients, i.e. sequences defined by (2.5). Tables 1 and 2 of [5] list the possible defective cases.

An inspection of Table 1 of [5], which concerns the sporadic examples, reveals that the only possible defective numbers with $2k \geq 4$ have $2k = 4$. Moreover, they are the odd numbers $u_3(\alpha,\beta) = 1$ or $u_4(\alpha,\beta) = \pm 85$.

To complete the proof, we consider the parametrized infinite families in Table 2 of [5]. If $u_n(\alpha,\beta)$ is even, then we only have to consider rows four, five, six, and seven of the table. A simple inspection reveals that $\{\pm 2, \pm 2\ell, \pm 2\ell^2\}$ never arises. This then leaves $u_n(\alpha,\beta) = \pm\ell$ as the only cases to consider. However, Lemma 2.1 of [5] includes these cases, giving (1) and (2) above. □

The following theorem from [5] restricts the prime factorizations of arguments of those Fourier coefficients that are powers of odd primes in absolute value.

Theorem 2.4. (Theorem 3.2 of [5]) *Assume the notation and hypotheses in Theorem 2.1, and suppose that $f(z)$ has weight $2k \geq 6$ and a residually reducible mod 2 Galois representation. If $|a_f(n)| = \ell^m$, with $m \in \mathbb{Z}^+$ and ℓ is an odd prime, then $n = p^{d-1}$, where $p \nmid N$ 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.*

3. Proof of Theorem 1.1 and Corollary 1.2

Here we use the previous section to prove Theorem 1.1 and Corollary 1.2.

[5]This paper included a few cases that were omitted in [11].

3.1. **Integer points on some curves.** To prove Theorem 1.1, we employ Theorem 2.1, Lemma 2.1, and Theorem 2.4. These results reduce the proof of Theorem 1.1 to establishing the unsolvability of equations in primes p of the form $|\tau(p^m)| = \ell^2$. We require a few important lemmas.

Lemma 3.1. *The following are true for odd primes ℓ.*

(1) If $3 \leq \ell \leq 97$, then there are no points $(p, c) \in C_{12,\ell^2}(\mathbb{Z})$, with p prime.
(2) If $5 \leq \ell \leq 97$ with $5 \mid \ell(\ell^2 - 1)$, then there are no points $(p, c) \in H_{12,\ell^2}(\mathbb{Z})$, with p prime.

Proof. To prove (1), we note that if $(p, c) \in C_{12,\ell^2}(\mathbb{Z})$, then $(c + \ell)(c - \ell) = p^{11}$. By considering the factorizations of p^{11}, we have $c = (\pm p^a \pm p^{11-a})/2$, where $0 \leq a \leq 10$. For each ℓ, we find that $p = 2$ does not correspond to a point. For odd p and $a = 0$, we also do not have a point on C_{12,ℓ^2}. Finally, if $1 \leq a \leq 10$, then we have $p \mid c$ leading to another contradiction, as one can show that $p \neq \ell$. Indeed, if $p = \ell$, then $\ell^{11} + \ell^2$ would have to be a perfect square.

A similar argument applies for (2) (i.e. $H_{12,\ell^2}(\mathbb{Z})$), by considering $(c + 2\ell)(c - 2\ell) = 5p^{22}$. □

Lemma 3.2. *For $3 \leq \ell < 500$ prime, there are no integer points $(p, c) \in C_{12,-\ell^2}(\mathbb{Z})$, with p prime.*

Proof. This lemma follows from nice work by Tengely on the Diophantine equation $x^2 + a^2 = y^b$, where $a \geq 3$ is odd and b is prime[6]. The $C_{12,-\ell^2}(\mathbb{Z})$ are the cases where $a = \ell$, $b = 11$, $x = Y$, and $y = X$. Using the theory of linear forms in logarithms, combined with some algebraic number theory, for $3 \leq a \leq 501$, he determines (see Corollary 2 of [21]) all of the integer solutions (x, y) with $|x| \geq a^2$ and $\gcd(x, y) = 1$. The only such points occur with $b = 3$, and none of them correspond to the points we seek on $C_{12,-9}(\mathbb{Z})$. Therefore, if $(p, c) \in C_{12,-\ell^2}(\mathbb{Z})$ is an alleged integer point with p prime, then either $|c| < \ell^2$ or $\gcd(p, c) \neq 1$.

For primes $\ell \leq 500$, we computed the finitely many integers $c^2 + \ell^2$, with $c < \ell^2$. None of the numbers are 11th powers. Therefore, any alleged point (p, c) has $\gcd(p, c) = p$. Therefore, $c = pc_0$, where c_0 is an integer, and $\ell^2 = p^{11} - c^2 = p^2(p^9 - c_0^2)$. Since ℓ is prime, we have $p = \ell$ and $\ell^9 - c_0^2 = 1$. None of the primes $\ell < 500$ have the property that $\ell^9 - 1$ is a perfect square. □

Lemma 3.3. *If $\ell \in \{5, 11, 19\}$, then there are no points $(p, y) \in H_{12,-\ell^2}(\mathbb{Z})$, with p prime. Under GRH, the same conclusion holds for $\ell \in \{29, 31, 59, 71, 79, 89\}$.*

Proof of Lemma 3.3. We implemented standard algorithms for finding integral points on affine models of hyperelliptic curves and curves defined by Thue equations. The calculations were performed in `SageMath`. The $H_{12,-\ell^2}$ are hyperelliptic curves, which can be handled using work of Barros [7] and Bugeaud, Mignotte, and Siksek [12] on equations of the form

$$x^2 + D = Cy^n, \tag{3.1}$$

where D and C are non-zero integers. An integral point (X, Y) can be viewed in $\mathbb{Q}(\sqrt{-D})$ as

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

Such equations have been studied extensively using Thue equations. Namely, Theorem 2.1 of [7] (also see Proposition 3.1 of [12]) gives an algorithm that takes alleged solutions of (3.1) and produces integral points on one of finitely many Thue equations constructed from C, D, and n via the arithmetic of $\mathbb{Q}(\sqrt{-D})$, i.e. using the units and the ideal class group of $\mathbb{Q}(\sqrt{-D})$.

The $H_{12,-\ell^2}$ correspond to (3.1) for the imaginary quadratic field $\mathbb{Q}(\sqrt{-1})$, where $x = Y, y = X, C = 5, D = 4\ell^2$, and $n = 22$. We implemented this algorithm in `SageMath` (see procedure `H-plus-minus` in [6] which can be run with or without assuming GRH). □

[6]The exponent b is p in [21]. We chose b to avoid confusion for the prime p in the lemma.

The proof of Theorem 1.1 requires further hyperelliptic curves $H_{12,-\ell^2}$ that we were unable to handle with the algorithms mentioned above. Using the Chabauty–Coleman method [13], we obtain the following lemma.

Lemma 3.4. *Assuming GRH, there are no points $(p, y) \in H_{12,-41^2}(\mathbb{Z})$, with p prime.*

Proof. We consider integral points on the affine curve $H_{12,-41^2}$. More precisely, we consider the integral points on the curve $A_{41} : Y^2 = 5X^{11} - 4 \cdot 41^2$ and pull back any points found via the map $(X, Y) \to (X^2, Y)$. Using `Magma`, we find, under the assumption of GRH, that the rank of the Jacobian of this genus 5 curve is 0. We make a change of coordinates to work with the monic model $A'_{41} : Y^2 = X^{11} - 4 \cdot 41^2 \cdot 5^{10}$, and we apply the Chabauty–Coleman method [6] in `SageMath` [22]. The prime $p = 3$ is a prime of good reduction for the curve, and taking the point at infinity ∞ as our basepoint, we compute the set of points

$$\left\{ z \in A'_{41}(\mathbb{Z}_3) : \int_\infty^z X^i \frac{dX}{2Y} = 0 \text{ for all } 0, 1, \ldots, 4 \right\},$$

where the integrals are Coleman integrals. By construction, this set contains the integral points on A'_{41}. The computation finds one point with Y-coordinate 0 in the residue disk corresponding to $(1, 0) \in A'_{41}(\mathbb{F}_3)$. We conclude that there are no integral points on the affine curve given by $H_{12,-41^2}$. □

Combined with Lemma 2.1, the four previous lemmas guarantee, for primes p, that $\tau(p^2) \neq \pm\ell^2$ and $\tau(p^4) \neq \pm\ell^2$. For higher even powers of p, we require the following lemma.

Lemma 3.5. *The following are true for $7 \leq \ell \leq 97$ prime.*

(1) If $7 \leq \ell \leq 31$, then there are no integer solutions to $F_{d-1}(X, Y) = \pm\ell^2$ of the form (p^{11}, y), with p prime, where $7 \leq d \mid \ell(\ell^2 - 1)$ is an odd prime.

(2) Under GRH, the same conclusion holds for primes $31 < \ell \leq 97$.

Proof. To solve these equations, we used the Thue solver package in `SageMath` (see procedures `thue_unconditional` and `thue_conditional` in [6]), which is based on [10]. For odd primes $d > 31$, the programs were run assuming GRH to speed up the runtime. □

Examples. *We give examples of the calculations used to prove Lemmas 3.3 and 3.5. As a hyperelliptic example, procedure* `H-plus-minus` *of* [6] *shows that $H_{12,-5^2}(\mathbb{Z}) = \varnothing$. Therefore, there are no integer points (p, y), with p prime. As a Thue example, procedure* `thue_unconditional` *of* [6] *establishes that the integer solutions to $F_6(X, Y) = \pm 13^2$ are $\{(\mp 5, \mp 11), (\mp 1, \pm 4), (\pm 6, \pm 7)\}$. None of the points are of the form (p^{11}, y), with p prime.*

3.2. **Proof of Theorem 1.1.** Theorem 1.1 consists of three different types of α.

(1) The case of $\alpha = \pm 2$.
(2) The case where $\alpha = \pm 2\ell$, where $3 \leq \ell \leq 97$ is prime or $\ell = 691$.
(3) The case where $\alpha = \pm 2\ell^2$, where $3 \leq \ell \leq 97$ is prime.

By Lemma 2.2 with $2k = 12$, the numbers $\{\pm 2, \pm\ell, \pm 2\ell, \pm 2\ell^2\}$ (if they arise) are never defective Lucas numbers in $\{\tau(p), \tau(p^2), \tau(p^3), \ldots\}$, where p is prime. Lemma 2.2 (1) and (2) covers the cases apart from $\pm\ell$, which were ruled out by Lemma 2.1 of [4].

Case (1). By (1.2), $\tau(n)$ is even for every $n > 1$ which is not an odd square. Moreover, since $|\tau(n)| \neq 1$ for any $n > 1$, it follows that $\tau(n) = \pm 2$ requires that $n = p^m$, where either $p = 2$ or p is an odd prime and m is odd. Since $4 \mid \tau(2^m)$ for every $m \geq 1$, the former case does not occur.

Now assume that $\tau(p^m) = \pm 2$, where m is odd and p is an odd prime. Applying Lemma 2.2 to the Lucas sequence $\{\tau(p), \tau(p^2), \tau(p^3), \dots\}$, we have that ± 2 is never defective, which implies, for $m \geq 2$, that there is always an odd prime divisor of $\tau(p^m)$. Hence, we have $m = 1$.

Case (2). Thanks to (1.4), if $\tau(n) = \pm 2\ell$, where ℓ is an odd prime, then either $n = p_1^{m_1}$, or $n = p_1^{m_1} p_2^{m_2}$, where the p_i are prime and the $m_i \geq 1$. In the latter case we would have $|\tau(p_1^{m_1})| = 2$ and $|\tau(p_2^{m_2})| = \ell$. Thanks to (1.3), this is impossible for $\ell = 691$ and primes $3 \leq \ell \leq 97$.

Therefore, we may assume that $\tau(p_1^{m_1}) = \pm 2\ell$. Arguing as above, we see that $p_1 \neq 2$, and so (1.2) implies that m_1 is odd. Moreover, since $\tau(p_1)$ is even, it must be that $\tau(p_1^{m_1})$ is the first term in the Lucas sequence that is divisible by ℓ. Otherwise, $\pm 2\ell$ would be defective, contradicting Lemma 2.2. Proposition 2.3 implies that $m_1 + 1$ is an even divisor of $\ell(\ell^2 - 1)$. By the relative divisibility of Lucas numbers given in Proposition 2.2, and the nondefectivity of ± 2 in Lemma 2.2, it follows that $m_1 + 1$ is also prime. Therefore, we have $m_1 = 1$.

Case (3). Since $3 \leq \ell \leq 97$ is prime, (1.3) implies that $|\tau(n)| \neq \ell$ for all n. Moreover, since $|\tau(n)| \neq 1$ for $n > 1$, for $|\tau(n)| = 2\ell^2$ it must be that either $|\tau(p_1^{m_1})| = 2\ell^2$, or $|\tau(p_1^{m_1})| = 2$ and $|\tau(p_2^{m_2})| = \ell^2$, where the p_i are prime and the $m_i \geq 1$. Furthermore, the nondefectivity guaranteed by Lemma 2.2, combined with the relative divisibility of Proposition 2.2, implies that $(m_2+1) \mid \ell(\ell^2-1)$ is prime. Moreover, (1.2) implies that (m_2+1) is an odd prime. Lemma 2.1 and Theorem 2.4 shows that the latter case requires the presence of integer points with $X \in \{p, p^{11}\}$, where p is prime, on specific curves considered in Lemmas 3.1-3.5. These lemmas show (in some cases conditional on GRH) that there are no such points.

Therefore, we may assume that $\tau(p_1^{m_1}) = \pm 2\ell^2$, where p_1 is an odd prime. The argument in Case (2), where the conclusion is that $m_1 = 1$, applies *mutatis mutandis*. In fact, the argument applies to all equations of the form $\tau(p_1^{m_1}) = \pm 2\ell^a$, where $a \geq 1$.

3.3. **Proof of Corollary 1.2.** We recall the following congruences of Ramanujan (see [9, 20]):

$$\tau(n) \equiv \begin{cases} n^3\sigma_1(n) \pmod 4, \\ n^2\sigma_1(n) \pmod 3, \\ n\sigma_1(n) \pmod 5, \\ n\sigma_3(n) \pmod 7. \end{cases}$$

where $\sigma_v(n) := \sum_{1 \leq d \mid n} d^v$. In particular, for primes p, the first four congruences imply that

$$\tau(p) \not\equiv \begin{cases} 10 \pmod{12}, \\ 14 \pmod{20}, \\ 6, 10, 26 \pmod{28}. \end{cases}$$

Since the tau-values in Theorem 1.1 can only arise for prime arguments, these claimed values are ruled out as they obey one of these forbidden congruences.

References

[1] M. Abouzaid. Les nombres de Lucas et Lehmer sans diviseur primitif. *J. Théor. Nombres Bordeaux* **18** (2006), 299-313. ↑5.

[2] M. Amir and L. Hong. On L-functions of modular elliptic curves and certain K3 surfaces. *Ramanujan Journal*, https://arxiv.org/abs/2007.09803, accepted for publication. ↑1.

[3] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.* **185** (1970), 134-160. ↑3.

[4] J. S. Balakrishnan, W. Craig, and K. Ono. Variations of Lehmer's conjecture for Ramanujan's tau-function. *J. Number Theory* (Prime), https://arxiv.org/abs/2005.10345, accepted for publication. ↑1, 3, 5, 7.
[5] J. S. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai. Variants of Lehmer's speculation for newforms, https://arxiv.org/abs/2005.10354, 2020. ↑1, 2, 3, 4, 5.
[6] J. S. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai. Sage code, https://github.com/jbalakrishnan/Lehmer. ↑6, 7.
[7] C. Barros. *On the Lebesgue-Nagell equation and related subjects*. Univ. Warwick Ph.D. Thesis, 2010. ↑6.
[8] M. A. Bennett, A. Gherga, V. Patel, and S. Siksek. Odd values of the Ramanujan tau function, https://arxiv.org/abs/2101.02933, 2021. ↑2.
[9] 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. ↑1, 8.
[10] Y. Bilu and G. Hanrot. Solving the Thue equations of high degree. *J. Numb. Th.* **60** (1996), 373-392. ↑7.
[11] Y. Bilu, G. Hanrot, P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.* **539** (2001), 75-122. ↑3, 4, 5.
[12] 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. ↑6.
[13] R. F. Coleman. Effective Chabauty, *Duke Math. J.* **52** (1985), no. 3, 765–770. ↑7.
[14] P. Deligne. La conjecture de Weil. I. *Publ. Math. de IHES* **43** (1974), 273-307. ↑3.
[15] P. Deligne. La conjecture de Weil. II. *Publ. Math. de IHES* **52** (1980), 137-252. ↑3.
[16] S. Dembner and V. Jain. Hyperelliptic curves and newform coefficients, https://arxiv.org/abs/2007.08358, 2020, preprint. ↑1.
[17] M. Hanada and R. Madhukara. Fourier Coefficients of Level 1 Hecke Eigenforms. *Acta Arithmetica* (https://arxiv.org/abs/2007.08683), accepted for publication. ↑1.
[18] D. H. Lehmer. The vanishing of Ramanujan's $\tau(n)$. *Duke Math. J.* **14** (1947), 429-433. ↑1.
[19] V. K. Murty, R. Murty, T. N. Shorey. Odd values of the Ramanujan tau function. *Bull. Soc. Math. France* **115** (1987), 391-395. ↑1.
[20] S. Ramanujan. On certain arithmetical functions. *Trans. Camb. Philos. Soc.* **22** no. 9 (1916), 159-184. ↑1, 8.
[21] S. Tengely. On the Diophantine equation $x^2 + a^2 = 2y^p$/ *Indag. Mathem., N.S.* **15** (2) (2004), 291-304. ↑3, 6.
[22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. https://www.sagemath.org. ↑7.

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: ken.ono691@virginia.edu
Email address: wt8zj@virginia.edu