



On values of Ramanujan's tau function involving two prime factors

Wenwen Lin¹ · Wenjun Ma² 

Received: 4 September 2022 / Accepted: 17 January 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

Lehmer's conjecture that $\tau(n)$ never vanishes remains open. In the spirit of this conjecture, it is natural to consider for a given integer α , whether there exists $n \in \mathbb{Z}_+$ such that $\tau(n) = \alpha$. Several recent papers exclude many odd α involving one prime factor or small values of the τ -function using the theory of congruences of $\tau(n)$, Lucas sequences, integer points of elliptic curves, and the Thue equation. In this paper, we generalize the results and methods to infinitely many odd α involving two prime factors, showing that $\tau(n) \neq \pm p_1 p_2^b$ for arbitrary $b \in \mathbb{Z}$, where $3 \leq p_1, p_2 \leq 31$ are primes such that $p_1 p_2 \leq 247$ or $p_1 = p_2$. Moreover, together with the previous results, we get $\tau(n) \neq 3^{b_1} 5^{b_2} 7^{b_3} 11^{b_4} 13^b$ for $b \in \mathbb{Z}$, and $b_i \in \{0, 1\}$, $i = 1, 2, 3, 4$. Besides, we show that $|\tau(n)| > |\tau(3)|$ for all odd $\tau(n)$, $n \neq 1$.

Keywords Lehmer's conjecture · Ramanujan τ -function · Modular forms · Newforms

Mathematics Subject Classification 11F11 · 11F30

Wenjun Ma was funded by National Natural Science Funds of China (NSFC, Grant No. 11801401) and Natural Science Foundation of Tianjin City (Grant No. 19JCQNJC14200).

✉ Wenjun Ma
wjma@tju.edu.cn

Wenwen Lin
wwlin@tju.edu.cn

¹ Department of Mathematics, Tianjin University, 135 Yaguan Road, Jinnan District, Tianjin 300072, People's Republic of China

² Center for Applied Mathematics, Tianjin University, 92 Weijin Road, Nankai District, Tianjin 300072, People's Republic of China

1 Introduction and statement of the result

Ramanujan's τ -function, introduced in the 1916 article titled "On certain arithmetical functions", is defined to be the Fourier coefficients of the normalized weight 12 cusp form for $SL_2(\mathbb{Z})$ given by

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

where $q := e^{2\pi iz}$ throughout. This τ -function plays an important role in the study of modular forms. Despite many advances that reveal its deep properties, Lehmer's conjecture [12] that $\tau(n)$ never vanishes remains open.

In the spirit of Lehmer's speculation, it is natural to consider for a given integer α , whether there exists $n \in \mathbb{Z}_+$ such that $\tau(n) = \alpha$. For odd α , due to the fact that

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

much is known. In 1987, Murty et al. [15] proved that $\tau(n) \neq \alpha$ for sufficiently large n , where α is odd. Lygeros and Rozier [14] showed that $\tau(n) \neq \pm 1$ for all $n > 1$ in 2013. This is the first time that specific integers were ruled out as values of $\tau(n)$. In 2020, new methods were introduced by Balakrishnan et al. [1]. They got that

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

Shortly afterwards, a series of results turned out. Hanada and Madhukara [9] additionally showed

$$\begin{aligned}\tau(n) &\notin \\ &\{-9, \pm 15, \pm 21, -25, -27, -33, \pm 35, \pm 45, \pm 49, -55, \pm 63, \pm 77, -81, \pm 91\},\end{aligned}$$

and Dembner and Jain [8] proved that $\tau(n) \neq \pm l$, and $\tau(n) \neq 5^m$, where $l < 100$ is any odd prime and $m \in \mathbb{Z}$. Bennett et al. [3] proved

$$\tau(n) \neq \pm 3^{b_1} 5^{b_2} 7^{b_3} 11^{b_4},$$

where $b_1, b_2, b_3, b_4 \in \mathbb{Z}_+$, and

$$\tau(n) \neq \pm q^b,$$

where $3 \leq q < 100$ is any prime and $b \in \mathbb{Z}_+$. Besides, they showed

$$\tau(p^6) \neq \pm 3^{b_1} 5^{b_2} 7^{b_3} 11^{b_4} 13^{b_5} 17^{b_6} 19^{b_7} 23^{b_8} 29^{b_9} 31^{b_{10}} 37^{b_{11}}, \quad (2)$$

where p is a prime, $b_i \in \mathbb{Z}$.

For even α , much less is known. Even whether $\tau(n) = \pm 2$ is solvable remains open. In 2021, Balakrishnan et al. [2] proved that for the indicated primes l ,

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

Later, Lakein and Larsen [11] show that if $0 < |\alpha| < 100$, and

$$\alpha \notin T := \{2^k, -24, -48, -70, -90, 92, -96\},$$

then $\tau(n) \neq \alpha$ for all $n > 1$.

The theory of Lucas sequences, integer points on elliptic curves, the Thue equation and congruences of $\tau(n)$ lead to the above results which state that $\tau(n)$ cannot take certain small values as well as many odd values having only one prime factor. It's natural to consider odd α involving two prime factors. We generalize the methods and get the following.

Theorem 1.1 *If $b \in \mathbb{Z}$, then the equation*

$$\tau(n) = \pm p_1 p_2^b \quad (3)$$

has no solution in primes p_1, p_2 with $3 \leq p_1, p_2 \leq 31$, $p_1 p_2 \leq 247$ or $p_1 = p_2$, and integer $n \geq 2$.

Theorem 1.1 shows that $\tau(n)$ cannot take some values with two different given prime factors. According to the Theorem 1.1 and the congruences of $\tau(n)$, we shall get the following values of $\tau(n)$ with multiple prime factors.

Corollary 1.2 *If $n > 1$ is an integer, then the equation*

$$\tau(n) = 3^{b_1} 5^{b_2} 7^{b_3} 11^{b_4} 13^b \quad (4)$$

has no solution, where $b_i \in \{0, 1\}$ for $i = 1, 2, 3, 4$, and $b \in \mathbb{Z}$.

Also, for odd $\tau(n)$, we could show that

Corollary 1.3 *If $n > 3$ is an integer for which $\tau(n)$ is odd, then*

$$|\tau(n)| > |\tau(3)|.$$

This paper is organized as follows: In Sect. 2 we show certain facts about Lucas sequences, τ function and the relation between elliptic curves and newforms that we use later in the paper. In Sect. 3 we obtain that if $n = p^m$ with $m = 2, 4, 10$, Eq. (3) has no solution in any odd prime p and some primes p_1, p_2 . Combining the results of Sect. 3, We present the proof of Theorem 1.1 and offer the proof of Corollary 1.2 and Corollary 1.3 in Sects. 4 and 5.

2 Preliminaries

In this section, we recall some facts about Lucas sequences, the τ -function, elliptic curves and newforms, which are needed in the proof of Theorem 1.1.

2.1 Lucas sequences

We recall some facts about Lucas sequences (see [5] for more details).

A Lucas pair is a pair (α, β) of algebraic integers such that $\alpha + \beta$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity. Given a Lucas pair (α, β) , one defines the corresponding sequence of Lucas numbers by

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad n = 0, 1, 2, \dots$$

Associated to Lucas pair (α, β) , the corresponding characteristic polynomial is

$$X^2 - (\alpha + \beta)X + \alpha\beta \in \mathbb{Z}[X].$$

Let $u_n(\alpha, \beta)$ be a Lucas sequence. It has the following well-known relative divisibility property.

Proposition 2.1 (Proposition 2.1 of [11]) *If $d \mid n$, then $u_d \mid u_n$.*

To prove Theorem 1.1, for odd prime l , we define

$$m_l(\alpha, \beta) := \min\{n \geq 1 : l \mid u_n(\alpha, \beta)\}. \quad (5)$$

Then we have $m_l(\alpha, \beta) = 2$ if and only if $\alpha + \beta \equiv 0 \pmod{l}$, and $m_l(\alpha, \beta)$ fulfills the following.

Proposition 2.2 (Proposition 2.3 of [2]) *If $l \nmid \alpha\beta$ is an odd prime with $2 < m_l(\alpha, \beta) < \infty$, then the following are true:*

- (i) *If $l \mid (\alpha - \beta)^2$, then $m_l(\alpha, \beta) = l$.*
- (ii) *If $l \nmid (\alpha - \beta)^2$, then $m_l(\alpha, \beta) \mid (l - 1)$ or $m_l(\alpha, \beta) \mid (l + 1)$.*

Besides, a prime $p \mid u_n(\alpha, \beta)$ is called a *primitive divisor* of $u_n(\alpha, \beta)$ if p does not divide $(\alpha - \beta)^2 u_1 u_2 \dots u_{n-1}$. We shall apply the celebrated Primitive Divisor Theorem of Bilu et al. [5].

Proposition 2.3 (Bilu, Hanrot and Voutier) *Let (α, β) be a Lucas pair. If $n \geq 5$ and $n \neq 6$ then u_n has a primitive divisor.*

2.2 Properties of $\tau(n)$

For future use, we recall some basic important facts of $\tau(n)$, such as Hecke multiplicativity and congruences of $\tau(n)$.

Proposition 2.4 (Theorem 2.3 of [11]) *The following are true:*

- (i) *If $(m, n) = 1$, then $\tau(mn) = \tau(m)\tau(n)$.*
- (ii) *If p is a prime, and integer $m \geq 2$, then*

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

- (iii) *If p is a prime and α, β are roots of $F_p(X) := X^2 - \tau(p)X + p^{11}$, then*

$$\tau(p^a) = u_{a+1}(\alpha, \beta) = \frac{\alpha^{a+1} - \beta^{a+1}}{\alpha - \beta}.$$

The following well-known congruences of $\tau(n)$ are needed as well.

Proposition 2.5 [17] *The following about congruences of τ function are true:*

$$\tau(n) \equiv n^{-610} \cdot \sigma_{1231}(n) \begin{cases} (\text{mod } 3^6) & \text{if } n \equiv 1 \pmod{3} \\ (\text{mod } 3^7) & \text{if } n \equiv 2 \pmod{3}, \end{cases} \quad (6)$$

$$\tau(n) \equiv n^{-30} \sigma_{71}(n) \pmod{5^3} \quad \text{if } 5 \nmid n, \quad (7)$$

$$\tau(n) \equiv n \cdot \sigma_9(n) \begin{cases} (\text{mod } 7) & \text{if } n \equiv 0, 1, 2 \text{ or } 4 \pmod{7} \\ (\text{mod } 7^2) & \text{if } n \equiv 3, 5 \text{ or } 6 \pmod{7}, \end{cases} \quad (8)$$

$$\begin{cases} \tau(n) \equiv \sigma_{11}(n) \pmod{2^{11}} & \text{if } n \equiv 1 \pmod{8} \\ \tau(n) \equiv 1217 \cdot \sigma_{11}(n) \pmod{2^{13}} & \text{if } n \equiv 3 \pmod{8} \\ \tau(n) \equiv 1537 \cdot \sigma_{11}(n) \pmod{2^{12}} & \text{if } n \equiv 5 \pmod{8} \\ \tau(n) \equiv 705 \cdot \sigma_{11}(n) \pmod{2^{14}} & \text{if } n \equiv 7 \pmod{8}, \end{cases} \quad (9)$$

$$\begin{cases} \tau(p) \equiv 0 \pmod{23} & \text{if } p \text{ is a quadratic non-residue mod } 23 \\ \tau(p) \equiv 2 \pmod{23} & \text{if } p = u^2 + 23v^2 \text{ with } u \neq 0 \\ \tau(p) \equiv -1 \pmod{23} & \text{for other } p \neq 23, \end{cases} \quad (10)$$

where $\sigma_k(n)$ indicates the sum of the k th powers of the divisors of n .

2.3 Elliptic curves and newforms

We also need the two celebrated Theorems about elliptic curves and newforms.

Theorem 2.6 (Modularity Theorem, Theorem 0.4. of [21]) *Elliptic curves over the field of rational numbers are related to modular forms.*

Ribet's theorem is a statement concerning properties of Galois representations associated with modular forms.

Theorem 2.7 (Ribet's theorem, Theorem 5.1 of [16]) *Let f be a weight 2 newform on $\Gamma_0(qN)$, where q does not divide N , with absolutely irreducible 2-dimensional mod p Galois representation $\rho_{f,p}$ unramified at q if $q \neq p$ and finite flat at $q = p$. Then there exists a weight 2 newform g of level N such that*

$$\rho_{f,p} \sim \rho_{g,p}.$$

3 The values of $\tau(p^m)$

To prove Theorem 1.1, we establish the following three propositions in this section.

Proposition 3.1 *The equation*

$$\tau(p^2) = \pm p_1 p_2^b \quad (11)$$

has no solution in odd primes p, p_1, p_2 with $3 \leq p_1, p_2 \leq 31$, $p_1 p_2 \leq 247$, $p_1 \neq p_2$, $\max\{p_1, p_2\} \geq 13$, and $b \in \mathbb{Z}_+$.

Proposition 3.2 *Suppose that at least one of p_1 and p_2 is in the set $\{11, 19, 29, 31\}$. The equation*

$$\tau(p^4) = \pm p_1 p_2^b \quad (12)$$

has no solution in odd primes p, p_1, p_2 with $3 \leq p_1, p_2 \leq 31$, $p_1 p_2 \leq 247$, $p_1 \neq p_2$, $\max\{p_1, p_2\} \geq 13$, $p_1, p_2 \neq 23$, and $b \in \mathbb{Z}_+$.

Proposition 3.3 *The equation*

$$\tau(p^{10}) = \pm p_1 p_2^b \quad (13)$$

has no solution in prime p , odd primes p_1, p_2 with $\min\{p_1, p_2\} \leq 7$, $\max\{p_1, p_2\} = 23$, and $b \in \mathbb{Z}_+$.

3.1 Proof of Proposition 3.1

Applying the method of section 7 of [3], with a hypothetical solution of a Frey–Hellegouarch curve, weight 2 modular form of small level, modularity of elliptic curves and Ribet's Theorem, we prove Proposition 3.1 by constructing suitable sets.

Consider the equation

$$\tau(p^2) = k p_2^b, \quad (14)$$

where $p, p_2, |k|$ are odd primes satisfying $p > 200$, $p_2 \neq |k| < 100$ and $b \in \mathbb{Z}_+$.

Suppose (p, b) be a solution of the above equation. Recall Proposition 2.4 (ii), we know $\tau(p^2) = \tau(p)^2 - p^{11}$. Hence we can write Eq. (14) as the following Diophantine equation of type (11, 11, 2):

$$p^{11} + (kp_2^b) \cdot 1^{11} = \tau(p)^2. \quad (15)$$

According to [4], the solution of (15) can be associated to a solution of the Frey-Hellegouarch curve

$$\begin{cases} E_p : Y^2 = X^3 + 2\tau(p)X^2 + (\tau(p)^2 - p^{11})X & \text{if } p \equiv 1 \pmod{4} \\ E_p : Y^2 = X^3 + 2\tau(p)X^2 + p^{11}X & \text{if } p \equiv 3 \pmod{4}. \end{cases} \quad (16)$$

Let

$$\begin{cases} N = 2^5 \cdot |k| \cdot p_2 \cdot p \\ \Delta = 2^6 \cdot k^2 \cdot p_2^{2b} \cdot p^{11} \end{cases}$$

denote the conductor and minimal discriminant of E_p respectively. Knowing that $p > 200$ is a prime, we have $p \nmid 2kp_2$ and so $\text{ord}_p(\Delta) \equiv 0 \pmod{11}$. Following from the recipes of [4], with Theorems 2.6 and 2.7, we know that there is a normalized weight 2 newform

$$f = q + \sum_{n=2}^{\infty} c_n q^n$$

of level N' , where

$$N' = \begin{cases} 2^5 \cdot |k| & \text{if } 11 \mid b \\ 2^5 \cdot |k| \cdot p_2 & \text{if } 11 \nmid b, \end{cases} \quad (17)$$

and a primitive element $\omega \mid 11$ in the domain $K = \mathbb{Q}(c_1, c_2, \dots)$ such that

$$\rho_{E_p, 11} \sim \rho_{f, \omega}. \quad (18)$$

Let l be a prime satisfying

$$l \nmid 2 \cdot 11 \cdot k \cdot p_2 \cdot p. \quad (19)$$

Taking traces of the images of the Frobenius element at l in (18), we have

$$a_l(E_p) \equiv c_l \pmod{\omega},$$

and so we obtain

$$\text{Norm}_{K/\mathbb{Q}}(a_l(E_p) - c_l) \equiv 0 \pmod{11}, \quad (20)$$

where c_l indicates the l th coefficient of f .

Together with the congruences of the τ function (6)–(10), we derive the existence of b in the following.

Let (s, t) be a pair of integers such that

$$\begin{cases} s \equiv p \pmod{l} \\ t \equiv \tau(p) \pmod{l}, \end{cases}$$

where l is a prime satisfying (19). Suppose that

$$A_l := \left\{ (s, t) : s, t \in \mathbb{F}_l, s \not\equiv 0 \pmod{l}, t^2 - s^{11} \not\equiv 0 \pmod{l} \right\}.$$

With (6), (7), (8) and (10), it's not hard to see that

$$B_l := \begin{cases} A_l & l \neq 3, 5, 7, 23; \\ \{(s, t) \in A_3 : t \equiv s + 1 \pmod{3}\} & l = 3; \\ \{(s, t) \in A_5 : t \equiv s^2(s^3 + 1) \pmod{5}\} & l = 5; \\ \{(s, t) \in A_7 : t \equiv s(s^3 + 1) \pmod{7}\} & l = 7; \\ \{(s, 0) : s \in \mathbb{F}_{23}^* \setminus (\mathbb{F}_{23}^*)^2\} \cup \{(s, t) : s \in (\mathbb{F}_{23}^*)^2, t = 2, -1\} & l = 23. \end{cases} \quad (21)$$

has the same elements as A_l . For $(s, t) \in B_l$, according to (16), we have the representation of E_p on the finite field $\mathbb{F}_l$:

$$\begin{cases} E_{s,t,1} : Y^2 = X^3 + 2tX^2 + (t^2 - s^{11})X \\ E_{s,t,3} : Y^2 = X^3 + 2tX^2 + s^{11}X. \end{cases}$$

According to (20), we have that each $(s, t) \in B_l$ must be in

$$C_{l,j}(f) := \left\{ (s, t) \in B_l : \text{Norm} \left(a_l(E_{s,t,j}) - c_l \right) \equiv 0 \pmod{11} \right\}, \quad (22)$$

where $j = 1, 3$. Then let

$$D_{l,j}(f) := \{t^2 - s^{11} : (s, t) \in C_{l,j}(f)\} \subseteq \mathbb{F}_l. \quad (23)$$

Recall that we have $t^2 - s^{11} \equiv \tau(p)^2 - p^{11} \equiv k \cdot p_2^b \pmod{l}$. Therefore, when $p \equiv j \pmod{4}$, we have $(k \cdot p_2^b \pmod{l}) \in D_{l,j}(f)$ for $j = 1, 3$.

Let M be an integer satisfying $22 \mid M$, and let $0 \leq \beta \leq M - 1$ be the unique integer such that

$$\beta \equiv b \pmod{M}. \quad (24)$$

Then we derive the existence of b from the existence of β .

When $p \equiv 1 \pmod{4}$, by (9) we get

$$k \cdot p_2^\beta \equiv k \cdot p_2^b \equiv \tau(p^2) \equiv \tau(p)^2 - p^{11} \equiv 1 + p + p^2 \equiv 3 \pmod{4}.$$

Similarly, when $p \equiv 3 \pmod{4}$, we obtain

$$k \cdot p_2^\beta \equiv 1 \pmod{4}.$$

For the above two situations, we construct the following sets to discuss the existence of β . Let

$$\begin{cases} \Omega_1 := \{0 \leq \beta \leq M-1 : k \cdot p_2^\beta \equiv 3 \pmod{4}\} \\ \Omega_3 := \{0 \leq \beta \leq M-1 : k \cdot p_2^\beta \equiv 1 \pmod{4}\}. \end{cases}$$

Let f be a weight 2 newform of level N' such that (18), and let

$$F_j(f) := \begin{cases} \{\beta \in \Omega_j : 11 \mid \beta\} & \text{if } N' = 2^5 \cdot |k| \\ \{\beta \in \Omega_j : 11 \nmid \beta\} & \text{if } N' = 2^5 \cdot |k| \cdot p_2, \end{cases}$$

where $j = 1, 3$. Let

$$L := \{l < 200 \text{ prime} : l \nmid 2 \cdot 11 \cdot k \cdot p_2 \cdot p, O_l(p_2) \mid M\},$$

where $O_l(p_2)$ denotes the multiplicative order of p_2 modulo l .

From the assumption that $O_l(p_2) \mid M$ and (24), we see that

$$k \cdot p_2^\beta \equiv k \cdot p_2^b \pmod{l}.$$

Therefore, by (23), when $k \cdot p_2^b \in D_{l,j}(f)$, we must have $k \cdot p_2^\beta \in D_{l,j}(f)$.

$\forall l \in L$ and $j = 1, 3$, let

$$G_{l,j}(f) := \{\beta \in F_j(f) : (k \cdot p_2^\beta \pmod{l}) \in D_{l,j}(f)\}.$$

Taking the intersection of $G_{l,j}(f)$, we limit β to

$$H_j(f) := \bigcap_{l \in L} G_{l,j}(f). \quad (25)$$

Through the above analysis, we can get the following lemma:

Lemma 3.4 Suppose (p, b) is a solution to (14), and $p \equiv j \pmod{4}$, where $j = 1, 3$. There exists some $\beta \in H_j(f)$ such that $\beta \equiv b \pmod{M}$, where $H_j(f)$ is defined as in (25).

Remark 3.5 Not hard to see, when $|k| = 1$, Lemma 3.4 also holds.

Table 1 The values of $a_{p_2}(E_{96a1})$ and $\pm(p_2 + 1)$ corresponding to different p_2

p_2	13	17	19	23	29	31
$a_{p_2}(E_{96a1})$	-2	-6	-4	0	2	4
$\pm(p_2 + 1)$	± 14	± 18	± 20	± 24	± 30	± 32

Now, we are ready to show Proposition 3.1.

Proof (Proof of Proposition 3.1) By inspection, when $p < 200$, we see that the Eq. (11) has no solution (see [13] for all of the values of $\tau(p^2)$ with $p < 200$, including the corresponding prime factorization). So we can suppose $p \geq 200$. Let $k = \pm p_1$ in (14) and $M = 396 = 2^2 \cdot 3^2 \cdot 11$. Then we show Proposition 3.1 in cases $11 \mid b$ and $11 \nmid b$ respectively.

Case I ($11 \mid b$). By (17), we have $N' = 2^5 \cdot p_1$. We wrote a SageMath [20] script (see [13] for the SageMath code required) which for each k and use LMFDB database [18] to compute the weight 2 newform f of level N' and the sets $H_1(f)$ and $H_3(f)$. When $k = 3$, $13 \leq p_2 \leq 31$, and $k = -3$, $p_2 = 19$, we have $N' = 96$. By calculation, we find that when f takes the newform corresponding to the elliptic curve

$$E_{96a1} : Y^2 = X^3 + X^2 - 2X$$

with Cremona label 96a1, $H_1(f) \neq \emptyset$ (All nonempty sets $H_j(f)$ list in Table 5). For the remaining $k = \pm p_1$ and p_2 , we have all the $H_1(f)$ and $H_3(f)$ being empty. Therefore, we have to use another method for the exceptional cases.

Consider the equation

$$\tau(p^2) = \pm 3 \cdot p_2^b, \quad (26)$$

where $13 \leq p_2 \leq 31$. Let (p, b) be a solution to (26). Then we have

$$\rho_{E_p, 11} \sim \rho_{E_{96a1}, 11}. \quad (27)$$

In the Diophantine equation (15), for the prime $13 \leq p_2 \leq 31$, there is $p_2 \mid p \cdot 3 \cdot p_2^b$. Therefore, by [4], we know that E_p has multiplicative reduction at p_2 . However, the conductor of E_{96a1} is 96, so E_{96a1} has a good reduction at p_2 . Comparing the traces of Frobenius at 11 in the two representations (27), by [10] we have

$$\pm(p_2 + 1) \equiv a_{p_2}(E_{96a1}) \pmod{11}. \quad (28)$$

Applying SageMath, we obtain the following results:

Thus, by Table 1, for all prime $13 \leq p_2 \leq 31$, (28) is not true, which gives a contradiction. So by Lemma 3.4, the Eq. (11) has no solution when $11 \mid b$.

Case II ($11 \nmid b$). By (17) we have $N' = 2^5 \cdot p_1 \cdot p_2$. For all k and p_2 , we wrote a SageMath script (see [13]) which for each k and p_2 and use LMFDB database to compute the weight 2 newform f of level N' and the sets $H_1(f)$ and $H_3(f)$ corresponding to each f . It turns out that all $H_1(f)$ and $H_3(f)$ are empty expect for

$$\begin{cases} k = 13, & p_2 = 5 \\ k = -5, & p_2 = 23. \end{cases}$$

For the first exception, we found that when f takes the newform corresponding to the elliptic curve

$$E_{2820d1} : Y^2 = X^3 + X^2 - 2X$$

with Cremona label 2820d1, we have $H_3(f) \neq \emptyset$. For the second exception, we found that when f takes the newform corresponding to the elliptic curve E_{3680d1} with Cremona label 3680d1 or E_{3680g1} with Cremona label 3680g1, we have $H_1(f) \neq \emptyset$ (Table 5 in the Appendix lists all the nonempty sets $H_j(f)$).

We use congruence of $\tau(n)$ to deal with these two exceptions. Suppose (p, b) is a solution to

$$\tau(p^2) = 13 \cdot 5^b. \quad (29)$$

Knowing that $p \geq 200$, we have $5 \nmid p^2$. Hence $p \equiv 1, 2, 3, 4 \pmod{5}$. Then by (7), we have

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

Thus, $\tau(p^2) \not\equiv 0 \pmod{5}$, which gives a contradiction. So the Eq. (29) has no solution. By similar analysis, we get $\tau(p^2) = -5 \cdot 23^b$ has no solution.

Therefore, by Lemma 3.4, when $11 \nmid b$, Proposition 3.1 holds. $\square$

3.2 Proof of Proposition 3.2

Consider the equation

$$\tau(p^4) = k \cdot p_2^b, \quad (30)$$

where $p, p_2, |k|$ are odd primes satisfying $p \geq 200, 5 \neq p_2 \neq |k| < 100$, and $b \in \mathbb{Z}_+$. Suppose (p, b) is a solution of the Eq. (30), then by Proposition 2.4 (ii) we have

$$\tau(p^4) = \tau(p)^4 - 3p^{11}\tau(p)^2 + p^{22}.$$

Therefore we rewrite (30) as the following Diophantine equation of type (11, 11, 2):

$$5(p^2)^{11} + (4 \cdot k \cdot p_2^b) \cdot 1^{11} = (2\tau(p)^2 - 3p^{11})^2. \quad (31)$$

According to [4], the solution of the Eq. (31) can be associated to the following Frey-Hellegouarch curve

$$\begin{cases} E_p : Y^2 = X^3 + (3p^{11} - 2\tau(p)^2)X^2 \\ \quad + (\tau(p)^4 - 3p^{11}\tau(p)^2 + p^{22})X & \text{if } p \equiv 1 \pmod{4} \\ E_p : Y^2 = X^3 + (2\tau(p)^2 - 3p^{11})X^2 \\ \quad + (\tau(p)^4 - 3p^{11}\tau(p)^2 + p^{22})X & \text{if } p \equiv 3 \pmod{4}. \end{cases} \quad (32)$$

Let

$$N = 2^3 \cdot 5 \cdot |k| \cdot p_2 \cdot p \quad (33)$$

denotes the conductor of E_p . With Theorems 2.6 and 2.7, we see that there exists a weight 2 newform f of level N' , where

$$N' = \begin{cases} 2^3 \cdot 5 \cdot |k| & \text{if } 11 \mid b \\ 2^3 \cdot 5 \cdot |k| \cdot p_2 & \text{if } 11 \nmid b, \end{cases} \quad (34)$$

and a prime element $\omega \mid 11$ in the field $K = \mathbb{Q}(c_1, c_2, \dots)$ such that (18) holds.

Let l be a prime satisfying

$$l \nmid 2 \cdot 5 \cdot 11 \cdot |k| \cdot p_2 \cdot p. \quad (35)$$

By a similar argument as in the proof of Proposition 3.1, we have

$$\text{Norm}_{K/\mathbb{Q}}(a_l(E_p) - c_l) \equiv 0 \pmod{11}.$$

Together with the congruences of the τ function, we derive the existence of b in the following.

Let

$$A_l := \left\{ (s, t) : s, t \in \mathbb{F}_l, s \not\equiv 0 \pmod{l}, t^4 - 3s^{11}t^2 + s^{22} \not\equiv 0 \pmod{l} \right\},$$

where l satisfies (35). With (6), (7), (8) and (10), we may construct set B_l the same as (21). For $(s, t) \in B_l$, according to (32), we have

$$\begin{cases} E_{s,t,1} : Y^2 = X^3 + (3s^{11} - 2t^2)X^2 + (t^4 - 3s^{11}t^2 + s^{22})X \\ E_{s,t,3} : Y^2 = X^3 + (2t^2 - 3s^{11})X^2 + (t^4 - 3s^{11}t^2 + s^{22})X. \end{cases}$$

By (20), construct set C_l the same as (22). Let

$$D_{l,j}(f) := \{t^4 - 3s^{11}t^2 + s^{22} : (s, t) \in C_{l,j}(f)\} \subseteq \mathbb{F}_l. \quad (36)$$

Therefore, when $p \equiv j \pmod{4}$, we have $(k \cdot p_2^b \pmod{l}) \in D_{l,j}(f)$, where $j = 1, 3$.

Then let M be an integer such that $22 \mid M$. Let $0 \leq \beta \leq M - 1$ be the unique integer satisfying

$$\beta \equiv b \pmod{M}. \quad (37)$$

Then, we derive the existence of b according to the existence of β .

By (9), we have

$$k \cdot p_2^\beta \equiv k \cdot p_2^b \equiv 1 + p^{11} + p^{22} + p^{33} + p^{44} \equiv 1 \pmod{4}. \quad (38)$$

Hence we construct set

$$\Omega := \{0 \leq \beta \leq M - 1 : k \cdot p_2^\beta \equiv 1 \pmod{4}\}$$

to discuss the existence of β . Let f be a weight 2 newform of level N' satisfying (18) and let

$$F(f) := \begin{cases} \{\beta \in \Omega : 11 \mid \beta\} & \text{if } N' = 2^3 \cdot 5 \cdot |k| \\ \{\beta \in \Omega : 11 \nmid \beta\} & \text{if } N' = 2^3 \cdot 5 \cdot |k| \cdot p_2. \end{cases}$$

Let

$$L := \{l < 200 \text{ prime} : l \nmid 2 \cdot 5 \cdot 11 \cdot |k| \cdot p_2 \cdot p, O_l(p_2) \mid M\}.$$

By $O_l(p_2) \mid M$ and (37), we have $k \cdot p_2^\beta \equiv k \cdot p_2^b \pmod{l}$. Then by (36), when $k \cdot p_2^b \in D_{l,j}(f)$, we see that $k \cdot p_2^\beta \in D_{l,j}(f)$. $\forall l \in L$ and $j = 1, 3$, let

$$G_{l,j}(f) := \{\beta \in F(f) : k \cdot q^\beta \pmod{l} \in D_{l,j}(f)\}.$$

Taking the intersection of $G_{l,j}(f)$, we limit β to

$$H_j(f) := \bigcap_{l \in L} G_{l,j}(f). \quad (39)$$

Through the above analysis, we get the following lemma:

Lemma 3.6 Suppose (p, b) is a solution of the Eq. (30) and $p \equiv j \pmod{4}$, where $j = 1, 3$. There exists $\beta \in H_j(f)$ such that (37), where $H_j(f)$ is defined as (39).

Remark 3.7 Not hard to see, when $|k| = 1$, Lemma 3.6 also holds.

Proof (Proof of Proposition 3.2) The proof of Proposition 3.2 is similar to the proof of Proposition 3.1.

Firstly, suppose $p_2 \neq 5$. By inspection, we know the Eq. (12) has no solution when $p < 200$ (see [13] for all of the values of $\tau(p^4)$ with $p < 200$, including the corresponding prime factorization). So we suppose $p \geq 200$. Let $k = \pm p_1$ in (30),

and suppose $M = 396 = 2^2 \cdot 3^2 \cdot 11$. Then, we show Proposition 3.2 with $p_2 \neq 5$ in cases $11 \mid b$ and $11 \nmid b$, respectively.

Case I ($11 \mid b$). By (34), we have $N' = 2^3 \cdot 5 \cdot p_1$. We wrote a SageMath script (see [13]) which for each k , use LMFDB database to compute the weight 2 newform f of level N' , and the sets $H_1(f)$ and $H_3(f)$ for prime k . After calculation, it is founded that when $k = 5, p_2 = 19, 29, 31$, and f takes the newform corresponding to the elliptic curve

$$E_{200b1} : Y^2 = X^3 + X^2 - 3X - 2$$

with Cremona label 200b1, $H_1(f) \neq \emptyset$ (All nonempty sets $H_j(f)$ list in Table 5). For the other $k = \pm p_1$ and p_2 , we have all the $H_1(f)$ and $H_3(f)$ being empty. For the exceptions, we have $\rho_{E_p, 11} \sim \rho_{E_{200b1}, 11}$. By (33), we know that E_p has multiplicative reduction at p_2 . The conductor of E_{200b1} is 200, and it shows that E_{200b1} has good reduction at p_2 . Comparing the traces of Frobenius at p_2 in the two representations, we have

$$\pm(p_2 + 1) \equiv a_{p_2}(E_{200b1}) \pmod{11}.$$

However, by calculation we get $a_{19}(E_{200b1}) = -4$, $a_{29}(E_{200b1}) = 2$, and $a_{31}(E_{200b1}) = 0$, which gives a contradiction. Therefore, by Lemma 3.6, we know when $11 \mid b$, the Eq. (12) has no solution.

Case II ($11 \nmid b$). By (34), we have $N' = 2^3 \cdot 5 \cdot p_1 \cdot p_2$. By similar argument and calculation, we obtain that all $H_1(f)$ and $H_3(f)$ are empty expect for

$$\begin{cases} k = 5, & p_2 = 29 \\ k = 11, & p_2 = 19 \\ k = -19, & p_2 = 7 \\ k = -31, & p_2 = 7. \end{cases}$$

We use congruences of $\tau(n)$ to deal with these exceptions. For the first exception, when f takes the newform corresponding to the elliptic curve

$$E_{5800f1} : y^2 = X^3 - 55X - 150$$

with Cremona label 5800f1,

$$H_1(f) = \{25, 69, 113, 157, 201, 245, 289, 333, 377\}. \quad (40)$$

And when f takes the newform corresponding to the elliptic curve

$$E_{5800m1} : Y^2 = X^3 - 1375X - 18750$$

with Cremona label 5800m1,

$$H_3(f) = \{3, 47, 91, 135, 179, 223, 267, 311, 355\}. \quad (41)$$

Suppose (p, b) is a solution of

$$\tau(p^4) = 5 \cdot 29^b. \quad (42)$$

Recall that $p \geq 200$, we have $5 \nmid p^4$. Hence $p \equiv 1, 2, 3, 4 \pmod{5}$. It follows that $p^4 \equiv 1 \pmod{5}$. So by (7),

$$\tau(p^4) \equiv \begin{cases} 0 \pmod{5} & \text{if } p \equiv 1 \pmod{5} \\ 1 \pmod{5} & \text{if } p \equiv 2, 3, 4 \pmod{5}. \end{cases} \quad (43)$$

Together with the fact $5 \cdot 29^b \equiv 0 \pmod{5}$, which gives $p \equiv 1 \pmod{5}$, we have

$$p \equiv 1, 6, 11, 16, 21 \pmod{25}.$$

Together with (7), we know

$$\tau(p) \equiv 2, 7, 12, 17, 22 \pmod{25}.$$

Therefore

$$\tau(p^4) \equiv p^{22} - 3p^{11}\tau(p)^2 + \tau(p)^4 \equiv 5 \pmod{25}, \quad (44)$$

which means $5 \cdot 29^b \equiv 5 \pmod{25}$. Hence $b \equiv 0 \pmod{2}$ follows. By (37), we have

$$\beta \equiv 0 \pmod{2}.$$

It is contradictory with (40) and (41). Thus Eq. (42) has no solution.

For the second exception, suppose (p, b) is a solution of

$$\tau(p^4) = 11 \cdot 19^b. \quad (45)$$

When $11 \nmid b$, $N' = 2^3 \cdot 5 \cdot 11 \cdot 19$. By writing SageMath script (see [13]) and using LMFDB database, it is founded that when f takes the newform corresponding to the elliptic curve E_{8360e1} with Cremona label 8360e1, we obtain

$$H_1(f) = \{17, 61, 105, 149, 193, 237, 281, 325, 369\}. \quad (46)$$

By $p \geq 200$, we have $5 \nmid p^4$ and (43).

However,

$$11 \cdot 19^b \equiv \begin{cases} 4 \pmod{5} & \text{if } b \text{ odd} \\ 1 \pmod{5} & \text{if } b \text{ even}. \end{cases}$$

So b must be even. By (37), β is even, which is contradictory to (46). Therefore, Eq. (45) has no solution.

For the third exception, suppose (p, b) is a solution of

$$\tau(p^4) = -19 \cdot 7^b. \quad (47)$$

By $p \geq 200$, we have $7 \nmid p^4$ and

$$p^4 \equiv \begin{cases} 1 \pmod{7} & \text{if } p \equiv 1, 6 \pmod{7} \\ 2 \pmod{7} & \text{if } p \equiv 2, 5 \pmod{7} \\ 4 \pmod{7} & \text{if } p \equiv 3, 4 \pmod{7}. \end{cases}$$

So by (8),

$$\tau(p^4) \not\equiv 0 \pmod{7}.$$

This is a contradiction! Thus (47) has no solution. Similarly, $\tau(p^4) = -31 \cdot 7^b$ has no solution. With Lemma 3.6, we get that Proposition 3.2 holds when $p_2 \neq 5$.

Second, suppose that $p_2 = 5$. Let $k = \pm p_1$ in the Eq. (12). Then, we have $k = \pm 19, \pm 29, \pm 31$. By [11], when $k = \pm 19$, the Eq. (12) has no solution. By (44), we have

$$k \cdot 5^b \equiv 5 \pmod{25}.$$

So when $k = 29, -31$, the Eq. (12) has no solution and when $k = -29, 31, b = 1$. By (38), we get

$$k \cdot p_2^b \equiv 1 \pmod{4}.$$

So when $k = -29, 31$, the Eq. (12) has no solution. Therefore, Proposition 3.2 holds when $p_2 = 5$. $\square$

3.3 Proof of Proposition 3.3

To prove Proposition 3.3, we apply the following two lemmas, which connect the solution of the Eq. (13) with the solution of the Thue–Mahler equation.

Lemma 3.8 (Lemma 5.1 of [1]) *Let p be a prime. Then, for odd $m \geq 3$,*

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

where

$$F_m(X, Y) = \prod_{j=1}^{\lfloor (m-1)/2 \rfloor} \left(Y - 4 \cos^2(\pi j/m) X \right).$$

Define

$$\Psi_m(X, Y) = \prod_{d|m} F_d(X, Y)^{\mu(m/d)} = \prod_{\substack{j=1 \\ (j,m)=1}}^{\lfloor (m-1)/2 \rfloor} (Y - 4 \cos^2(\pi j/m) X).$$

To solve the needed Thue–Mahler equation, we apply the following Lemma:

Lemma 3.9 (Lemma 4.10 of [3]) *Let $m = 5$ or $m \geq 7$. Let x and y be coprime integers, and q be a prime. Suppose $q^a \parallel \Psi_m(x, y)$ with $a \geq 1$ an integer. Then, either $q \equiv \pm 1 \pmod{m}$ or $q^a \mid m$.*

Proof of Proposition 3.3. Let $m = 11$. According to Lemma 3.8, we have

$$\tau(p^{10}) = F_{11}(p^{11}, \tau(p)^2) = \Psi_{11}(p^{11}, \tau(p)^2).$$

Therefore, $(p^{11}, \tau(p)^2, b)$ is the solution of the equation

$$\begin{aligned} \Psi_{11}(X, Y) &= \prod_{\substack{j=1 \\ (j,11)=1}}^{\lfloor (11-1)/2 \rfloor} (Y - 4 \cos^2(\pi j/11) X) \\ &= -X^5 + 15X^4Y - 35X^3Y^2 + 28X^2Y^3 - 9XY^4 + Y^5 \\ &= \pm p_1 p_2^b. \end{aligned} \quad (48)$$

Hence, we only need to deal with the Thue–Mahler equation (48).

In this equation, we have $p_1 = 23$ or $p_2 = 23$. When $p_2 = 23$, we have $(X, Y) = 1$, $p_1 \not\equiv \pm 1 \pmod{11}$ and $p_1 \nmid 11$. Then we get $p_1 \nmid \Psi_{11}(X, Y)$ by Lemma 3.9. So the Eq. (48) has no solution. When $p_1 = 23$, similarly, we have $(X, Y) = 1$, $p_2 \not\equiv \pm 1 \pmod{11}$ and $p_2 \nmid 11$. Hence by Lemma 3.9, we know $p_2^b \nmid \Psi_{11}(X, Y)$. Therefore the Eq. (48) also has no solution. Proposition 3.3 follows. $\square$

4 Proof of Theorem 1.1

Using the previous results described in Sect. 1, it suffices to show that the equation $\tau(n) = \pm p_1 p_2^b$ has no solution, where $3 \leq p_1, p_2 \leq 31$ are primes satisfying $p_1 p_2 \leq 247$, $p_1 \neq p_2$, $\max\{p_1, p_2\} \geq 13$, and $b \in \mathbb{Z}_+$.

Lemma 4.1 *If the equation $\tau(n) = \pm p_1 p_2^b$ has a solution, where $3 \leq p_1, p_2 \leq 31$ are primes such that $p_1 p_2 \leq 247$, $p_1 \neq p_2$, $\max\{p_1, p_2\} \geq 13$, $n > 1$ is an integer and $b \in \mathbb{Z}_+$. Then there exists an odd prime p and $a \in 2\mathbb{Z}_+$ such that $n = p^a$.*

Proof By (1) and the fact that $\pm p_1 p_2^b$ is odd, n must be the square of an odd number. Suppose $n = q_1^{a_1} q_2^{a_2} \cdots q_s^{a_s}$, where $a_i \in 2\mathbb{Z}_+$, and $q_i > 0$, $1 \leq i \leq s$ are different odd primes. By Proposition 2.4 (i),

$$\tau(n) = \tau(q_1^{a_1}) \tau(q_2^{a_2}) \cdots \tau(q_s^{a_s}) = \pm p_1 p_2^b.$$

Table 2 The possible values of a and corresponding (p_1, p_2)

a	(p_1, p_2)
2	(3, 13), (3, 17), (5, 13), (5, 17), (7, 13), (7, 17), (13, 3), (13, 5), (13, 7), (13, 17), (17, 3), (17, 5), (17, 7), (17, 13)
2, 4	(3, 19), (3, 29), (3, 31), (5, 19), (5, 29), (5, 31), (7, 19), (7, 29), (7, 31), (11, 13), (11, 17), (11, 19), (13, 11), (13, 19), (17, 11), (19, 3), (19, 5), (19, 7), (19, 11), (19, 13), (29, 3), (29, 5), (29, 7), (31, 3), (31, 5), (31, 7)
2, 10	(3, 23), (5, 23), (7, 23), (23, 3), (23, 5), (23, 7)

However, by [14], we have $\tau(n) \neq \pm 1$ for $n > 1$. Moreover, for any $n \in \mathbb{Z}_+$, by [3], we know that $\tau(n) \neq \pm p_1$ and $\tau(n) \neq p_2^d$ with $d \in \mathbb{Z}_+$. Thus, $s = 1$, there must be an odd prime p and $a \in 2\mathbb{Z}_+$ such that $n = p^a$. $\square$

Lemma 4.2 *If the equation*

$$\tau(p^a) = \pm p_1 p_2^b, \quad (49)$$

has a solution, where $3 \leq p_1, p_2 \leq 31$ are primes such that $p_1 p_2 \leq 247$, $p_1 \neq p_2$, $\max\{p_1, p_2\} \geq 13$, and $b \in \mathbb{Z}_+$, $a \in 2\mathbb{Z}_+$. Then (p_1, p_2, a) have to be inside Table 2.

Proof Suppose (p, b) is a solution of the Eq. (49).

First, we show that $\{1, \tau(p), \tau(p^2) \cdots\}$ forms a Lucas sequence. Observe that

$$\frac{\alpha}{\beta} + \frac{\beta}{\alpha} + 2 = \frac{\tau(p)^2}{p^{11}}.$$

By Deligne's bound ([6], [7]), we have $|\tau(p)| \leq 2p^{\frac{11}{2}}$. Together with the fact that $\tau(2)^2/2^{11} = -9/32$ and $\tau(3)^2/3^{11} = 784/2187$ aren't integers, we know the rational number $\tau(p^2)/p^{11}$ is not an integer and therefore not an algebraic integer. It follows that α/β is not a root of unity. Then by the definition of Lucas sequence and Proposition 2.4 (iii), it suffices to show $p \nmid \tau(p)$. Indeed, if $p \mid \tau(p)$, then by Proposition 2.4 (ii), we have $p^a \mid \tau(p^a)$, which means $p^a \mid \pm p_1 p_2^b$. Together with $a \in 2\mathbb{Z}_+$, $p = p_2$ follows.

If $11 \leq p_2 \leq 31$, we have $p_2 \nmid \tau(p_2)$, which gives a contradiction.

If $3 \leq p_2 \leq 7$, consider

$$\tau(p^a) = \pm p_1 p^b, \quad (50)$$

where prime $13 \leq p_1 \leq 31$ and $p = p_2$. Let $r_p = \text{ord}_p(\tau(p))$, which indicates the maximum order that p can divide $\tau(p)$, and let

$$\begin{cases} \gamma = \frac{\alpha}{p^{r_p}} \\ \delta = \frac{\beta}{p^{r_p}} \end{cases}$$

Table 3 The possible values of p_1 and a

p_1	13	17	19	23	29	31
a	2	2	2, 4	2, 10	2, 4	2, 4

Then we have $(\gamma + \delta, \gamma\delta) = 1$ and γ/δ is not a root of unity, where (α, β) is defined in Proposition 2.4 (iii). So we claim (γ, δ) is a Lucas pair. Using u_n to represent the Lucas sequence, we have

$$u_n = \frac{\tau(p^{n-1})}{p^{r_p(n-1)}}.$$

Therefore we have $u_n \mid \tau(p^{n-1})$ and $p \nmid u_n$, for all $n \in \mathbb{Z}_+$. Through calculation, we have $r_3 = 2$, $r_5 = 1$ and $r_7 = 1$. Hence we obtain the following results:

$$\begin{cases} p = 3 : u_{a+1} = \frac{\pm p_1 \times 3^b}{3^{2a}} = \pm p_1 \text{ and } b = 2a \\ p = 5 : u_{a+1} = \frac{\pm p_1 \times 5^b}{5^a} = \pm p_1 \text{ and } b = a \\ p = 7 : u_{a+1} = \frac{\pm p_1 \times 7^b}{7^a} = \pm p_1 \text{ and } b = a. \end{cases}$$

For this Lucas sequence, by Proposition 2.3 we know that when $a + 1 \geq 5$, u_{a+1} has a primitive divisor p_1 . That is, $p_1 \mid u_{a+1}$ and $p_1 \nmid (\gamma - \delta)^2 u_1 u_2 \cdots u_a$, which gives $p_1 \nmid (\gamma - \delta)^2$. So by (5), $m_{p_1} = a + 1 > 2$. Thus by Proposition 2.2 we have

$$a + 1 \mid (p_1 - 1)(p_1 + 1).$$

Besides, we claim $a + 1$ is an odd prime. Indeed, if there is an odd prime λ such that $\lambda \mid a + 1$ and $\lambda < a + 1$, then by Proposition 2.1 we have $u_\lambda \mid u_{a+1}$, that is, $\tau(p^{\lambda-1}) \mid \pm p_1 p^b$. So we have

$$u_\lambda = \tau(p^{\lambda-1}) = \pm p_1 p^m, \quad (51)$$

where $1 \leq m \leq b$. However, by $3 \leq \lambda < a + 1$, we know that (51) is contradictory to the fact that p_1 is primitive divisor of u_{a+1} . So $a + 1$ is an odd prime. What's more, from (2), we know that $a \neq 6$. Then, we only need to consider whether the Eq. (50) has a solution when $p = 3, 5, 7$, and Table 3 lists the possible values of p_1 and a . By calculation, we find that for all p_1 and a in Table 3, the Eq. (50) has no solution.

Therefore, we have $p \nmid \tau(p)$ and $\{1, \tau(p), \tau(p^2) \cdots\}$ forms a Lucas sequence.

Secondly, we discuss the specific values of a . By (2), we have $a \neq 6$. By Proposition 2.3, if $a \geq 4$, u_{a+1} must have a primitive divisor. By the definition of primitive divisor, we know primitive divisors of u_{a+1} must be p_1 or p_2 . Suppose p_1 is a primitive divisor of u_{a+1} , then we have $p_1 \mid u_{a+1}$ and

$$p_1 \nmid (\alpha - \beta)^2 u_1 u_2 \cdots u_a.$$

Thus, we have $p_1 \nmid (\alpha - \beta)^2$. It's easy to see $m_{p_1} = a + 1 > 2$. Then by Proposition 2.2 we get

$$a + 1 \mid (p_1 - 1)(p_1 + 1).$$

If p_2 is a primitive divisor of u_{a+1} , by similar argument, we obtain

$$a + 1 \mid (p_2 - 1)(p_2 + 1).$$

Besides, by similar argument of the previous proof, we can obtain $a + 1$ must be an odd prime. Through easy calculation, we get the Table 2. $\square$

Proof of Theorem 1.1. With Lemmas 4.1 and 4.2, it suffices to deal with the cases listed in Table 2. That's to say, we only need to show

(1) $\tau(p^2) = \pm p_1 p_2^b$ has no solution in prime p , $b \in \mathbb{Z}_+$, and (p_1, p_2) taken from row 2, 3 and 4 of Table 2.

(2) $\tau(p^4) = \pm p_1 p_2^b$ has no solution in prime p , $b \in \mathbb{Z}_+$, and (p_1, p_2) taken from row 3 of Table 2.

(3) $\tau(p^{10}) = \pm p_1 p_2^b$ has no solution in prime p , $b \in \mathbb{Z}_+$, and (p_1, p_2) taken from row 4 of Table 2.

By Propositions 3.1, 3.2 and 3.3, it's not hard to see (1), (2) and (3) hold. Thus we get Theorem 1.1. $\square$

5 Proof of Corollary 1.2 and 1.3

5.1 Proof of Corollary 1.2

We study the equation case by case.

If $b_i = 0$ for $i = 1, 2, 3, 4$ in the equation $\tau(n) = 3^{b_1} 5^{b_2} 7^{b_3} 11^{b_4} 13^b$, it turns to be $\tau(n) = 13^b$, where $n, b \in \mathbb{Z}$ and $n > 1$. Then by Theorem 6 of [3], we know it has no solution.

If $\exists i$ such that $b_i = 1$, Theorem 1.1 tells us that the Eq. (4) has no solution directly.

If there are two non-zero numbers in $\{b_1, b_2, b_3, b_4\}$, equation $\tau(n) = 3^{b_1} 5^{b_2} 7^{b_3} 11^{b_4} 13^b$ turns to be $\tau(n) = l_1 l_2 \cdot 13^b$, where $l_1, l_2 \in \{3, 5, 7, 11\}$ and $l_1 \neq l_2$. As we know $\tau(n) \neq l_1, 13^b, l_1 l_2, l_1 \cdot 13^b$, together with the fact that $\tau(q_1^{a_1} q_2^{a_2} \cdots q_s^{a_s}) = \tau(q_1^{a_1}) \tau(q_2^{a_2}) \cdots \tau(q_s^{a_s})$, where $a_i, s \in \mathbb{Z}_{\geq 0}$ and $q_i, 1 \leq i \leq s$ are different primes, it suffices to prove the equation

$$\tau(p^a) = l_1 l_2 \cdot 13^b \quad (52)$$

has no solution, where $l_1, l_2 \in \{3, 5, 7, 11\}$ and $l_1 < l_2$. Apply similar argument as the proof of Lemma 4.2, we obtain $a + 1 \neq 7$ is an odd prime dividing

$$\prod_{i=1}^2 (l_i - 1)(l_i + 1) \cdot (13 - 1)(13 + 1).$$

Table 4 The remaining values of a and congruences for the Eq. (52)

l_1	l_2	Remaining a and congruences for the Eq. (52)
3	5	$a = 2 : (\text{mod } 5)$
3, 5	7	$a = 2 : (\text{mod } 7)$
3	11	$a = 2 : (\text{mod } 9); a = 4 : (\text{mod } 3)$
5	11	$a = 2 : (\text{mod } 5); a = 4 : (\text{mod } 4)$
7	11	$a = 2 : (\text{mod } 7); a = 4 : (\text{mod } 7)$

By congruences of $\tau(n)$, we clear up the remaining a . For example, when $l_1 = 3, l_2 = 5$, only $a = 2$ remains, that's to say, when $a \neq 2$, the equation $\tau(p^a) = 3 \cdot 5 \cdot 13^b$ has no solution. Consider $\tau(p^2) = 3 \cdot 5 \cdot 13^b$, by calculation we know $p \neq 5$. Hence we have

$$\tau(p^2) \equiv p^{-60} \sigma_{71}(p^2) \not\equiv 0 (\text{mod } 5),$$

which says $\tau(p^2) = 3 \cdot 5 \cdot 13^b$ is impossible. Therefore, when $(l_1, l_2) = (3, 5)$, the Eq. (52) has no solution. By the same way, we deal with the rest part. Table 4 lists the remaining values of a for each case and some possible corresponding congruences to deal with them.

If $\exists! i$ such that $b_i = 0$, by similar arguments as before, it suffices to prove the equation

$$\tau(p^a) = l_1 l_2 l_3 \cdot 13^b \quad (53)$$

has no solution, where $l_1, l_2, l_3 \in \{3, 5, 7, 11\}$ and $l_1 < l_2 < l_3$. By congruence of modulo 7, we have

$$\begin{cases} \tau(p^a) \not\equiv 3 \cdot 5 \cdot 7 \cdot 13^b & a = 2 \\ \tau(p^a) \not\equiv 3 \cdot 7 \cdot 11 \cdot 13^b & a = 2, 4 \\ \tau(p^a) \not\equiv 5 \cdot 7 \cdot 11 \cdot 13^b & a = 2, 4. \end{cases}$$

And through the congruences of modulo 5 and 3, we get $\tau(p^2) \not\equiv 3 \cdot 5 \cdot 11 \cdot 13^b$ and $\tau(p^4) \not\equiv 3 \cdot 5 \cdot 11 \cdot 13^b$ respectively. Knowing that the Eq. (53) has no solution except for when $a + 1 \neq 7$ is an odd prime dividing

$$\prod_{i=1}^3 (l_i - 1)(l_i + 1) \cdot (13 - 1)(13 + 1),$$

we get the conclusion.

If $b_i = 1$ for $i = 1, 2, 3, 4$ in Eq. (4), applying the same method, we get $\tau(n) \neq 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13^b$ with the congruences of modulo 7.

5.2 Proof of Corollary 1.3

Similarly, we give a brief proof of Corollary 1.3.

Together with the previous results, it suffices to prove the equation

$$\tau(n) = m \quad (54)$$

has no solution, where $100 < |m| < 252$ is an odd integer and $n \in \mathbb{Z}_+$. By Theorem 1.1 and Corollary 1.2, when

$$m \in S := \{ \pm 105, \pm 115, \pm 117, \pm 119, \pm 121, \pm 125, \pm 133, \pm 135, \pm 143, \pm 145, \pm 147, \\ \pm 153, \pm 155, \pm 161, \pm 165, \pm 169, \pm 171, \pm 175, \pm 187, \pm 189, 195, \pm 203, \\ \pm 207, \pm 209, \pm 217, \pm 221, \pm 225, \pm 231, \pm 243, \pm 245, \pm 247 \},$$

the Eq. (54) has no solution. Thus we only need to show the Eq. (54) has no solution with $m \in \{m : 100 < |m| < 252, m \equiv 1 \pmod{2}\} \setminus S$. We use the congruences of $\tau(n)$, integer points on Thue equation, Lemmas 3.4 and 3.6 to deal with it.

Applying similar arguments as the proof of Lemma 4.1, it suffices to show the Eq. (54) has no solution when $n = p^a$. Again by the method in the proof of Lemma 4.2, when $6 \leq a \leq 40$, the equation $\tau(p^a) = m$ has no solution except for (m, a) are as follows:

$$(\pm 101, 16), (\pm 103, 12), (\pm 103, 16), (\pm 109, 10), (\pm 111, 18), (\pm 113, 6), (\pm 113, 18), \\ (\pm 123, 6), (\pm 127, 6), (\pm 129, 6), (\pm 129, 10), (\pm 131, 10), (\pm 131, 12), (\pm 137, 16), \\ (\pm 137, 22), (\pm 139, 6), (\pm 139, 22), (\pm 141, 22), (\pm 149, 36), (\pm 151, 18), (\pm 157, 12), \\ (\pm 159, 12), (\pm 163, 40), (\pm 167, 6), (\pm 173, 28), (\pm 177, 28), (\pm 181, 6), (\pm 181, 12), \\ (\pm 183, 30), (\pm 185, 18), (\pm 191, 18), (\pm 197, 6), (\pm 197, 10), (\pm 199, 10), (\pm 201, 10), \\ (\pm 201, 16), (\pm 205, 6), (\pm 211, 6), (\pm 213, 6), (\pm 215, 6), (\pm 215, 10), (\pm 219, 36), \\ (\pm 223, 6), (\pm 223, 36), (\pm 227, 18), (\pm 229, 18), (\pm 229, 22), (\pm 233, 12), (\pm 233, 28), \\ (\pm 235, 22), (\pm 237, 12), (\pm 239, 6), (\pm 239, 16), (\pm 241, 10), (\pm 249, 6), (\pm 249, 40), \\ (\pm 251, 6), (-195, 6).$$

For these pairs of (m, a) , by Lemma 3.8, we only need to solve the corresponding Thue equations (see [13] for the list). By calculation with PARI/GP [19] (see [13] for the PARI/GP code required), none of the solutions are of the form $(p^{11}, \tau(p)^2)$. Thus, when $n = p^a$ with $6 \leq a \leq 40$, the Eq. (54) has no solution.

Besides, when $m = -137, -139, -179, -227$, we show the Eq. (54) has no solution with Lemmas 3.4 and 3.6. By the previous proof, we only need to prove

$$\tau(p^a) = m \quad (55)$$

has no solution with $(m, a) = (-137, 2), (-139, 2), (-139, 4), (-179, 2), (-179, 4), (-179, 88), (-227, 2), (-227, 112)$. Applying congruences (10) and (9), we obtain that the Eq. (55) has no solution with $(-139, 2), (-179, 2)$ and $(-179, 88)$,

$(-227, 112)$ respectively. Calculating with SageMath and LMFDB, we get $H_1(f)$ and $H_3(f)$ are empty for all weight 2 newform f of level $N' = 2^5 \times 1 \times 137$, $2^5 \times 1 \times 227$, $2^3 \times 5 \times 1 \times 139$ and $2^3 \times 5 \times 1 \times 179$. Therefore, Lemmas 3.4 and 3.6 tell us that the Eq. (55) has no solution with $(-137, 2)$, $(-227, 2)$ and $(-139, 4)$, $(-179, 4)$ respectively.

Finally, when $m \neq -137, -139, -179, -227$, Table 6 in the Appendix lists the remaining possible values of a with $a = 2, 4$ or $a > 40$ corresponding to different m . By congruences of $\tau(n)$, we can have them cleaned up. Some possible corresponding congruences of $\tau(n)$ to deal with them are also listed in Table 6 in the Appendix.

Appendix

See Tables 5 and 6.

Table 5 All nonempty sets $H_j(f)$

Case	k	p_2	Nonempty $H_j(f)$, $j = 1$ or 3
$\tau(p^2) \mid 11 \mid b$	3	13, 17, 19, 23	$H_1(f) = \{0, 44, 88, 132, 176, 220, 264, 308, 352\}$
$\tau(p^2) \mid 11 \mid b$	3	29, 31	$H_1(f) = \{0, 22, 44, 66, 88, 110, 132, 154, 176, 198, 220, 242, 264, 286, 308, 330, 352, 374\}$
$\tau(p^2) \mid 11 \mid b$	-3	19	$H_1(f) = \{11, 33, 55, 77, 99, 121, 143, 165, 187, 209, 231, 253, 275, 297, 319, 341, 363, 385\}$
$\tau(p^2) \mid 11 \nmid b$	13	5	$H_3(f) = \{2, 24, 46, 68, 90, 112, 134, 156, 178, 200, 222, 244, 266, 288, 310, 332, 354, 376\}$
$\tau(p^2) \mid 11 \nmid b$	-5	23	$H_1(f) = \{2, 4, 6, 8, 10, 18, 20, 24, 26, 28, 30, 32, 40, 42, 46, 48, 50, 52, 54, 62, 64, 68, 70, 72, 74, 76, 84, 86, 90, 92, 94, 96, 98, 106, 108, 112, 114, 116, 118, 120, 128, 130, 134, 136, 138, 140, 142, 150, 152, 156, 158, 160, 162, 164, 172, 174, 178, 180, 182, 184, 186, 194, 196, 200, 202, 204, 206, 208, 216, 218, 222, 224, 226, 228, 230, 238, 240, 244, 246, 248, 250, 252, 260, 262, 266, 268, 270, 272, 274, 282, 284, 288, 290, 292, 294, 296, 304, 306, 310, 312, 314, 316, 318, 326, 328, 332, 334, 336, 338, 340, 348, 350, 354, 356, 358, 360, 362, 370, 372, 376, 378, 380, 382, 384, 392, 394\}$
$\tau(p^4) \mid 11 \mid b$	5	19, 29, 31	$H_1(f) = \{0, 22, 44, 66, 88, 110, 132, 154, 176, 198, 220, 242, 264, 286, 308, 330, 352, 374\}$
$\tau(p^4) \mid 11 \nmid b$	5	29	$H_1(f) = \{25, 69, 113, 157, 201, 245, 289, 333, 377\}$ $H_3(f) = \{3, 47, 91, 135, 179, 223, 267, 311, 355\}$
$\tau(p^4) \mid 11 \nmid b$	11	19	$H_1(f) = \{17, 61, 105, 149, 193, 237, 281, 325, 369\}$
$\tau(p^4) \mid 11 \nmid b$	-19	7	$H_1(f) = \{16, 60, 104, 148, 192, 236, 280, 324, 368\}$
$\tau(p^4) \mid 11 \nmid b$	-31	7	$H_3(f) = \{20, 64, 108, 152, 196, 240, 284, 328, 372\}$

Table 6 The values of m , a and the congruences for $\tau(p^a) \neq m$

m	a and congruences for $\tau(p^a) \neq m$
$\pm 101, \pm 109, \pm 123, \pm 131, \pm 151,$ $\pm 177, 181, \pm 191, \pm 213, \pm 241,$ $\pm 251, -149, -199, -239$	$a = 2 : (\text{mod } 23); a = 4 : (\text{mod } 23)$
$\pm 103, \pm 111, \pm 113, \pm 127, \pm 129,$ $\pm 159, \pm 163, \pm 197, \pm 201, \pm 219,$ $\pm 223, \pm 237, \pm 249, -141, -185,$ $-205, -215, -233, -235$	$a = 2 : (\text{mod } 23)$
107	$a = 2 : (\text{mod } 3); a = 52 : (\text{mod } 8)$
137, 233	$a = 2 : (\text{mod } 3)$
139, 149, 199, 229, 239	$a = 2 : (\text{mod } 5); a = 4 : (\text{mod } 5)$
141	$a = 2 : (\text{mod } 9)$
± 157	$a = 2 : (\text{mod } 23); a = 78 : (\text{mod } 7)$
167	$a = 2 : (\text{mod } 3); a = 82 : (\text{mod } 25)$
173	$a = 2 : (\text{mod } 3); a = 42 : (\text{mod } 3)$
179	$a = 2 : (\text{mod } 3); a = 4 : (\text{mod } 5); a = 88 : (\text{mod } 8)$
183	$a = 2 : (\text{mod } 23); a = 4 : (\text{mod } 3)$
185, 205, 215, 235, -195	$a = 2 : (\text{mod } 5)$
193	$a = 2 : (\text{mod } 3); a = 96 : (\text{mod } 5)$
211	$a = 2 : (\text{mod } 23); a = 4 : (\text{mod } 23); a = 52 : (\text{mod } 8)$
227	$a = 2 : (\text{mod } 3); a = 112 : (\text{mod } 7)$
-107	$a = 2 : (\text{mod } 23); a = 52 : (\text{mod } 7)$
-167	$a = 2 : (\text{mod } 23); a = 82 : (\text{mod } 23)$
-173	$a = 2 : (\text{mod } 23); a = 42 : (\text{mod } 7)$
-181	$a = 2 : (\text{mod } 3); a = 4 : (\text{mod } 5)$
-183	$a = 2 : (\text{mod } 9); a = 4 : (\text{mod } 3)$
-193	$a = 2 : (\text{mod } 23); a = 96 : (\text{mod } 3)$
-211	$a = 2 : (\text{mod } 23); a = 4 : (\text{mod } 23); a = 52 : (\text{mod } 5)$
-229	$a = 2 : (\text{mod } 3); a = 4 : (\text{mod } 4)$

References

1. Balakrishnan, J.S., Craig, W., Ono, K., Tsai, W.L.: Variants of Lehmer's speculation for newforms (2020). arXiv preprint [arXiv:2005.10354](https://arxiv.org/abs/2005.10354)
2. Balakrishnan, J.S., Ono, K., Tsai, W.-L.: Even values of Ramanujan's tau-function. *Matematica* **1**(2), 395–403 (2022)
3. Bennett, M., Gherga, A., Patel, V., Siksek, S.: Odd values of the Ramanujan tau function. *Math. Ann.* **382**(1–2), 203–238 (2022)
4. Bennett, M.A., Skinner, C.M.: Ternary Diophantine equations via Galois representations and modular forms. *Can. J. Math.* **56**(1), 23–54 (2004)
5. Bilu, Y., Hanrot, G., Voutier, P.M.: Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.* **539**, 75–122 (2001)
6. Deligne, P.: La conjecture de Weil. I. *Publ. Math. de IHES* **43**, 273–307 (1974)
7. Deligne, P.: La conjecture de Weil. II. *Publ. Math. de IHES* **52**, 137–252 (1980)

8. Dembner, S., Jain, V.: Hyperelliptic curves and newform coefficients. *J. Number Theory* **225**, 214–239 (2021)
9. Hanada, M., Madhukara, R.: Fourier coefficients of level 1 Hecke Eigenforms. *Acta Arith.* **200**(4), 371–388 (2021)
10. Kraus, A., Oesterlé, J.: Sur une question de B. Mazur. *Math. Ann.* **293**(2), 259–275 (1992)
11. Lakein, K., Larsen, A.: Some remarks on small values of $\tau(n)$. *Arch. Math. (Basel)* **117**(6), 635–645 (2021)
12. Lehmer, D.H.: The vanishing of Ramanujan's function $\tau(n)$. *Duke Math. J.* **14**, 429–433 (1947)
13. Lin, W., Ma, W.: Sage and PARI/GP code. <https://github.com/LinWenwen1/tau-function>
14. Lygeros, N., Rozier, O.: Odd prime values of the Ramanujan Tau function. *Ramanujan J.* **32**(2), 269–280 (2013)
15. Murty, M.R., Murty, V.K., Shorey, T.N.: Odd values of the Ramanujan τ -function. *Bull. Soc. Math. France* **115**(3), 391–395 (1987)
16. Ribet, K.: From the Taniyama-Shimura conjecture to Fermat's last theorem. *Ann. Fac. Sci. Toulouse Math.* **11**(1), 116–139 (1990)
17. Swinnerton-Dyer, H.P.F., On ℓ -adic representations and congruences for coefficients of modular forms. In: *Modular functions of one variable, III* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp,; Lecture Notes in Math., vol. 350, pp. 1–55. Springer, Berlin 1973 (1972)
18. The LMFDB Collaboration, The L-functions and modular forms database (2023). <http://www.lmfdb.org>
19. The PARI Group, PARI/GP version 2.13.4, Univ. Bordeaux (2023). <http://pari.math.u-bordeaux.fr/>
20. The Sage Developers, SageMath, the Sage Mathematics Software System (Version 9.7) (2023). <https://www.sagemath.org>
21. Wiles, A.: Modular elliptic curves and Fermat's last theorem. *Ann. Math.* **141**(3), 443–551 (1995)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.