Mathematische Annalen (2022) 382:203–238
https://doi.org/10.1007/s00208-021-02241-3

Mathematische Annalen

Odd values of the Ramanujan tau function

Michael A. Bennett[1] · Adela Gherga[2] · Vandita Patel[3] · Samir Siksek[2]

Received: 15 January 2021 / Revised: 9 July 2021 / Accepted: 11 July 2021 /
Published online: 9 August 2021

Abstract
We prove a number of results regarding odd values of the Ramanujan τ-function. For example, we prove the existence of an effectively computable positive constant κ such that if $\tau(n)$ is odd and $n \geq 25$ then either

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

or there exists a prime $p \mid n$ with $\tau(p) = 0$. Here $P(m)$ denotes the largest prime factor of m. We also solve the equation $\tau(n) = \pm 3^{b_1} 5^{b_2} 7^{b_3} 11^{b_4}$ and the equations $\tau(n) = \pm q^b$ where $3 \leq q < 100$ is prime and the exponents are arbitrary nonnegative integers. We make use of a variety of methods, including the Primitive Divisor Theorem of Bilu, Hanrot and Voutier, bounds for solutions to Thue–Mahler equations due to Bugeaud and Győry, and the modular approach via Galois representations of Frey–Hellegouarch elliptic curves.

Communicated by Kannan Soundararajan.

Michael A. Bennett is supported by NSERC. Adela Gherga and Samir Siksek are supported by an EPSRC Grant EP/S031537/1 "Moduli of elliptic curves and classical Diophantine problems".

✉ Michael A. Bennett
bennett@math.ubc.ca

Adela Gherga
Adela.Gherga@warwick.ac.uk

Vandita Patel
vandita.patel@manchester.ac.uk

Samir Siksek
S.Siksek@warwick.ac.uk

[1] Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada

[2] Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK

[3] Department of Mathematics, University of Manchester, Manchester M13 9PL, UK

Mathematics Subject Classification Primary 11D61 · Secondary 11D41 · 11F80 · 11F41

1 Introduction

The *Ramanujan τ-function* $\tau(n)$ is defined via the expansion

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n, \quad q = e^{2\pi iz}. \tag{1}$$

It was conjectured by Ramanujan [33] and proved by Mordell [29] that $\tau(n)$ is a multiplicative function, i.e. that

$$\tau(n_1n_2) = \tau(n_1)\tau(n_2),$$

for all coprime pairs of positive integers n_1 and n_2. Further, we have

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

via Jacobi's triple product formula, whence $\tau(n)$ is odd precisely when n is an odd square and, in particular, $\tau(p)$ is even for every prime p.

Amongst the many open questions about the possible values of $\tau(n)$, the most notorious is a conjecture of Lehmer [20] to the effect that $\tau(n)$ never vanishes. In terms of the size of values of τ, one has the upper bound of Deligne [14] (originally conjectured by Ramanujan) :

$$|\tau(p)| \leq 2\cdot p^{11/2}, \tag{2}$$

valid for prime p. In the other direction, Atkin and Serre [34] conjectured (as a strengthening of Lehmer's conjecture) that, for $\epsilon > 0$,

$$|\tau(p)| \gg_{\epsilon} p^{9/2-\epsilon},$$

so that, in particular, given a fixed integer a, there are at most finitely many primes p for which $\tau(p) = a$. While this problem remains open, in the special case where the integer a is odd, Murty et al. [32] proved that the equation

$$\tau(n) = a, \tag{3}$$

has at most finitely many solutions in integers n (note that, in this case, n is necessarily an odd square). More precisely, they demonstrated the existence of an effectively computable positive constant c such that if $\tau(n)$ is odd, then

$$|\tau(n)| > (\log(n))^c.$$

A number of recent papers have treated the problem of explicitly demonstrating that equation (3) has, in fact, no solutions, for various odd values of a, including $a = \pm 1$ (Lygeros and Rozier [27]), $|a| < 100$ an odd prime (Balakrishnan et al. [1], Balakrishnan et al. [2], Dembner and Jain [15]), and $|a| < 100$ an odd integer (Hanada and Madhukara [18]).

In this paper, we derive what might be considered a non-Archimedean analogue of the work of Murty et al. Let us define $P(m)$ to be the greatest prime factor of an integer $|m| > 1$. We prove the following.

Theorem 1 *There exists an effectively computable constant $\kappa > 0$ such that if $\tau(n)$ is odd, with $n \geq 25$, then either*

$$P(\tau(n)) \ > \ \kappa \cdot \frac{\log\log\log n}{\log\log\log\log n}, \tag{4}$$

or there exists a prime $p \mid n$ for which $\tau(p) = 0$.

Recall that a *powerful number* (also known as *squarefull* or 2-*full*) is defined to be an integer n with the property that if a prime $p \mid n$, then necessarily $p^2 \mid n$. Equivalently, we can write such an integer as $n = a^2b^3$, where a and b are integers. Our techniques actually show the following (from which Theorem 1 is an immediate consequence).

Theorem 2 *We have*

$$\lim_{n\to\infty} P(\tau(n)) = \infty,$$

where the limit is taken over powerful numbers n for which $\tau(p) \neq 0$ for each $p \mid n$. More precisely, there exists an effectively computable constant $\kappa > 0$ such that if $n \geq 25$ is powerful, either

$$P(\tau(n)) \ > \ \kappa \cdot \frac{\log\log\log n}{\log\log\log\log n} \tag{5}$$

or there exists a prime $p \mid n$ for which $\tau(p) = 0$.

The restriction that n has no prime divisors p for which $\tau(p) = 0$ is, in fact, necessary if one wishes to obtain a lower bound upon $P(\tau(n))$ that tends to ∞ with n. Indeed, one may observe that, if $\tau(p) = 0$, then (see (18) below)

$$P\left(\tau(p^{2k})\right) = P\left((-1)^k p^{11k}\right) = p$$

is bounded independently of k. While Lehmer's conjecture remains unproven, we do know that if there is a prime p for which $\tau(p) = 0$, then

$$p > 816212624008487344127999, \tag{6}$$

by work of Derickx, van Hoeij and Zeng [16].

Theorem 3 *There is a computable positive constant η such that for any prime p with $\tau(p) \neq 0$ and any $m \geq 2$,*

$$P(\tau(p^m)) \ > \ \eta \cdot \frac{\log\log(p^m)}{\log\log\log(p^m)}. \tag{7}$$

We note that Theorem 3 implies Theorem 2. Indeed, let n be a powerful number and p^m be the largest prime power divisor of n. Then $m \geq 2$, and $p^m \gg \log n$, whence (5) follows immediately from (8). Our arguments show the following.

Theorem 4 *Let $m \geq 2$. There is a computable positive constant $\delta(m)$, depending only on m, such that for any prime p with $\tau(p) \neq 0$,*

$$P(\tau(p^m)) \ > \ \delta(m) \cdot \log\log(p). \tag{8}$$

We note that our bounds neither imply nor are implied by work of Luca and Shparlinski [25] who proved that

$$P\left(\tau(p)\tau(p^2)\tau(p^3)\right) \gg \frac{\log\log(p)\log\log\log(p)}{\log\log\log\log(p)}.$$

To demonstrate that these results and the techniques underlying them are somewhat practical, we prove the following computational "coda", solving equation (3) where the prime divisors of a, rather than a itself, are fixed.

Theorem 5 *If n is a powerful positive integer, then either $n = 8$, where we have*

$$\tau(8) = 2^9 \cdot 3 \cdot 5 \cdot 11,$$

or

$$P(\tau(n)) \geq 13.$$

Corollary 1.1 *If n is a positive integer for which $\tau(n)$ is odd, then*

$$P(\tau(n)) \geq 13. \tag{9}$$

In other words, the equation

$$\tau(n) = \pm 3^\alpha 5^\beta 7^\gamma 11^\delta \tag{10}$$

has no solutions in integers $n \geq 2$ and $\alpha, \beta, \gamma, \delta \geq 0$.

It is conjectured that $|\tau(n)|$ takes on infinitely many prime values, the smallest of which corresponds to

$$\tau(251^2) = -80561663527802406257321747.$$

Our arguments enable us to eliminate the possibility of powers of small primes arising as values of τ. By way of example, we have the following.

Theorem 6 *The equation*

$$\tau(n) = \pm q^{\alpha}$$

has no solutions in prime q with $3 \leq q < 100$, and $\alpha \geq 0$, $n \geq 2$ integers.

It is worth observing that the techniques we employ here are readily extended to treat more generally coefficients $\lambda_f(n)$ of cuspidal newforms of (even) weight $k \geq 4$ for $\Gamma_0(N)$, with trivial character and $\lambda_f(p)$ even for suitably large prime p; our results correspond to the case of $\Delta(z)$ in (1), where $k = 12$ and $N = 1$. For simplicity, we will restrict our attention to $\tau(n)$ and $\Delta(z)$; readers interested in the more general situation should consult the paper of Murty and Murty [31] (see also [2]).

We should also comment on the particular choice of the constant "13" on the right hand side of inequality (9) in Corollary 1.1 (and analogously in Theorem 5). As we shall observe, the weaker result with 13 replaced by 11 (corresponding to equation (10) with $\delta = 0$) reduces via local arguments to the resolution of a single Thue equation; this is the content of Proposition 6 of Luca et al. [24]. Corollary 1.1 as stated requires (apparently at least) the full use of our various techniques, including the Primitive Divisor Theorem, solution of a variety of Thue–Mahler equations, and resolution of hyperelliptic equations through appeal to the modularity of Galois representations attached to Frey–Hellegouarch elliptic curves. A stronger version of Corollary 1.1 with 13 replaced by 17 in (9) is possibly within range of this approach, though computationally significantly more involved. An analogous result with 13 replaced by 19 would likely require fundamentally new ideas.

This paper is organized as follows. In Sect. 2, we recall some standard congruences for the Ramanujan-tau function that we use later in the paper. In Sect. 3, we connect the sequence $m \mapsto \tau(p^{m-1})$, for a fixed prime p, to a Lucas sequence $\{u_m\}$, allowing us to appeal to the Primitive Divisor Theorem of Bilu et al. In Sect. 4, we introduce a sequence of homogenous polynomials $\Psi_m(X, Y) \in \mathbb{Z}[X, Y]$ that are intimately connected to the $\{u_m\}$. We will use these polynomials in Sect. 5, together with a theorem of Bugeaud on prime divisors of $ax^u + by^v$, to prove Theorem 4. In Sect. 6, we relate the equation $\tau(p^m) = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_1}$ to a Thue–Mahler equation, whence a theorem of Bugeaud and Győry enables us to deduce Theorem 3. In Sects. 7, 8 and 9 , we solve the equations $\tau(p^k) = \pm q^b$ where $k \in \{2, 4\}$, p and q are prime, and $3 \leq b < 100$, and also the equations $\tau(p^k) = \pm 3^{b_1} 5^{b_2} 7^{b_3} 11^{b_4}$, where $2 \leq k \leq 4$ and p is prime. Our method in Sects. 7, 8 and 9 is to associate to a hypothetical solution a Frey–Hellegouarch curve and relate this to a weight 2 modular form of small level, using recipes of the first author and Skinner which in turn builds on the modularity of elliptic curves due to Wiles, Breuil, Conrad Diamond and Taylor, and on Ribet's Level-Lowering Theorem. In Sect. 10, we prove Theorem 5, by combining the results of Sects. 7, 8 and 9 , and using the Primitive Divisor Theorem. Finally, in Sect. 11, we prove Theorem 6; the results of previous sections allow us to reduce the equation $\tau(n) = \pm q^a$ with $3 \leq q < 100$ prime to Thue–Mahler equations of high degree,

which are then solved using an algorithm of the second and fourth author, von Känel and Matschke.

2 Congruences for the τ function

For future use, it will be of value for us to record some basic arithmetic facts about $\tau(n)$; these are taken from Swinnerton–Dyer's article [38]. Here $\sigma_v(n)$ denotes the sum of the v-th powers of the divisors of n.

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

$$\tau(n) \equiv n^{-610} \cdot \sigma_{1231}(n) \begin{cases} \mod 3^6 & \text{if } n \equiv 1 \mod 3 \\ \mod 3^7 & \text{if } n \equiv 2 \mod 3 \end{cases} \tag{12}$$

$$\tau(n) \equiv n^{-30}\sigma_{71}(n) \mod 5^3 \quad \text{if } 5 \nmid n \tag{13}$$

$$\tau(n) \equiv n \cdot \sigma_9(n) \begin{cases} \mod 7 & \text{if } n \equiv 0,\ 1,\ 2 \text{ or } 4 \mod 7 \\ \mod 7^2 & \text{if } n \equiv 3,\ 5 \text{ or } 6 \mod 7 \end{cases} \tag{14}$$

$$\begin{cases} \tau(p) \equiv 0 \mod 23 & \text{if } p \text{is a quadratic non-residue mod } 23 \\ \tau(p) \equiv 2 \mod 23 & \text{if } p = u^2 + 23v^2 \text{ with } u \neq 0 \\ \tau(p) \equiv -1 \mod 23 & \text{for other } p \neq 23 \end{cases} \tag{15}$$

$$\tau(n) \equiv \sigma_{11}(n) \mod 691. \tag{16}$$

Lemma 2.1 *Let $p \neq 7$ be a prime. Then $7 \nmid \tau(p^2)$.*

Proof Suppose $7 \mid \tau(p^2)$. Then by (14)

$$p^{18} + p^9 + 1 \equiv 0 \mod 7.$$

But $p^{18} = (p^6)^3 \equiv 1$ and $p^9 \equiv p^3 \equiv \pm 1 \mod 7$ giving a contradiction. □

Lemma 2.2 *Let $p \neq 5$ be a prime. Then $5 \nmid \tau(p^2)$.*

Proof Suppose $5 \mid \tau(p^2)$. Then by (13)

$$(p^{71})^2 + p^{71} + 1 \equiv 0 \mod 5.$$

However, this contradicts the fact that the congruence $x^2 + x + 1 \equiv 0 \mod 5$ has no solutions. □

Lemma 2.3 *Let $p \neq 3$ be a prime. Then $9 \nmid \tau(p^2)$.*

Proof Suppose $9 \mid \tau(p^2)$. Then by (12)

$$(p^{1231})^2 + p^{1231} + 1 \equiv 0 \mod 9.$$

Since the congruence $x^2 + x + 1 \equiv 0 \mod 9$ has no solutions, we obtain the desired contradiction. □

3 Lucas sequences

In this section, for a fixed prime p with $\tau(p) \neq 0$, we show that the sequence $m \mapsto \tau(p^{m-1})$ can be appropriately scaled to yield a Lucas sequence. We begin by introducing Lucas sequences and recalling some of their properties, mostly following the article of Bilu et al. [7].

A **Lucas pair** is a pair (α, β) of algebraic numbers such that $\alpha + \beta$ and $\alpha\beta$ are non-zero coprime rational integers, and α/β is not a root of unity. In particular, associated to the Lucas pair (α, β) is a **characteristic polynomial**

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

This polynomial has discriminant $D = (\alpha - \beta)^2 \in \mathbb{Z}\backslash\{0\}$. Given a Lucas pair (α, β), the corresponding **Lucas sequence** is given by

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad n = 0, 1, 2, \ldots .$$

Let (α, β) be a Lucas pair. A prime ℓ is a **primitive divisor** of the n-th term of the corresponding Lucas sequence if ℓ divides u_n but ℓ fails to divide $(\alpha - \beta)^2 \cdot u_1 u_2 \ldots u_{n-1}$. We shall make essential use of the celebrated Primitive Divisor Theorem of Biluet al. [7].

Theorem 7 (Bilu et al.) *Let (α, β) be a Lucas pair. If $n \geq 5$ and $n \neq 6$ then u_n has a primitive divisor.*

Let ℓ be a prime. The smallest positive integer m such that $\ell \mid u_m$ is called the **rank of apparition of** ℓ; we denote this by m_ℓ. We shall also have need of the following classical theorem of Carmichael [12].

Theorem 8 (Carmichael) *Let (α, β) be a Lucas pair and ℓ be a prime.*

(i) *If $\ell \mid \alpha\beta$ then $\ell \nmid u_m$ for all positive integers m.*
(ii) *Suppose $\ell \nmid \alpha\beta$. Write $D = (\alpha - \beta)^2 \in \mathbb{Z}$.*

(a) *If $\ell \neq 2$ and $\ell \mid D$, then $m_\ell = \ell$.*
(b) *If $\ell \neq 2$ and $\left(\frac{D}{\ell}\right) = 1$, then $m_\ell \mid (\ell - 1)$.*
(c) *If $\ell \neq 2$ and $\left(\frac{D}{\ell}\right) = -1$, then $m_\ell \mid (\ell + 1)$.*
(d) *If $\ell = 2$, then $m_\ell = 2$ or 3.*

(iii) *If* $\ell \nmid \alpha\beta$ *then*

$$\ell \mid u_m \iff m_\ell \mid m.$$

Proof Note that the sequence $\{u_n\}$ satisfies the recurrence

$$u_{n+2} - (\alpha+\beta)u_{n+1} + \alpha\beta u_n = 0, \qquad u_0 = 0, \quad u_1 = 1.$$

If $\ell \mid \alpha\beta$ then $u_n \equiv (\alpha+\beta)^{n-1} \pmod{\ell}$ for all $n \geq 1$. Since $\alpha+\beta$ and $\alpha\beta$ are coprime, $\ell \nmid (\alpha+\beta)$ and so $\ell \nmid u_n$ for all $n \geq 1$.

Suppose now that $\ell \nmid \alpha\beta$. Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{D})$ and λ be a prime of $\mathcal{O}_K$ above ℓ. We first consider (a). Here $\alpha = \beta + \gamma$ where $\lambda \mid \gamma$. Thus

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{(\beta+\gamma)^n - \beta^n}{\gamma} \equiv n\beta^{n-1} \pmod{\lambda}.$$

Thus $\ell \mid u_n$ if and only if $\ell \mid n$.

Next we consider cases (b) and (c) together. Note that

$$\ell \mid u_n \iff (\alpha/\beta)^n \equiv 1 \pmod{\lambda}.$$

Thus m_ℓ is equal to the multiplicative order of the image of α/β in $(\mathcal{O}_K/\lambda)^*$. If D is a quadratic residue modulo ℓ, then ℓ splits as a product of two degree 1 primes λ, λ' of $\mathcal{O}_K$. Thus $(\mathcal{O}_K/\lambda)^* \cong \mathbb{F}_\ell^*$ and so $m_\ell \mid (\ell-1)$. Finally we suppose D is a quadratic non-residue modulo ℓ. Then $\lambda = \ell\mathcal{O}_K$, and so the natural map $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{F}_\lambda/\mathbb{F}_\ell)$ is an isomorphism. Note that α and β are conjugates, and so $(\alpha/\beta)^\ell \equiv \beta/\alpha \pmod{\lambda}$. Thus $(\alpha/\beta)^{\ell+1} \equiv 1 \pmod{\lambda}$, whence $m_\ell \mid (\ell+1)$. The final part of the theorem is now also clear. □

Let us fix a prime p and consider the sequence

$$\left\{1, \tau(p), \tau(p^2), \tau(p^3), \ldots\right\}. \tag{17}$$

We will associate to this a Lucas pair and a corresponding Lucas sequence. Our starting point is the identity

$$\tau(p^m) = \tau(p)\tau(p^{m-1}) - p^{11}\tau(p^{m-2}), \tag{18}$$

valid for all integer $m \geq 2$. Once again, this was conjectured by Ramanujan [33] and proved by Mordell [29].

Let γ and δ be the roots of the quadratic equation

$$X^2 - \tau(p)X + p^{11} = 0,$$

so that

$$\gamma + \delta = \tau(p) \qquad \text{and} \qquad \gamma\delta = p^{11}.$$

Then

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

It follows from Deligne's bounds (2) that γ and δ are non-real Galois conjugates. From (18), we have

$$\tau(p^m) = \frac{\gamma^{m+1} - \delta^{m+1}}{\gamma - \delta}. \tag{19}$$

Lemma 3.1 *Suppose* $\tau(p) \neq 0$. *Then* $\mathrm{ord}_p(\tau(p)) \leq 5$.

Proof From (2), if $p^6 \mid \tau(p)$ and $\tau(p) \neq 0$, then necessarily $p \leq 3$. However,

$$\tau(2) = -2^3 \times 3 \quad \text{and} \quad \tau(3) = 2^2 \times 3^2 \times 7,$$

providing a contradiction and completing the proof. □

Lemma 3.2 *Suppose* $\tau(p) \neq 0$. *Then* γ/δ *is not a root of unity.*

Proof Observe that

$$\frac{\gamma}{\delta} + \frac{\delta}{\gamma} + 2 = \frac{\tau(p)^2}{p^{11}}.$$

By the previous lemma, the rational number $\tau(p)^2/p^{11}$ is not an integer and therefore not an algebraic integer. It follows that γ/δ is not a root of unity. □

The following is an immediate consequence of (19) and Lemma 3.2.

Lemma 3.3 *If* $\tau(p) = 0$ *then*

$$\tau(p^m) = \begin{cases} 0 & \text{if } m \text{ is odd,} \\ (-p^{11})^{m/2} & \text{if } m \text{ is even.} \end{cases}$$

If $\tau(p) \neq 0$ *then* $\tau(p^m) \neq 0$ *for all* $m \geq 1$.

Note that $\gcd(\gamma + \delta, \gamma\delta) = \gcd(\tau(p), p^{11}) = 1$ if and only if $p \nmid \tau(p)$. Thus the sequence $m \mapsto \tau(p^{m-1})$ is a Lucas sequence precisely when $p \nmid \tau(p)$. We note that $p \mid \tau(p)$ for

$$p = 2, 3, 5, 7, 2411, 7758337633, \ldots$$

We expect that $p \mid \tau(p)$ for infinitely many primes p; see Lygeros and Rozier [26] for a discussion of this problem and related computations. We will scale the pair (γ, δ) to obtain a Lucas pair, provided $\tau(p) \neq 0$.

Lemma 3.4 *Suppose* $\tau(p) \neq 0$. *Write* $r = \mathrm{ord}_p(\tau(p))$ *and let*

$$\alpha = \frac{\gamma}{p^r}, \qquad \beta = \frac{\delta}{p^r}.$$

Then (α, β) *is a Lucas pair. Denoting the corresponding Lucas sequence by* u_n, *we have*

$$u_n = \frac{\tau(p^{n-1})}{p^{r(n-1)}}, \qquad n \geq 1. \tag{20}$$

Moreover, $p \nmid u_n$ *for all* $n \geq 1$.

Proof Note that $\alpha + \beta = \tau(p)/p^r$ and $\alpha\beta = p^{11-2r}$ are coprime rational integers thanks to Lemma 3.1. The identity (20) follows immediately from (19). The last part is a consequence of part (i) of Theorem 8 since $p \mid \alpha\beta$.

For future reference, we note that, for $\{u_n\}$, we have

$$D = (\alpha - \beta)^2 = p^{-2r}\left(\tau^2(p) - 4p^{11}\right). \tag{21}$$

□

4 On three sequences of polynomials

We begin by defining, for $m \geq 0$, a sequence of polynomials $H_m(Z, W) \in \mathbb{Z}[Z, W]$

$$H_m(Z, W) = \begin{cases} (Z^m - W^m)/(Z - W) & \text{if } m \text{ is odd} \\ (Z^m - W^m)/(Z^2 - W^2) & \text{if } m \text{ is even.} \end{cases} \tag{22}$$

Let G be the group generated the involutions κ_1 and κ_2 on $\mathbb{Z}[Z, W]$ given by

$$\kappa_1 \ : \ \begin{cases} Z \mapsto -Z, \\ W \mapsto -W, \end{cases} \qquad \kappa_2 \ : \ \begin{cases} Z \mapsto W, \\ W \mapsto Z. \end{cases}$$

We compute the subring of invariants $\mathbb{Z}[Z, W]^G$.

Lemma 4.1 $\mathbb{Z}[Z, W]^G = \mathbb{Z}[ZW, (Z + W)^2]$.

Proof It is clear that $\mathbb{Z}[ZW, (Z + W)^2]$ belongs to the ring of invariants. Let $F \in \mathbb{Z}[Z, W]$ belong to the ring of invariants. We would like to show that $F \in \mathbb{Z}[ZW, (Z + W)^2]$. Observe that κ_1 and κ_2 send monomials to monomials and preserve the degree. Thus every homogenous component of F belongs to the ring of invariants, and we may suppose that F is homogeneous. As F is invariant under κ_1 it has even degree, $2n$ say, and we may write

$$F = \sum_{k=0}^{2n} a_k Z^{2n} W^{2n-k}.$$

As F is invariant under κ_2 we have $a_k = a_{2n-k}$ for $k = 0, \ldots, n$. Thus

$$F = a_0(Z^{2n} + W^{2n}) + a_1(ZW)(Z^{2n-2} + W^{2n-2}) + a_2(ZW)^2(Z^{2n-4} + W^{2n-4}) + \cdots + a_n(ZW)^n.$$

To complete the proof all we need to show is that $Z^{2n} + W^{2n} \in \mathbb{Z}[ZW, (Z+W)^2]$ for all n. This follows from an easy induction using the identity

$$Z^{2n} + W^{2n} = ((Z+W)^2 - 2ZW) \cdot (Z^{2n-2} + W^{2n-2}) - (ZW)^2 \cdot (Z^{2n-4} + W^{2n-4}).$$

□

Note that the $H_m(Z, W)$ are invariant under κ_1, κ_2 and so belongs to the invariant ring $\mathbb{Z}[ZW, (Z+W)^2]$. It follows that there is a sequence of polynomials $F_m(X, Y) \in \mathbb{Z}[X, Y]$ such that

$$F_m(ZW, (Z+W)^2) = H_m(Z, W). \tag{23}$$

The following lemma aids in the computation of the F_m.

Lemma 4.2 *The sequence $F_m(X, Y) \in \mathbb{Z}[X, Y]$ satisfies*

$$F_0 = 0, \quad F_1 = F_2 = 1, \quad F_3 = -X + Y,$$

and the recurrence

$$F_{m+2}(X, Y) = (-2X + Y) \cdot F_m(X, Y) - X^2 \cdot F_{m-2}(X, Y), \qquad \text{for } m \geq 2. \tag{24}$$

Proof Since $H_0 = 0$ and $H_1 = H_2 = 1$ we have $F_0 = 0$ and $F_1 = F_2 = 1$. Moreover, $H_3 = Z^2 + ZW + W^2 = -ZW + (Z+W)^2$ so $F_3 = -X + Y$. The map

$$\mathbb{Z}[X, Y] \to \mathbb{Z}[ZW, (Z+W)^2], \qquad X \mapsto ZW, \quad Y \mapsto (Z+W)^2$$

is an isomorphism of rings that sends $F_m(X, Y)$ to $H_m(Z, W)$. Applying this isomorphism to (24) gives

$$H_{m+2}(Z, W) = (Z^2 + W^2)H_m(Z, W) - (ZW)^2 H_{m-2}(Z, W)$$

and so it is enough to prove this identity. However this identity easily follows from the definition of H_m in (22). □

Lemma 4.3 *If m and n are positive integers, then*

(i) *F_m is homogeneous of degree $\lfloor (m-1)/2 \rfloor$.*
(ii) *$F_n \mid F_m$ whenever $n \mid m$.*

Proof These follow immediately from the corresponding properties for the H_m. □

Lemma 4.4 *Let $m \geq 3$. Then*

$$F_m(X, Y) = \prod_{j=1}^{\lfloor (m-1)/2 \rfloor} (Y - 4\cos^2(\pi j/m)X) \tag{25}$$

Proof Fix $m \geq 3$ and write $\zeta = \exp(2\pi i/m)$. Note that

$$\begin{aligned} H_m(Z, W) &= \prod_{j=1}^{\lfloor (m-1)/2 \rfloor} (Z - \zeta^j W)(Z - \zeta^{-j} W) \\ &= \prod_{j=1}^{\lfloor (m-1)/2 \rfloor} (Z^2 + W^2 - (\zeta^j + \zeta^{-j})ZW) \\ &= \prod_{j=1}^{\lfloor (m-1)/2 \rfloor} ((Z + W)^2 - (\zeta^j + \zeta^{-j} + 2)ZW) \\ &= \prod_{j=1}^{\lfloor (m-1)/2 \rfloor} ((Z + W)^2 - (2 + 2\cos 2\pi j/m)ZW) \\ &= \prod_{j=1}^{\lfloor (m-1)/2 \rfloor} ((Z + W)^2 - 4\cos^2(\pi j/m)ZW). \end{aligned}$$

The lemma follows. □

Next we define

$$\Psi_m(X, Y) = \prod_{\substack{j=1 \\ (j,m)=1}}^{\lfloor (m-1)/2 \rfloor} (Y - 4\cos^2(\pi j/m)X). \tag{26}$$

Note that $\Psi_m(X, Y) \in \mathbb{Z}[X, Y]$. Indeed,

$$\Psi_m(X, Y) = \frac{F_m(X, Y)}{\mathrm{LCM}\{F_n(X, Y) \,:\, n \mid m,\ n < m\}}.$$

It follows that $\Psi_m(X, Y) \mid \Psi_n(X, Y)$ (with the divisibility being valid in $\mathbb{Z}[X, Y]$) whenever $m \mid n$. From (25) and (26), we see that

$$F_m(X, Y) = \prod_{d \mid m} \Psi_d(X, Y).$$

We deduce that

$$\Psi_m(X, Y) = \prod_{d \mid m} F_d(X, Y)^{\mu(m/d)} \tag{27}$$

where μ denotes the Möbius function.

Lemma 4.5 *Let $m \geq 3$ and write $\zeta_m = \exp(2\pi i/m)$. The polynomial $\Psi_m(1, Y)$ is monic and irreducible of degree $\phi(m)/2$. It is a defining polynomial for the abelian extension $\mathbb{Q}(\zeta_m)^+/\mathbb{Q}$.*

Proof Recall that $\mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. The elements of the Galois group for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ are the automorphisms $\sigma_j : \zeta_m \mapsto \zeta_m^j$ with $\gcd(j, m) = 1$. Therefore Galois conjugates of $\zeta_m + \zeta_m^{-1} + 2$ are precisely $\zeta_m^j + \zeta_m^{-j} + 2$ with $\gcd(j, m) = 1$, and these are the roots of $\Psi_m(1, Y)$. The lemma follows. □

We shall need the following weak bound for the coefficients of Ψ_m.

Lemma 4.6 *The coefficients of Ψ_m are bounded in absolute value by $5^{\phi(m)/2}$.*

Proof The roots of the monic polynomial $\Psi_m(1, Y)$ are bounded in absolute value by 4. Writing $\Psi_m(1, Y) = \sum a_i Y^i$ and $(4+Y)^{\phi(m)/2} = \sum b_i Y^i$ we have $|a_i| \leq b_i$. Thus

$$\sum |a_i| \leq \sum b_i = 5^{\phi(m)/2}.$$

□

Lemma 4.7 *Let $m \geq 3$ and write $\zeta_m = \exp(2\pi i/m)$. Write h_m and R_m for the class number and regulator of $K_m = \mathbb{Q}(\zeta_m)$. Then as $m \to \infty$,*

$$\log(h_m) = O(m \log m), \qquad \log(h_m R_m) = O(m \log m)$$

where the implicit constants are absolute and effective.

Proof Write $d = \phi(m)/2$ for the degree of K_m. By [39, Propostion 2.7] and [39, Lemma 4.19],

$$\log(|\mathrm{Disc}(K_m)|) \leq \frac{1}{2} \log(\mathrm{Disc}(\mathbb{Q}(\zeta_m))) \leq \frac{1}{2} \phi(m) \log(m).$$

A theorem of Lenstra [21, Theorem 6.5] asserts that for a number field K of degree $d \geq 2$, signature (r, s), absolute discriminant D, class number h and regulator R,

$$h \leq \frac{1}{(d-1)!} \cdot \Delta \cdot (d - 1 + \log \Delta)^s, \qquad \Delta = (2/\pi)^s \cdot D^{1/2}.$$

and

$$hR \leq \frac{1}{(d-1)!} \cdot \Delta \cdot (d - 1 + \log \Delta)^s \cdot (\log \Delta)^{d-1-s}.$$

We take $K = K_m$, so $d = \phi(m)/2$, $s = 0$, and $\Delta = |\mathrm{Disc}(K_m)|^{1/2}$. The lemma follows. □

We can also deduce the bound $\log(h_m R_m) = O(m \log m)$ from the Brauer–Siegel theorem, at the cost of introducing ineffectivity.

Lemma 4.8 *Let p be a prime. Then, for $m \geq 1$,*

$$\tau(p^{m-1}) = \tau(p)^{\varepsilon} \cdot F_m(p^{11}, \tau(p)^2), \qquad \varepsilon = \begin{cases} 0 & \text{if } m \text{ is odd} \\ 1 & \text{if } m \text{ is even.} \end{cases}$$

In particular, $\Psi_m(p^{11}, \tau(p)^2) \mid \tau(p^{m-1})$.

Proof From (19)

$$\tau(p^{m-1}) = \frac{\gamma^m - \delta^m}{\gamma - \delta} = \begin{cases} H_m(\gamma, \delta) & \text{if } m \text{ is odd} \\ (\gamma + \delta) H_m(\gamma, \delta) & \text{if } m \text{ is even,} \end{cases}$$

where $\gamma + \delta = \tau(p)$ and $\gamma\delta = p^{11}$. The lemma follows from (23). □

Lemma 4.9 *Let $m = 5$ or $m \geq 7$. Then precisely the same primes ramify in $L_m = \mathbb{Q}(\zeta_m)$ as in $K_m = \mathbb{Q}(\zeta_m)^+$.*

Proof Note that for $m \in \{2, 3, 4, 6\}$, we have $K_m = \mathbb{Q}$ so the conclusion of the lemma is false in those cases.

By the proof of Proposition 2.15 of [39], we know that L_m/K_m is unramified if m is divisible by at least two distinct odd primes, or divisible by 4 and an odd prime. We may therefore suppose that $m \in \{2^a, p^a, 2p^a\}$ where p is an odd prime and a is a positive integer. If $m = 2^a$ with $a \geq 3$, then K_m has degree $2^{a-2} > 1$, and the set of ramified primes for both L_m and K_m is $\{2\}$. Let p be an odd prime and $a \geq 1$. Then $L_{2p^a} = L_{p^a}$ and $K_{2p^a} = K_{p^a}$. Now the set of ramified primes for L_{p^a} and K_{p^a} is just $\{p\}$ as long as the degree $\phi(p^a)/2$ of K_{p^a} is > 1. The lemma follows. □

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

Proof Write $L_m = \mathbb{Q}(\zeta_m)$. Recall the isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^* \cong \mathrm{Gal}(L_m/\mathbb{Q}), \qquad j \mapsto (\sigma_j : \zeta_m \mapsto \zeta_m^j).$$

The subfield $K_m = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is the fixed field for $\langle \sigma_{-1} \rangle = \{\sigma_1, \sigma_{-1}\}$. Let q be a rational prime that does not ramify in K_m (and hence in L_m by Lemma 4.9). The Frobenius automorphism for q is simply σ_q. The prime q splits completely in K_m if and only if the restriction of σ_q to K_m is trivial. This is equivalent to $\sigma_q \in \{\sigma_1, \sigma_{-1}\}$ and therefore equivalent to $q \equiv \pm 1 \pmod{m}$.

Let $\lambda = \zeta_m + \zeta_m^{-1} + 2$. This is a root for $\Psi_m(1, Y)$ and also a generator for K_m. Note [39, Proposition 2.16] that $\mathcal{O}_{K_m} = \mathbb{Z}[\lambda]$. We are given that $q \mid \Psi_m(x, y)$. Since $\Psi_m(1, Y)$ is monic, if $q \mid x$ then $q \mid y$ giving a contradiction. Hence $q \nmid x$ and so

$\Psi_m(1, y/x) \equiv 0 \pmod{q}$. By the Dedekind–Kummer Theorem, there is a degree 1 prime ideal $\mathfrak{q}$ above q. As $K_m/\mathbb{Q}$ is Galois, all primes above q must therefore have degree 1. Thus q is either totally split or ramified in K_m. If q is totally split, then $q \equiv \pm 1 \pmod{m}$ and we are finished.

We shall therefore suppose that q is ramified in K_m. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be the prime ideals of $\mathcal{O}_{K_m}$ above q. Write G for the Galois group of $\mathrm{Gal}(K_m/\mathbb{Q})$, and let I be the inertia subgroup for $\mathfrak{q}_1$. As G is abelian, I is also the inertia subgroup for all $\mathfrak{q}_i$. Thus $\mathfrak{q}_i^\sigma = \mathfrak{q}_i$ for all $\sigma \in I$ and for $i = 1, \ldots, r$. Since q is ramified, $I \neq 1$. Fix $\sigma_j \in \mathrm{Gal}(L_m/\mathbb{Q})$ whose restriction to K_m is a non-trivial element of I. Thus $\gcd(j, m) = 1$ and $j \not\equiv \pm 1 \pmod{m}$. Write $\lambda_j = \zeta_m^j + \zeta_m^{-j} + 2 = \sigma_j(\lambda)$.

We factor the ideal $(y - \lambda x)\mathcal{O}_{K_m}$ as

$$(y - \lambda x)\mathcal{O}_{K_m} = \mathfrak{a}\mathfrak{b} \tag{28}$$

where $\mathfrak{a}, \mathfrak{b}$ are ideals with $\mathfrak{a}$ supported on $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$, and $\mathfrak{b}$ not divisible by $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$. By assumption $q^a \mid\mid \Psi_m(x, y)$. However $\Psi_m(x, y) = \mathrm{Norm}_{K_m/\mathbb{Q}}(y - \lambda x)$ and thus $\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{a}) = q^a$. Note that any ideal dividing both x and $\mathfrak{a}$ must also divide y by (28). As x, y are coprime, we deduce that x and $\mathfrak{a}$ are coprime.

Since $\mathfrak{q}^{\sigma_j} = \mathfrak{q}$ for all $\mathfrak{q} \mid \mathfrak{a}$, we have $\mathfrak{a}^{\sigma_j} = \mathfrak{a}$. Hence $\mathfrak{a}$ divides

$$(y - \lambda^{\sigma_j} x) - (y - \lambda x) = (\lambda - \lambda^{\sigma_j})x.$$

Thus $\mathfrak{a}$ divides

$$\lambda - \lambda^{\sigma_j} = (\zeta_m + \zeta_m^{-1}) - (\zeta_m^j + \zeta_m^{-j}) = \zeta_m^{-1}(\zeta_m^{j+1} - 1)(\zeta_m^{-j+1} - 1)$$

and it follows that $q^{2a} = \mathrm{Norm}_{K_m/K}(\mathfrak{a})^2$ divides

$$\begin{aligned}(\mathrm{Norm}_{K_m/\mathbb{Q}}(\lambda - \lambda^{\sigma_j}))^2 &= \mathrm{Norm}_{L_m/\mathbb{Q}}(\lambda - \lambda^{\sigma_j}) \\ &= \mathrm{Norm}_{L_m/\mathbb{Q}}(\zeta_m^{j+1} - 1) \cdot \mathrm{Norm}_{L_m/\mathbb{Q}}(\zeta_m^{-j+1} - 1).\end{aligned}$$

This divides $\prod_{i=1}^{m-1}(\zeta_m^i - 1)^2 = m^2$. Hence $q^a \mid m$ as required. □

Lemma 4.11 *Let p be a prime and suppose $\tau(p) \neq 0$. Let $r = \mathrm{ord}_p(\tau(p))$ and write*

$$x = p^{11-2r} \quad \text{and} \quad y = \frac{\tau(p)^2}{p^{2r}}.$$

Let $\{u_m\}$ be the Lucas sequence defined in Lemma 3.4. Then, for $m \geq 3$,

$$\Psi_m(x, y) = \prod_{d \mid m} u_d^{\mu(m/d)}. \tag{29}$$

Moreover, if $m = 5$ or $m \geq 7$, then $\Psi_m(x, y)$ is divisible by some prime $\ell \nmid m$.

Proof Note that x and y are in fact integers by Lemma 3.1, and are coprime by the definition of r. Let $\{u_m\}$ be the Lucas sequence defined in Lemma 3.4. Thus

$$u_m = \frac{\tau(p^{m-1})}{p^{r(m-1)}} = \frac{\alpha^m - \beta^m}{\alpha - \beta}, \qquad \alpha\beta = p^{11-2r}, \qquad \alpha + \beta = \tau(p)/p^r.$$

Write

$$\varepsilon(m) = \begin{cases} 0 & \text{if } m \text{ is odd} \\ 1 & \text{if } m \text{ is even.} \end{cases}$$

Then

$$\begin{aligned} F_m(x, y) &= \frac{1}{p^{2r\deg(F_m)}} \cdot F_m(p^{11}, \tau(p)^2) \\ &= \frac{\tau(p^{m-1})}{p^{2r\deg(F_m)} \cdot \tau(p)^{\varepsilon(m)}} \qquad \text{(by Lemma 4.8)} \\ &= \frac{p^{r(m-1)} \cdot u_m}{p^{2r\deg(F_m)} \cdot \tau(p)^{\varepsilon(m)}}. \end{aligned}$$

However, since $\deg(F_m) = \lfloor (m-1)/2 \rfloor$, it follows that

$$F_m(x, y) = \left(\frac{p^r}{\tau(p)}\right)^{\varepsilon(m)} \cdot u_m.$$

By (27),

$$\Psi_m(x, y) = \left(\frac{p^r}{\tau(p)}\right)^{\sum_{d|m} \varepsilon(d)\mu(m/d)} \cdot \prod_{d|m} u_d^{\mu(m/d)}.$$

It is easy to see that

$$\sum_{d|m} \varepsilon(d)\mu(m/d) = \begin{cases} 0 & \text{if } m \neq 2 \\ 1 & \text{if } m = 2. \end{cases}$$

This completes the proof of (29).

Now let $m = 5$ or $m \geq 7$. By Theorem 7, the term u_m has a prime divisor ℓ that does not divide $(\alpha - \beta)^2$ nor $u_1 u_2 \cdots u_{m-1}$. By Theorem 8, we know that $\ell \neq p$, that $m = m_\ell$, and that $m \mid (\ell - 1)$ or $m \mid (\ell + 1)$. In particular, $\ell \nmid m$. From (29), we have $\ell \mid \Psi_m(x, y)$ as required. □

5 Proof of Theorem 4

We shall need the following theorem [9, Theorem 1].

Theorem 9 (Bugeaud) *Let K be a number field. Let $u \geq 2$ and $v \geq 3$ be integers, and let $a, b \in \mathcal{O}_K \backslash \{0\}$. There exist effectively computable positive constants $\varepsilon_1, \varepsilon_2$ depending only on a, b, u, v and K such that every pair of coprime $x, y \in \mathcal{O}_K$ with*

$$\max\{|\mathrm{Norm}_{K/\mathbb{Q}}(x)|,\ |\mathrm{Norm}_{K/\mathbb{Q}}(y)|\} \ > \ \varepsilon_1$$

satisfy

$$P(ax^u + by^v) \ > \ \varepsilon_2 \cdot \log\log \max\{|\mathrm{Norm}_{K/\mathbb{Q}}(x)|,\ |\mathrm{Norm}_{K/\mathbb{Q}}(y)|\}.$$

In the above theorem, $P(\delta)$ for $\delta \in \mathcal{O}_K$ denotes the largest rational prime that is below a prime ideal dividing δ.

We now prove Theorem 4. Let p be a prime and suppose $\tau(p) \neq 0$. Let $m \geq 3$. We want to show that

$$P(\tau(p^{m-1})) \ \gg_m \ \log\log p.$$

Let $r = \mathrm{ord}_p(\tau(p))$ and recall that $\mathrm{ord}_p(\tau(p^{m-1})) = r(m-1)$ by Lemma 3.1. If $r \geq 1$ then

$$P(\tau(p^{m-1})) \ \geq \ p,$$

whereby we may suppose that $r = 0$. Recall that $\Psi_m(p^{11}, \tau(p)^2) \mid \tau(p^{m-1})$ by Lemma 4.8. Let $K = K_m = \mathbb{Q}(\zeta_m)^+$ and let $\lambda = \zeta_m + \zeta_m^{-1} + 2$ which is a root of the monic polynomial $\Psi_m(1, Y)$. Then

$$\Psi_m(p^{11}, \tau(p)^2) \ = \ \mathrm{Norm}_{K/\mathbb{Q}}(\tau(p)^2 - \lambda \cdot p^{11})$$

and therefore

$$P(\tau(p^{m-1})) \ \geq \ P(\Psi_m(p^{11}, \tau(p)^2)) \ = \ P(\tau(p)^2 - \lambda \cdot p^{11}).$$

We now apply Bugeaud's theorem with $u = 2$, $v = 11$, $a = 1$, $b = -\lambda$, $x = \tau(p)$, $y = p$ to deduce that $P(\tau(p)^2 - \lambda \cdot p^{11}) \ \gg_m \ \log\log p$. This completes the proof.

6 Proof of Theorem 3

In this section, we prove Theorem 3. For this we appeal to a result of Bugeaud and Győry [10] which provides bounds for solutions to Thue–Mahler equations. Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be an irreducible binary form of degree $n \geq 3$, and let b a non-zero rational integer with absolute value at most $B \geq e$. Let $H \geq 3$ be an upper bound for the absolute values of the coefficients of F.

Let α_1, α_2 and α_3 be three distinct roots of $F(1, Y)$. Define

$$\mathbb{M} = \mathbb{Q}(\alpha_1), \quad \mathbb{M}_{123} = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \quad \text{and} \quad N = [\mathbb{M}_{123} : \mathbb{Q}].$$

Write $h_{\mathbb{M}}$ for the class number of $\mathbb{M}$ and $R_{\mathbb{M}}$ for its regulator. Let $p_1, p_2, \ldots, p_s$ ($s > 0$) be distinct primes not exceeding P. Consider the **Thue–Mahler equation**

$$F(x, y) = b \cdot p_1^{z_1} p_2^{z_2} \cdots p_s^{z_s}, \qquad x,\ y,\ z_i \in \mathbb{Z}, \qquad \gcd(x, y, p_1 p_2 \cdots p_s) = 1. \tag{30}$$

For a positive real number a, we write $\log^* a = \max\{1, \log a\}$.

Theorem 10 (Bugeaud and Győry) *All solutions to* (30) *satisfy*

$$\log \max\{|x|,\ |y|,\ p_1^{z_1} \cdots p_k^{z_k}\} \le c(n, s) \cdot P^N \cdot (\log P)^{ns+2} \cdot R_{\mathbb{M}} h_{\mathbb{M}} \cdot (\log^*(R_{\mathbb{M}} h_{\mathbb{M}}))^2 \cdot (R_{\mathbb{M}} + s h_{\mathbb{M}} + \log(HB)),$$

where

$$c(n, s) = 3^{n(2s+1)+27} \cdot n^{2n(7s+13)+13} \cdot (s+1)^{5n(s+1)+15}.$$

The theorem as stated is the first part of Theorem 4 in [10], with only one minor difference. In [10] the authors take $N = n(n-1)(n-2)$. However, in their proof N is simply taken as an upper bound for the degree $[\mathbb{M}_{123} : \mathbb{Q}]$, and so we can take $N = [\mathbb{M}_{123} : \mathbb{Q}]$.

We now embark on the proof of Theorem 3. In what follows $\eta_2, \eta_3, \ldots$ will denote absolute effectively computable positive constants. Let us fix a prime p and suppose $\tau(p) \neq 0$. We will in fact show that

$$P(\tau(p^{m-1})) \ge \eta_2 \cdot \frac{\log\log(p^m)}{\log\log\log(p^m)}, \tag{31}$$

for $m \ge 3$ which implies (7). In view of Theorem 4 (which was proved in Section 5), we shall suppose that $m = 7$, 9, 11 or $m \ge 13$. In particular, $\Psi_m(X, Y)$ is irreducible of degree $\phi(m)/2 \ge 3$. Write $r = \mathrm{ord}_p(\tau(p))$. By Lemma 3.4, we have $\mathrm{ord}_p(\tau(p^{m-1})) = r(m-1)$. Recall that $r = \mathrm{ord}_p(\tau(p)) \le 5$ by Lemma 3.1. Let

$$x = p^{11-2r}, \qquad y = \tau(p)^2 / p^{2r},$$

and observe that $\gcd(x, y) = 1$. By Lemma 4.8, we know that $\Psi_m(x, y)$ is a divisor of $\tau(p^{m-1})$ and therefore

$$P(\tau(p^{m-1})) \ge P(\Psi_m(x, y)).$$

To prove (31), we shall show that

$$P(\Psi_m(x, y)) > \eta_3 \cdot \frac{\log\log(p^m)}{\log\log\log(p^m)}. \tag{32}$$

By Lemma 4.10, we can write

$$\Psi_m(x, y) \;=\; b \cdot p_1^{z_1} p_2^{z_2} \cdots p_s^{z_s}, \tag{33}$$

where the p_i are primes, and

$$b \mid m, \quad p_i \equiv \pm 1 \pmod{m} \quad \text{and} \quad p_1 < p_2 < \cdots < p_s.$$

From Lemma 4.11, we have $s \geq 1$. It is clear that

$$s \;<\; \eta_4 \cdot \frac{p_s}{m}.$$

In what follows we make use of the following inequalities

$$n \;<\; m \quad \text{and} \quad ns \;<\; ms \;<\; \eta_4 \cdot p_s.$$

Moreover, since $p_s \equiv \pm 1 \pmod{m}$, we have

$$p_s \;\geq\; m - 1.$$

We will apply Theorem 10 to (33). We take

$$F = \Psi_m, \quad B = m, \quad P = p_s, \quad n = N = \phi(m)/2 \quad \text{and} \quad H = 5^{n/2}.$$

where the choice of H is justified by Lemma 4.6. By Lemma 4.7, we have

$$\log(h_{\mathbb{M}}) \;<\; \eta_5 \cdot m \log m \quad \text{and} \quad \log(h_{\mathbb{M}} R_{\mathbb{M}}) \;<\; \eta_6 \cdot m \log m.$$

Since $x = p^{11-2r}$ with $r \leq 5$, we have $\log\log p \leq \log\log x$. Taking logarithms in Theorem 10, and making repeated use of the above inequalities and bounds, yields

$$\log\log p \;<\; \eta_7 \cdot p_s \cdot \log p_s.$$

But

$$\begin{aligned} \log\log(p^m) \;&=\; \log\log p + \log m \;<\; \eta_7 \cdot p_s \cdot \log p_s \\ &+ \log(p_s + 1) \;<\; \eta_8 \cdot p_s \cdot \log p_s. \end{aligned}$$

The desired inequality (32) follows, completing the proof of Theorem 3.

7 The equation $\tau(p^2) = \kappa \cdot q^b$

In this section we establish the following two propositions.

Proposition 7.1 *Let $3 \leq q < 100$ be a prime. The equation*

$$\tau(p^2) \;=\; \pm q^b, \qquad p \text{ prime}, \qquad b \geq 0 \tag{34}$$

has no solutions.

Proposition 7.2 *The equation*

$$\tau(p^2) \;=\; \pm 3^{b_1} 5^{b_2} 7^{b_3} 11^{b_4}, \qquad p \text{ prime}, \qquad b_1,\ b_2,\ b_3,\ b_4 \geq 0 \tag{35}$$

has no solutions.

We consider first the following general equation.

$$\tau(p^2) \;=\; \kappa \cdot q^b, \qquad p \nmid 2\kappa q \text{ prime}, \qquad b \geq 0. \tag{36}$$

Here κ is an odd integer, q is an odd prime, and we assume for convenience that $q \nmid \kappa$. Recall that $\tau(p^2) = \tau(p)^2 - p^{11}$. Equation (36) can be written as

$$p^{11} + (\kappa \cdot q^b) \cdot 1^{11} \;=\; \tau(p)^2$$

and so is an equation of signature $(11, 11, 2)$. Following the first author and Skinner [5], we associate to a solution of (36) the Frey–Hellegouarch curve

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

Let

$$N = \begin{cases} 2^5 \cdot \mathrm{Rad}(\kappa) \cdot q \cdot p & \text{if } b > 0 \\ 2^5 \cdot \mathrm{Rad}(\kappa) \cdot p & \text{if } b = 0, \end{cases} \qquad N' = \begin{cases} 2^5 \cdot \mathrm{Rad}(\kappa) \cdot q & \text{if } 11 \nmid b \\ 2^5 \cdot \mathrm{Rad}(\kappa) & \text{if } 11 \mid b. \end{cases} \tag{37}$$

Here $\mathrm{Rad}(\kappa)$ denotes the product of the prime divisors of κ. The Frey–Hellegouarch curve E_p has conductor N. Moreover, it follows from the recipes of the first author and Skinner [5] (based on the modularity theorem and Ribet's level lowering theorem) that there is a normalized newform

$$f = q + \sum_{n=1}^{\infty} c_n q^n \tag{38}$$

of weight 2 and level N' and a prime $\varpi \mid 11$ in the integers of $K = \mathbb{Q}(c_1, c_2, \ldots)$ so that

$$\overline{\rho}_{E_p,11} \sim \overline{\rho}_{f,\varpi}. \tag{39}$$

The restrictions on κ and q being coprime odd integers merely reduce the number of possibilities for N, N', yet cover all the cases we are interested in solving. The restriction $p \nmid 2\kappa q$ is needed so that the minimal discriminant Δ of the Frey–Hellegouarch

curve E_p satisfies $\mathrm{ord}_p(\Delta) \equiv 0 \mod 11$ which is necessary for application of Ribet's level lowering theorem in order to obtain a weight 2 newform f of level N' not divisible by p.

Throughout what follows, ℓ will be a prime satisfying

$$\ell \nmid 2 \cdot 11 \cdot \kappa q p. \tag{40}$$

Then, taking traces of the images of the Frobenius element at ℓ in (39) we obtain $a_\ell(E_p) \equiv c_\ell \mod \varpi$ and so

$$\mathrm{Norm}_{K/\mathbb{Q}}(a_\ell(E_p) - c_\ell) \equiv 0 \mod 11. \tag{41}$$

We shall use both the congruences for the τ-function (11)–(15) and also (41) to derive congruences for b.

Lemma 7.3 *Let (p, b) be a solution to (36) and suppose $p \neq 3, 23$. Let ℓ be a prime satisfying (40). Let*

$$\mathcal{A}_\ell = \{(s,t) \,:\, s,\ t \in \mathbb{F}_\ell,\quad s \not\equiv 0 \mod \ell,\qquad t^2 - s^{11} \not\equiv 0 \mod \ell\},$$

and

$$\mathcal{B}_\ell = \begin{cases} \mathcal{A}_\ell & \ell \neq 3,\ 5,\ 7,\ 23; \\ \{(s,t) \in \mathcal{A}_3 \,:\, t \equiv s+1 \mod 3\} & \ell = 3; \\ \{(s,t) \in \mathcal{A}_5 \,:\, t \equiv s^2(s^3+1) \mod 5\} & \ell = 5; \\ \{(s,t) \in \mathcal{A}_7 \,:\, t \equiv s(s^3+1) \mod 7\} & \ell = 7; \\ \{(s,0) : s \in \mathbb{F}_{23}^* \backslash (\mathbb{F}_{23}^*)^2\} \cup \{(s,t) : s \in (\mathbb{F}_{23}^*)^2,\ t = 2,\ -1\} & \ell = 23. \end{cases} \tag{42}$$

For $(s,t) \in \mathcal{B}_\ell$ let

$$E_{s,t,1}/\mathbb{F}_\ell \,:\, Y^2 = X(X^2 + 2tX + t^2 - s^{11}),$$
$$E_{s,t,3}/\mathbb{F}_\ell \,:\, Y^2 = X(X^2 + 2tX + s^{11}).$$

Let f be a newform of weight 2 and level N' so that (39) is satisfied, and c_ℓ be its ℓ-th coefficient. For $j = 1, 3$, let

$$\mathcal{C}_{\ell,j}(f) = \{(s,t) \in \mathcal{B}_\ell \,:\, \mathrm{Norm}(a_\ell(E_{s,t,j}) - c_\ell) \equiv 0 \mod 11\}, \tag{43}$$

and

$$\mathcal{D}_{\ell,j}(f) = \{t^2 - s^{11} \,:\, (s,t) \in \mathcal{C}_{\ell,j}(f)\} \subseteq \mathbb{F}_\ell.$$

If $p \equiv 1 \mod 4$ then $(\kappa \cdot q^b \mod \ell) \in \mathcal{D}_{\ell,1}(f)$. If $p \equiv 3 \mod 4$ then $(\kappa \cdot q^b \mod \ell) \in \mathcal{D}_{\ell,3}(f)$.

Proof Since $\ell \nmid 2\kappa qp$, and $\tau(p)^2 - p^{11} = \tau(p^2) = \kappa \cdot q^b$ we see that there is some $(s,t) \in \mathcal{A}_\ell$ so that $(p, \tau(p)) \equiv (s,t) \mod \ell$. Moreover, from the congruences for τ in (12)–(15) there is some $(s,t) \in \mathcal{B}_\ell$ so that $(p, \tau(p)) \equiv (s,t) \mod \ell$; it is here that we make use of the assumption $p \neq 3, 23$. For such a pair (s,t), the reduction modulo ℓ of the Frey–Hellegouarch curve E_p is $E_{s,t,j}/\mathbb{F}_\ell$, where $j = 1$ or 3 according to whether $p \equiv 1$ or $3 \mod 4$. Thus $a_\ell(E_{s,t,j}) = a_\ell(E_p)$. Hence, $\mathrm{Norm}(a_\ell(E_{s,t,j}) - c_\ell) \equiv 0 \mod 11$ by (41), and so $(s,t) \in \mathcal{C}_{\ell,j}(f)$. Since $t^2 - s^{11} \equiv \tau(p)^2 - p^{11} \equiv \kappa \cdot q^b \mod \ell$ we see that $(\kappa \cdot q^b \bmod \ell) \in \mathcal{D}_{\ell,j}(f)$. □

For any prime ℓ satisfying (40), the lemma gives congruences for q^b modulo ℓ, and hence leads to congruences for b modulo $O_\ell(q)$, where $O_\ell(q)$ will be our notation for the multiplicative order of q modulo ℓ. This idea is formalized in the following lemma.

Lemma 7.4 *Let (p,b) be a solution to (36) with $p \neq 3, 23$, and let M be a positive integer satisfying $22 \mid M$. Define $\mathcal{E}_1$ and $\mathcal{E}_3$ via*

$$\mathcal{E}_1 = \{0 \leq \beta \leq M-1 \ : \ \kappa \cdot q^\beta \equiv 3 \mod 4\} \quad \textit{and}$$
$$\mathcal{E}_3 = \{0 \leq \beta \leq M-1 \ : \ \kappa \cdot q^\beta \equiv 1 \mod 4\}.$$

Let f be a newform of weight 2 and level N' so that (39) is satisfied. For $j = 1, 3$, define

$$\mathcal{F}_j(f) = \begin{cases} \{\beta \in \mathcal{E}_j \ : \ 11 \nmid \beta\} & \text{if } N' = 2^5 \cdot \mathrm{Rad}(\kappa) \cdot q \\ \{\beta \in \mathcal{E}_j \ : \ 11 \mid \beta\} & \text{if } N' = 2^5 \cdot \mathrm{Rad}(\kappa). \end{cases}$$

Suppose now that $\mathcal{L}$ is a set of primes satisfying

$$\ell \nmid 2 \cdot 11 \cdot \kappa qp, \qquad O_\ell(q) \mid M. \tag{44}$$

For $\ell \in \mathcal{L}$ and $j = 1, 3$, let

$$\mathcal{G}_{\ell,j}(f) \ = \ \{\beta \in \mathcal{F}_j(f) \ : \ (\kappa \cdot q^\beta \bmod \ell) \in \mathcal{D}_{\ell,j}(f)\}.$$

Let

$$\mathcal{H}_j(f) \ = \ \bigcap_{\ell \in \mathcal{L}} \mathcal{G}_{\ell,j}(f).$$

If $p \equiv 1 \mod 4$ then there is some $\beta \in \mathcal{H}_1(f)$ such that $b \equiv \beta \mod M$. If $p \equiv 3 \mod 4$ then there is some $\beta \in \mathcal{H}_3(f)$ such that $b \equiv \beta \mod M$.

Proof Let $0 \leq \beta \leq M-1$ be the unique integer such that $\beta \equiv b \mod M$. Let $j = 1, 3$ according to whether $p \equiv 1$ or $3 \mod 4$ respectively. As $2 \mid M$ and q is odd we have $\kappa \cdot q^\beta \equiv \kappa \cdot q^b \mod 4$. Note from (11) that

$$\kappa \cdot q^{\beta} \equiv \kappa \cdot q^{b} = \tau(p^2)$$
$$= \tau(p)^2 - p^{11} \equiv p^2 + p + 1 \equiv \begin{cases} 3 \mod 4 & \text{if } p \equiv 1 \mod 4 \\ 1 \mod 4 & \text{if } p \equiv 3 \mod 4. \end{cases}$$

Thus $\beta \in \mathcal{E}_j$.

Also $11 \mid M$. Hence $11 \mid b$ if and only if $11 \mid \beta$. From the definition of N' in (37) we see that $\beta \in \mathcal{F}_j(f)$.

Now let $\ell \in \mathcal{L}$. By Lemma 7.3, we know that $(\kappa \cdot q^b \bmod \ell) \in \mathcal{D}_{\ell,j}(f)$. However $O_\ell(q) \mid M$ and $M \mid (\beta - b)$. Thus $\kappa \cdot q^{\beta} \equiv \kappa \cdot q^{b} \mod \ell$, and so $(\kappa \cdot q^{\beta} \bmod \ell) \in \mathcal{D}_{\ell,j}(f)$. We deduce that $\beta \in \mathcal{G}_{\ell,j}(f)$ for all $\ell \in \mathcal{L}$. Therefore $\beta \in \mathcal{H}_j(f)$ completing the proof. □

Proof of Proposition 7.1 We checked that (34) has no solutions with $p < 200$ for primes $3 \le q < 100$. We shall henceforth suppose that $p > 200$. In particular, $p \ne q$. Moreover, any solution to (34) is a solution to (36) with $\kappa = 1$ or -1. For a given $3 \le q < 100$ we shall let

$$M = 396 = 2^2 \cdot 3^2 \cdot 11, \qquad \mathcal{L} = \{3 \le \ell < 200 \text{ prime}, \ell \ne 11,\ q \ :\ O_\ell(q) \mid M\}.$$

Observe that since $p > 200$ that every $\ell \in \mathcal{L}$ satisfies (44).

Suppose first that $11 \mid b$ and write $b = 11c$. Then $(x, y, z) = (p, \pm q^c, \tau(p))$ is a solution to the equation $x^{11} + y^{11} = z^2$ satisfying $\gcd(x, y, z) = 1$. Darmon and Merel [13] showed that the equation $x^n + y^n = z^2$ has no solutions $(x, y, z) \in \mathbb{Z}^3$ with $n \ge 4$, $\gcd(x, y, z) = 1$. This contradiction completes the proof for $q \ne 3$.

Thus $11 \nmid b$, and so in (37) the level is $N' = 2^5 q$. We will consider the case $q = 3$ a little later. Suppose $5 \le q < 100$. We wrote a `Magma` script which for each prime $5 \le q < 100$, computes the weight 2 newforms f of level $N' = 2^5 q$, and the sets $\mathcal{H}_1(f)$ and $\mathcal{H}_3(f)$ both for $\kappa = 1, \kappa = -1$. We found all of these to be empty. By Lemma 7.4, we conclude that (34) has no solutions with $5 \le q < 100$.

It remains to consider the case $q = 3$. By Lemma 2.3, we see that $b = 0$ or 1. But $11 \nmid b$, therefore $b = 1$. Thus

$$\tau(p)^2 - p^{11} = \pm 3. \tag{45}$$

We consider this modulo 23 using (15). If p is a quadratic non-residue modulo 23, then $p^{11} \equiv -1 \mod 23$ and $\tau(p) \equiv 0 \mod 23$ giving a contradiction. If p is a quadratic residue modulo 23, then $p^{11} \equiv 1 \mod 23$ and $\tau(p) \equiv 2, -1 \mod 23$. We conclude that $\tau(p) \equiv 2 \mod 23$ and $\tau(p)^2 - p^{11} = 3$. Thus

$$(\tau(p) + \sqrt{3})(\tau(p) - \sqrt{3}) = p^{11}.$$

The two factors on the left-hand side are coprime integers in $\mathbb{Z}[\sqrt{3}]$. We see that

$$\tau(p) + \sqrt{3} = (2 + \sqrt{3})^a \gamma^{11}, \qquad \gamma \in \mathbb{Z}[\sqrt{3}], \qquad \text{Norm}(\gamma) = p, \qquad 0 \le a \le 10.$$

Let $\mathfrak{q} = (2+3\sqrt{3})\mathbb{Z}[\sqrt{3}]$. Then $23\mathbb{Z}[\sqrt{3}] = \mathfrak{q}\bar{\mathfrak{q}}$. Since $\mathfrak{q}$ has residue field $\mathbb{F}_{23}$, we see that $\gamma^{11} \equiv \pm 1 \mod \mathfrak{q}$. Moreover, as $\tau(p) \equiv 2 \mod 23$ we have

$$2+\sqrt{3} \equiv \pm(2+\sqrt{3})^a \mod \mathfrak{q}.$$

However, $2+\sqrt{3}$ has multiplicative order 11 in $\mathbb{Z}[\sqrt{3}]/\mathfrak{q} = \mathbb{F}_{23}$. As $0 \le a \le 10$, we conclude that $a = 1$. Thus

$$\tau(p) + \sqrt{3} = (2+\sqrt{3})(U+V\sqrt{3})^{11}, \qquad U,\ V \in \mathbb{Z}.$$

Comparing coefficients of $\sqrt{3}$ we obtain the Thue equation

$$\begin{aligned} U^{11} + 22U^{10}V + 165U^9V^2 + 990U^8V^3 + 2970U^7V^4 8316U^6V^5 + \\ +12474U^5V^6 + 17820U^4V^7 + 13365U^3V^8 + 8910U^2V^9 \\ +2673UV^{10} + 486V^{11} \ = \ 1. \end{aligned}$$

The `Magma` Thue equation solver (based on algorithms in [36]) gives that the only solution is $(U, V) = (1, 0)$. Thus $p = U^2 - 3V^2 = 1$ which is a contradiction. □

Remark. The reader might be wondering if the case $11 \mid b$ can also be tackled using Lemma 7.4 instead of appealing to Darmon and Merel. In that case, $N' = 32$, and there is precisely one weight 2 newform f of level 32. This has rational eigenvalues and corresponds to the elliptic curve

$$E \ : \ Y^2 = X^3 - X.$$

Let $\ell \neq 2$ be a prime. By inspection of the definition of $\mathcal{B}_\ell$ in Lemma 7.3, we note that $(-1, 0) \in \mathcal{B}_\ell$ and that $E_{-1,0,3}$ is the reduction modulo ℓ of the elliptic curve E. Thus $a_\ell(E_{-1,0,3}) = a_\ell(E) = c_\ell$ where c_ℓ is the ℓ-th coefficient of f. Thus $(-1, 0) \in \mathcal{C}_{\ell,3}(f)$, and therefore $1 \in \mathcal{D}_{\ell,3}(f)$. Let $\kappa = 1$. Going through the definitions in Lemma 7.4, it it easy to verify that $0 \in \mathcal{H}_3(f)$ regardless of the choice of M and $\mathcal{L}$. Hence we cannot use Lemma 7.4 to rule out the case $\kappa = 1$ and $11 \mid b$.

There is a similar explanation for why we are unable to use Lemma 7.4 on its own to rule out the case $q = 3$, $\kappa = 1$ and $11 \nmid b$. Here $N' = 96$. There are two weight 2 newforms of level 96 and we take f to be the one corresponding to the elliptic curve

$$E \ : \ Y^2 = X^3 + 4X^2 + 3X.$$

Let $\ell \nmid 6$ be a prime. We note that $(1, 2) \in \mathcal{B}_\ell$. Moreover, $E_{1,2,1}$ is the reduction modulo ℓ of E. Hence $a_\ell(E_{1,2,1}) = a_\ell(E) = c_\ell$ which is as before the ℓ-th coefficient of f. We therefore have $(1, 2) \in \mathcal{C}_\ell(f)$ and so $3 \in \mathcal{D}_{\ell,1}(f)$. It follows, for $\kappa = 1$, that $1 \in \mathcal{H}_1(f)$ regardless of the choice of M and $\mathcal{L}$.

Proof of Proposition 7.2 Again we checked that equation (35) has no solutions with $p < 200$ so we may suppose that $p > 200$. Moreover, by Lemmas 2.1, 2.2 and 2.3 , we have $b_1 = 0$ or $b_1 = 1$, and $b_2 = b_3 = 0$ in (35). If $b_1 = 0$ then equation (35)

becomes $\tau(p)^2 - p^{11} = \pm 11^{b_4}$ which does not have any solutions by Proposition 7.1. Hence $b_1 = 1$. For convenience we write b for b_4, so equation (35) becomes

$$\tau(p)^2 - p^{11} = \pm 3 \cdot 11^b. \tag{46}$$

We apply Lemma 7.4 with $q = 11$ and $\kappa = \pm 3$. Here $N' = 96$ if $11 \mid b$ and $N' = 96 \times 11 = 1056$ if $11 \nmid b$. For the newforms f at both these levels and for $\kappa = 3$ and $\kappa = -3$, we computed $\mathcal{H}_1(f)$ and $\mathcal{H}_3(f)$. We found that all these are empty with precisely one exception. For that exception $\kappa = 3$, and f is the newform of level 96 corresponding to the elliptic curve E with Cremona label `96a1` :

https://www.lmfdb.org/EllipticCurve/Q/96a1/

where we find

$$\mathcal{H}_1(f) = \{0,\ 22,\ 44,\ 66,\ 88,\ 110,\ 132,\ 154,\ 176,\ 198,\ 220,\ 242,\ 264,\ 286,\ 308,\ 330,\ 352,\ 374\},$$

and so Lemma 7.4 does not provide a contradiction. However, we know that if (p, b) is a solution to (46) then $\overline{\rho}_{E_p,11} \sim \overline{\rho}_{f,\varpi} \sim \overline{\rho}_{E,11}$. Suppose $b \neq 0$. Then the Frey–Hellegouarch curve E_p has conductor $96 \cdot 11$ and so multiplicative reduction at 11. The curve E has conductor 96 and hence good reduction at 11. Comparing the traces of Frobenius at 11 in the two representations $\overline{\rho}_{E_p,11} \sim \overline{\rho}_{E,11}$ (see [19]) we obtain $\pm(11+1) \equiv a_{11}(E) \mod 11$. However, $a_{11}(E) = 4$ giving a contradiction. Thus $b = 0$. Equation (46) now becomes equation (45), which we showed, in the proof of Proposition 7.1, to have no solutions. This completes the proof. □

8 The equation $\tau(p^4) = \kappa \cdot q^b$

In this section, we establish the following two propositions.

Proposition 8.1 *Let $3 \leq q < 100$ be a prime. The equation*

$$\tau(p^4) = \pm q^b, \quad p \text{ prime}, \quad b \geq 0 \tag{47}$$

has no solutions.

Proposition 8.2 *The equation*

$$\tau(p^4) = \pm 3^{b_1} 5^{b_2} 7^{b_3} 11^{b_4}, \quad p \text{ prime}, \quad b_1,\ b_2,\ b_3,\ b_4 \geq 0 \tag{48}$$

has no solutions.

We consider first the following general equation.

$$\tau(p^4) = \kappa \cdot q^b, \quad p \nmid 2\kappa q \text{ prime}, \quad b \geq 0. \tag{49}$$

Here κ is an odd integer, q is an odd prime, and we assume for convenience that

$$q \nmid 5\kappa, \qquad \mathrm{ord}_5(\kappa) = 0 \text{ or } 1.$$

Using the recursion (18) we find that

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

which can be written as

$$4\tau(p^4) = (2\tau(p)^2 - 3p^{11})^2 - 5p^{22}. \tag{50}$$

We may therefore rewrite (49) as

$$5(p^2)^{11} + (4 \cdot \kappa \cdot q^b) \cdot 1^{11} \;=\; (2\tau(p)^2 - 3p^{11})^2,$$

which is an equation of signature $(11, 11, 2)$. As before we follow the first author and Skinner [5], and associate to a solution of (49) the Frey–Hellegouarch curve

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

Let

$$N = \begin{cases} 2^3 \cdot 5 \cdot \mathrm{Rad}(\kappa) \cdot q \cdot p & \text{if } b > 0, \mathrm{ord}_5(\kappa) = 0 \\ 2^3 \cdot 5 \cdot \mathrm{Rad}(\kappa) \cdot p & \text{if } b = 0, \mathrm{ord}_5(\kappa) = 0 \\ 2^3 \cdot 5^2 \cdot \mathrm{Rad}(\kappa/5) \cdot q \cdot p & \text{if } b > 0, \mathrm{ord}_5(\kappa) = 1 \\ 2^3 \cdot 5^2 \cdot \mathrm{Rad}(\kappa/5) \cdot p & \text{if } b = 0, \mathrm{ord}_5(\kappa) = 1, \end{cases} \tag{51}$$

and

$$N' = \begin{cases} 2^3 \cdot 5 \cdot \mathrm{Rad}(\kappa) \cdot q & \text{if } 11 \nmid b, \mathrm{ord}_5(\kappa) = 0 \\ 2^3 \cdot 5 \cdot \mathrm{Rad}(\kappa) & \text{if } 11 \mid b, \mathrm{ord}_5(\kappa) = 0 \\ 2^3 \cdot 5^2 \cdot \mathrm{Rad}(\kappa/5) \cdot q & \text{if } 11 \nmid b, \mathrm{ord}_5(\kappa) = 1 \\ 2^3 \cdot 5^2 \cdot \mathrm{Rad}(\kappa/5) & \text{if } 11 \mid b, \mathrm{ord}_5(\kappa) = 1. \end{cases} \tag{52}$$

The Frey curve E_p has conductor N, and again it follows from the recipes of the first author and Skinner [5] that there is a normalized newform f as in (38) of weight 2 and level N' and a prime $\varpi \mid 11$ in the integers of $K = \mathbb{Q}(c_1, c_2, \dots)$ so that (39) holds.

Throughout what follows, ℓ will be a prime satisfying

$$\ell \nmid 2 \cdot 5 \cdot 11 \cdot \kappa \cdot q \cdot p. \tag{53}$$

As before (41) holds.

Lemma 8.3 *Let (p, b) be a solution to (49) and suppose $p \neq 3, 23$. Let ℓ be a prime satisfying (53). Let*

$$\mathcal{A}_\ell = \{(s,t) \ : \ s,\ t \in \mathbb{F}_\ell, \quad s \not\equiv 0 \mod \ell, \qquad t^4 - 3s^{11}t^2 + s^{22} \not\equiv 0 \mod \ell\},$$

and let $\mathcal{B}_\ell$ be as in (42). For $(s,t) \in \mathcal{B}_\ell$ let

$$E_{s,t,1}/\mathbb{F}_\ell \ : \ Y^2 = X(X^2 + (3s^{11} - 2t^2)X + t^4 - 3s^{11}t + s^{22})$$

and

$$E_{s,t,3}/\mathbb{F}_\ell \ : \ Y^2 = X(X^2 + (2t^2 - 3s^{11})X + t^4 - 3s^{11}t + s^{22}),$$

again corresponding to $p \equiv 1 \mod 4$ and $p \equiv 3 \mod 4$, respectively. Let f be a newform of weight 2 and level N' so that (39) is satisfied, and c_ℓ be its ℓ-th coefficient. For $j = 1, 3$, let $\mathcal{C}_{\ell,j}(f)$ be as in (43), and let

$$\mathcal{D}_{\ell,j}(f) = \{t^4 - 3s^{11}t^2 + s^{22} \ : \ (s,t) \in \mathcal{C}_{\ell,j}(f)\} \subseteq \mathbb{F}_\ell.$$

If $p \equiv 1 \mod 4$ then $(\kappa \cdot q^b \mod \ell) \in \mathcal{D}_{\ell,1}(f)$. If $p \equiv 3 \mod 4$ then $(\kappa \cdot q^b \mod \ell) \in \mathcal{D}_{\ell,3}(f)$.

Proof The proof is practically identical to that of Lemma 7.3. □

Lemma 8.4 *Let (p, b) be a solution to (49) with $p \neq 3, 23$. Let M be a positive integer satisfying $22 \mid M$. Let*

$$\mathcal{E} = \{0 \leq \beta \leq M - 1 \ : \ \kappa \cdot q^\beta \equiv 1 \mod 4\}.$$

Let f be a newform of weight 2 and level N' so that (39) is satisfied. Let

$$\mathcal{F}(f) = \begin{cases} \{\beta \in \mathcal{E} \ : \ 11 \nmid \beta\} & \text{if } N' = 2^3 \cdot 5 \cdot \mathrm{Rad}(\kappa) \cdot q \text{ or } 2^3 \cdot 5^2 \cdot \mathrm{Rad}(\kappa/5) \cdot q \\ \{\beta \in \mathcal{E} \ : \ 11 \mid \beta\} & \text{if } N' = 2^3 \cdot 5 \cdot \mathrm{Rad}(\kappa) \text{ or } 2^3 \cdot 5^2 \cdot \mathrm{Rad}(\kappa/5) \end{cases}$$

Let $\mathcal{L}$ be a set of primes satisfying

$$\ell \nmid 2 \cdot 5 \cdot 11 \cdot \kappa q p, \qquad O_\ell(q) \mid M. \tag{54}$$

For $\ell \in \mathcal{L}$ and $j = 1, 3$

$$\mathcal{G}_{\ell,j}(f) \ = \ \{\beta \in \mathcal{F}(f) \ : \ (\kappa \cdot q^\beta \bmod \ell) \in \mathcal{D}_{\ell,j}(f)\}.$$

Let

$$\mathcal{H}_j(f) \ = \ \bigcap_{\ell \in \mathcal{L}} \mathcal{G}_{\ell,j}(f).$$

If $p \equiv 1 \pmod 4$ *then there is some* $\beta \in \mathcal{H}_1(f)$ *such that* $b \equiv \beta \pmod M$. *If* $p \equiv 3 \pmod 4$ *then there is some* $\beta \in \mathcal{H}_3(f)$ *such that* $b \equiv \beta \pmod M$.

Proof This is almost identical to the proof of Lemma 7.4. The main difference is that the sets $\mathcal{E}, \mathcal{F}(f)$ do not depend on the class of p modulo 4, and we explain this now. Observe from (11) that

$$\kappa \cdot q^b = \tau(p^4) \equiv p^{44} + p^{33} + p^{22} + p^{11} + 1 \equiv 3 + 2p \equiv 1 \pmod 4$$

regardless of the residue class of p modulo 4. □

Lemma 8.5 *The equations* $\tau(p^4) = \pm 1$ *and* $\tau(p^4) = \pm 5$ *have no solutions with* p *prime.*

Proof From the proof of Lemma 8.4, we know that $\tau(p^4) \equiv 1 \pmod 4$. Thus we need only consider the equations $\tau(p^4) = 1$ and $\tau(p^4) = 5$. Suppose $\tau(p^4) = 1$ and write $z = 2\tau(p)^2 - 3p^{11}$. From (50) we have

$$z^2 - 5p^{22} = 4.$$

Write $\varepsilon = (1 + \sqrt{5})/2$. Then $(|z| + p^{11}\sqrt{5})/2$ is a positive unit in $\mathbb{Z}[\varepsilon]$ with norm $+1$. Hence

$$\frac{z + p^{11}\sqrt{5}}{2} = \varepsilon^{2n}, \qquad \varepsilon = (1 + \sqrt{5})/2.$$

for some $n \in \mathbb{Z}$. Thus

$$p^{11} = \frac{\varepsilon^{2n} - \overline{\varepsilon}^{2n}}{\sqrt{5}} = F_{2n}$$

where F_n denotes the n-th Fibonacci number. By [11] the only perfect powers in the Fibonacci sequence are 0, 1, 8 and 144, giving a contradiction. Alternatively, $F_{2n} = F_n L_n$ where L_n is the n-th Lucas number. From the identity $L_n^2 - 5F_n^2 = 4 \cdot (-1)^n$ we see that $\gcd(F_n, L_n) = 1$ or 2. Thus $F_n = 1$ or $L_n = 1$ quickly leading to a contradiction.

Next we suppose that $\tau(p^4) = 5$ and write $z = 5w$. Hence

$$5w^2 - p^{22} = 4$$

and it follows that there is an integer n such that

$$p^{11} = \varepsilon^n + \overline{\varepsilon}^n = L_n,$$

where L_n denotes the n-th Lucas number. By [11], the only perfect powers in the Lucas sequence are 1 and 4, again giving a contradiction. □

Proof of Proposition 8.1 We checked that (47) has no solutions with $p < 200$ for primes $3 \le q < 100$. We shall henceforth suppose that $p > 200$. In particular, $p \neq q$. Moreover, any solution to (47) is a solution to (49) with $\kappa = 1$ or -1.

We consider $q = 5$ first. By (50), $\mathrm{ord}_5(\tau(p^4)) = 0$ or 1. Thus we reduce to the equations $\tau(p^4) = \pm 1$ and $\tau(p^4) = \pm 5$. These do not have solutions by Lemma 8.5 and hence we may assume that $q \neq 5$. From Lemma 8.5 again we have $b > 0$. By (50), 5 is a quadratic residue modulo q. The possible values of q are

$$11,\ 19,\ 29,\ 31,\ 41,\ 59,\ 61,\ 71,\ 79,\ 89. \tag{55}$$

For each of these values we take

$$M = 396 = 2^2 \cdot 3^2 \cdot 11, \qquad \mathcal{L} = \{3 \le \ell < 200 \text{ prime}, \ell \neq 5, 11, q \ :\ O_\ell(q) \mid M\}. \tag{56}$$

Observe that since $p > 200$ that $\ell \neq p$, and thus satisfies (54).

We consider first the case $11 \nmid b$. Thus, in (52), the level $N' = 2^3 \cdot 5 \cdot q$. We computed for each newform f of level N' the sets $\mathcal{H}_1(f)$ and $\mathcal{H}_3(f)$, both for $\kappa = 1$, $\kappa = -1$. We found all of these to be empty. By Lemma 7.4, we conclude that (47) has no solutions with $11 \nmid b$.

Next we consider $11 \mid b$. Thus $N' = 2^3 \cdot 5$. There is a unique newform f of level N' which corresponds to the elliptic curve E with Cremona label `40a1` :

https://www.lmfdb.org/EllipticCurve/Q/40a1/

Thus, from (39) we obtain $\overline{\rho}_{E_p} \sim \overline{\rho}_E$. Note, by (51) that E_p has multiplicative reduction at q. However, E has good reduction at q. Thus, by [19], we have $\pm(q+1) \equiv a_q(E) \pmod{11}$. We checked that this does not hold for all the values of q in (55). This completes the proof. □

Proof of Proposition 8.2 Again we checked that (48) has no solutions with $p < 200$, whence we may suppose $p > 200$. Moreover, as 5 is a quadratic non-residue modulo 3 and 7, we see from (50) that $b_1 = b_3 = 0$ in (48). Also $5^2 \nmid \tau(p^4)$ from (50), so $b_2 = 0$ or 1. But from Proposition 8.1 we have $b_2 \neq 0$, and so $b_2 = 1$. We have thus reduced to consideration of the equation

$$\tau(p^4) = \pm 5 \cdot 11^b,$$

whereby we have $\kappa = \pm 5$ and $q = 11$. Observe that $b > 0$ by Lemma 8.5. Suppose $11 \nmid b$. Thus $N' = 8 \cdot 25 \cdot 11 = 2200$. We take M and $\mathcal{L}$ as in (56). There are 25 conjugacy classes of newforms f of weight 2 and level 2200. For each, we found $\mathcal{H}_1(f)$ and $\mathcal{H}_3(f)$ to be empty, both for $\kappa = 5$ and $\kappa = -5$. By Lemma 8.4, there are no solutions with $11 \nmid b$. Thus $11 \mid b$, and so $N' = 2^3 \cdot 25 = 200$. There are five weight 2 newforms of level 200. We computed $\mathcal{H}_1(f)$ and $\mathcal{H}_3(f)$ for these, both for $\kappa = 5$ and $\kappa = -5$. The only non-empty one we found was $\mathcal{H}_3(f)$ for $\kappa = 5$ where f is the rational newform corresponding to the elliptic curve E with Cremona label `200b1` :

https://www.lmfdb.org/EllipticCurve/Q/200b1/

Then $\overline{\rho}_{E_p,11} \sim \overline{\rho}_{E,11}$. Here E_p has multiplicative reduction at 11, though E has good reduction at 11. As before, $\pm(11+1) \equiv a_{11}(E) \mod 11$. However, $a_{11}(E) = -4$, giving a contradiction and completing the proof. □

9 On the largest prime divisor of $\tau(p^3)$

Proposition 9.1 *Let p be a prime for which $\tau(p) \neq 0$. Then $P(\tau(p^3)) \geq 13$, unless $p = 2$, in which case we have $\tau(8) = 2^9 \cdot 3 \cdot 5 \cdot 11$.*

We consider

$$P(\tau(p^3)) \leq 11. \tag{57}$$

We checked that the only $p < 200$ satisfying (57) is $p = 2$. We shall therefore suppose $p > 200$. Recall that $\tau(p^3) = \tau(p) \cdot (\tau(p)^2 - 2p^{11})$. From (12) and (14), we easily see that 3 and 7 do not divide $\tau(p)^2 - 2p^{11}$. Moreover, we recall that $\tau(p)$ is even, so $\mathrm{ord}_2(\tau(p)^2 - 2p^{11}) = 1$. Thus

$$\tau(p)^2 - 2p^{11} = \pm 2 \cdot 5^a \cdot 11^b \quad \text{and} \quad \tau(p) = \pm 2^r \cdot 3^s \cdot 5^t \cdot 7^u \cdot 11^v. \tag{58}$$

As before, we associate to this a Frey–Hellegouarch curve

$$E_p \ : \ Y^2 = X(X^2 + 2\tau(p)X + 2p^{11}).$$

By the recipes of the first author and Skinner, the conductor of E_p is one of

$$N = 2^8 \cdot p, \qquad 2^8 \cdot 5 \cdot p, \qquad 2^8 \cdot 11 \cdot p, \qquad 2^8 \cdot 5 \cdot 11 \cdot p,$$

and (39) holds for some weight 2 newform f whose level N' is one of the following

$$N' = 2^8, \qquad 2^8 \cdot 5, \qquad 2^8 \cdot 11, \qquad 2^8 \cdot 5 \cdot 11. \tag{59}$$

There are a total of 123 conjugacy classes of newforms f at these levels. Let f be any of these such that (39) holds. Let $\ell \neq 2, 5, 11$, p be a prime. Then $11 \mid \mathrm{Norm}(a_\ell(E_p) - c_\ell(f))$ where $c_\ell(f)$ is the ℓ-th coefficient of f.

Lemma 9.2 *Let $\ell \neq 2, 5, 11$ be a prime < 200. Let p be an odd prime with $\tau(p) \neq 0$ and $P(\tau(p^3)) \leq 11$. Let f be a newform of weight 2 and one of the levels N' in (59) so that (39) is satisfied. Write*

$$\mathcal{A}_\ell = \begin{cases} \{(s,t) \ : \ s,\ t \in \mathbb{F}_\ell, \quad s(t^2 - 2s^{11}) \not\equiv 0 \mod \ell\}, & \ell = 3,\ 7 \\ \{(s,t) \ : \ s,\ t \in \mathbb{F}_\ell, \quad st(t^2 - 2s^{11}) \not\equiv 0 \mod \ell\}, & \ell \geq 13. \end{cases}$$

Let $\mathcal{B}_\ell$ be as in (42). Let

$$E_{s,t}/\mathbb{F}_\ell \ : \ Y^2 = X(X^2 + 2tX + s^{11}),$$

and

$$\mathcal{C}_\ell(f) = \{(s,t) \in \mathcal{B}_\ell \ : \ \mathrm{Norm}(a_\ell(E_{s,t}) - c_\ell(f)) \equiv 0 \pmod{11}\}.$$

Then there is some $(s,t) \in \mathcal{C}_\ell(f)$ *so that* $(p, \tau(p)) \equiv (s,t) \pmod{\ell}$.

Proof This is is similar to the proof of Lemma 7.3. □

Proof of Proposition 9.1 For each of the 123 conjugacy classes of newforms f we computed $\mathcal{C}_\ell(f)$ for $\ell = 3$, 7, 13 and 23. We found that at least one of these four empty, except for the three rational newforms which correspond to the elliptic curves (in Cremona's labelling) `256a1`, `256b1` and `256c1` :

https://www.lmfdb.org/EllipticCurve/Q/?hst=List&conductor=256&search_type=List

All three elliptic curves have CM, respectively by $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-1})$. Note that 11 splits in $\mathbb{Q}(\sqrt{-2})$ and is inert in $\mathbb{Q}(\sqrt{-1})$. Hence the image of $\rho_{E_p,11} \sim \rho_{f,11}$ belongs to the normalizer of split Cartan subgroup in the first case, and the normalizer of a non-split Cartan subgroup in the second and third case. Thanks to the work of Momose [28], and Darmon and Merel [13, Theorem 8.1], the $j(E_p) \in \mathbb{Z}[1/11]$. However, E_p has multiplicative reduction at p giving a contradiction. □

10 Proof of Theorem 5

Lemma 10.1 *Let* $p \le 11$ *be a prime. Suppose* $P(\tau(p^{m-1})) \le 11$ *with* $m \ge 3$. *Then* $p = 2$ *and* $m = 4$.

Proof First let $p = 2$. Let $m \ge 3$ be such that $P(\tau(2^{m-1})) \le 11$. Note that $\tau(2) = -2^3 \times 3$. Let $\{u_n\}$ be the Lucas sequence defined in Lemma 3.4, with characteristic polynomial $X^2 - 3X + 2^5$. Then $P(u_m) \le 11$. Moreover, by part (i) of Theorem 8, we have $2 \nmid u_n$ for all $n \ge 1$. We note that

$$u_2 = -3, \quad u_3 = -23, \quad u_4 = 3 \times 5 \times 11, \quad u_5 = 241,$$
$$u_6 = -3^2 \times 23 \times 29, \quad u_7 = 7 \times 1471, \quad u_8 = 3 \times 5 \times 11 \times 977.$$

By the Primitive Divisor Theorem (Theorem 7), every term u_n with $n \ge 9$ is divisible by some prime $\ell \ge 13$. Thus the only terms with $P(u_n) \le 11$ are u_2 and u_4. Since $m \ge 3$ we have $m = 4$.

By a similar strategy we checked that $P(\tau(p^{m-1})) \ge 13$ for $3 \le p \le 11$ and $m \ge 3$. □

Lemma 10.2 *Let* p *be a prime. Let* $m \ge 3$ *be an integer such that* $\tau(p^{m-1}) \ne 0$ *and*

$$P(\tau(p^{m-1})) \le 11. \tag{60}$$

Then $p = 2$ *and* $m = 4$.

Proof By Lemma 10.1, we may suppose $p \geq 13$. If $\tau(p) = 0$, by Lemma 3.3, we have $\tau(p^{m-1}) = 0$ or a power of p contradicting the hypotheses of the lemma. We may therefore suppose $\tau(p) \neq 0$. Fix p and let m be the least value ≥ 3 such that (60) is satisfied. By Propositions 7.2, 8.2 and 9.1, we know that $m \geq 6$.

Suppose first that $p \mid \tau(p)$. By induction from (18) we have $p \mid \tau(p^n)$ for all $n \geq 1$. Hence $p \mid \tau(p^{m-1})$ and so $p \leq 11$ giving a contradiction. Thus $p \nmid \tau(p)$. Let $u_n = \tau(p^{n-1})$ for $n \geq 1$. Then $\{u_n\}$ is a Lucas sequence by Lemma 3.4. Now $u_k \mid u_n$ if $k \mid n$. As $m \geq 6$, it is divisible either by 4 or an odd prime. However $u_4 = \tau(p^3)$, and so $P(u_4) \geq 13$ by Proposition 9.1. Hence m is divisible by an odd prime, and from the minimality of m it follows that $m \geq 7$ is a prime. By the Primitive Divisor Theorem, $u_m = \tau(p^{m-1})$ has a prime divisor q that does not divide $u_1 u_2 \cdots u_{m-1}$ nor $D = (\alpha - \beta)^2$ (where α, β are as in Lemma 3.4). Here $q = 2, 3, 5, 7$ or 11. But m_q, the rank of apparition of q, divides m by Theorem 8, and so $m_q = m$. However $m_q \mid (q-1)(q+1)$, again from Theorem 8. But $(q-1)(q+1)$ is not divisible by a prime ≥ 7 for $q = 2, 3, 5, 7$ or 11. This contradiction completes the proof. □

Proof of Theorem 5 Suppose n is a powerful number such that $\tau(n) \neq 0$ and $P(\tau(n)) \leq 11$. Let p be a prime divisor of n. Thus $p^{m-1} \mid\mid n$, where, as n is powerful, $m \geq 3$. Now, as τ is multiplicative, $\tau(p^{m-1}) \neq 0$ and $\tau(p^{m-1}) \mid \tau(n)$. In particular, $P(\tau(p^{m-1})) \leq 11$. By Lemma 10.2 we have $p = 2$ and $m = 4$. Thus $n = 8$ as required. □

11 Proof of Theorem 6

Proof of Theorem 6 Suppose $\tau(n) = \pm q^\alpha$ where $3 \leq q < 100$ is a prime and $n \geq 2$. Then $\tau(n)$ is odd, and so n must be an odd square. Thus there is a prime p and an integer $m \geq 3$ such that $p^{m-1} \mid\mid n$. Hence $\tau(p^{m-1}) = \pm q^a$ for some $a \geq 0$. The following lemma completes the proof. □

Lemma 11.1 *Let $3 \leq q < 100$ be a prime and a be a nonnegative integer. Let p be a prime and $m \geq 3$ an odd integer. Then $\tau(p^{m-1}) \neq \pm q^a$.*

Proof We argue by contradiction. Suppose $m \geq 3$ is the smallest odd integer such that

$$\tau(p^{m-1}) = \pm q^a. \tag{61}$$

By Propositions 7.1 and 8.1, we have $m \geq 7$. We treat first the case $\tau(p) = 0$. By Lemma 3.3, we see that $\pm q^a = \tau(p^{m-1})$ is either 0 or a power of p. Thus $p = q < 100$, which gives a contradiction since any p for which $\tau(p) = 0$ satisfies (6). Thus $\tau(p) \neq 0$.

Let $\{u_n\}$ be the Lucas sequence given in Lemma 3.4. It follows from that lemma that $u_n \mid \tau(p^{n-1})$ and $p \nmid u_n$ for all $n \geq 1$. If $p = q$, then $u_m = \pm 1$ which contradicts the Primitive Divisor Theorem (Theorem 7), as $m \geq 7$. We conclude that $p \neq q$.

Next we consider the case $p \mid \tau(p)$. Then $p \mid \tau(p^n)$ for all $n \geq 1$ by (18), and so $p = q$, giving a contradiction. Thus $p \nmid \tau(p)$. It follows that $u_n = \tau(p^{n-1})$ for all $n \geq 1$. Recall that if $k \mid n$ then $u_k \mid u_n$. By the minimality of m we see that $m \geq 7$ is a prime. We invoke the Primitive Divisor Theorem again to conclude

that $q \nmid (\alpha - \beta)^2 u_1 u_2 \cdots u_{m-1}$ (in the notation of Lemma 3.4). From Theorem 8, $m = m_q \mid (q-1)(q+1)$. The possible pairs of primes (q, m) with $3 \le q < 100$ and $m \mid (q-1)(q+1)$ are

$$\begin{aligned}&(13,7),\ (23,11),\ (29,7),\ (37,19),\ (41,7),\ (43,7),\\ &\quad(43,11),\ (47,23),\ (53,13),\ (59,29),\\ &(61,31),\ (67,11),\ (67,17),\ (71,7),\ (73,37),\ (79,13),\\ &\quad(83,7),\ (83,41),\ (89,11),\ (97,7).\end{aligned}$$

Fixing any of these pairs (q, m), it remains to solve $\tau(p^{m-1}) = \pm q^a$. By Lemma 4.8, and the fact that m is prime, we see that $(X, Y, a) = (p^{11}, \tau(p), a)$ is a solution to the Thue–Mahler equation

$$\Psi_m(X, Y) = \pm q^a.$$

We solved these Thue–Mahler equations using the `Magma` implementation of the Thue–Mahler solver described in [17]. None of the solutions are of the form $(p^{11}, \tau(p), a)$. This completes the proof of Theorem 6. We illustrate this by providing more details for the case $q = 83$. Here m is a prime ≥ 7 dividing $83^2 - 1 = 2^3 \times 3 \times 7 \times 41$, and thus the possible pairs (q, m) are $(83, 7)$ and $(83, 41)$. For the first pair, the Thue–Mahler equation is

$$-X^3 + 6X^2Y - 5XY^2 + Y^3 = 83^a,$$

and the solutions are

$$\begin{aligned}&(X, Y, a)\\ &\quad= (5,1,0),\ (-9,-14,0),\ (2,3,0),\ (-7,-1,1),\ (5,2,1),\ (0,1,0),\\ &\qquad(-1,-2,0),(-17,-38,2),\ (-8,-13,1),\ (13,20,1),\ (1,1,0),\ (4,13,0),\\ &\qquad(-6,-19,1),\ (-1,0,0),\ (21,25,2),\\ &\qquad(3,11,1),\ (-4,13,2),\ (-1,-3,0),\ (-5,-2,1),\ (0,-1,0),\\ &\qquad(17,38,2),\ (6,19,1),\ (7,1,1),\\ &\qquad(1,0,0),\ (-4,-13,0),\ (4,-13,2),\ (9,14,0),\ (-3,-11,1),\\ &\qquad(1,3,0),\ (-1,-1,0),\\ &\qquad(-13,-20,1),\ (-5,-1,0),\ (-21,-25,2),\ (8,13,1),\ (1,2,0),\ (-2,-3,0).\end{aligned}$$

For the pair $(q, m) = (83, 41)$ the Thue–Mahler equation is

$$\begin{aligned}&X^{20} - 210X^{19}Y + 7315X^{18}Y^2 - 100947X^{17}Y^3 + 735471X^{16}Y^4 - 3268760X^{15}Y^5\\ &\quad+9657700X^{14}Y^6 - 20058300X^{13}Y^7 + 30421755X^{12}Y^8\\ &\quad-34597290X^{11}Y^9 + 30045015X^{10}Y^{10}\\ &\quad-20160075X^9Y^{11} + 10518300X^8Y^{12} - 4272048X^7Y^{13}\end{aligned}$$

$$+1344904X^6Y^{14} - 324632X^5Y^{15}$$
$$+58905X^4Y^{16} - 7770X^3Y^{17} + 703X^2Y^{18} - 39XY^{19} + Y^{20} = \pm 83^a,$$

and the solutions are

$$(-1,-3,0),\ (-1,-2,0),\ (1,2,0),\ (1,0,0),\ (-1,0,0),$$
$$(1,3,0),\ (0,1,0),\ (0,-1,0),\ (1,1,0),\ (-1,-1,0).$$

□

Remark. The aforementioned Thue–Mahler solver requires knowledge of the class group and unit group of the number field defined by the equation $\Psi_m(1, Y) = 0$; this number field has degree $\phi(m)/2 = (m-1)/2$. Ordinarily, if the degree is too large, this might not be practical, or might require assuming the Generalized Riemann Hypothesis. However, from Lemma 4.5, this number field is $\mathbb{Q}(\zeta_m)^+$. For the values of m under consideration (and in fact for all prime $m \leq 67$), the class number h_m^+ of $\mathbb{Q}(\zeta_m)^+$ is known to be 1; see for example [22, Theorem 1]. Moreover, if we denote the unit group of $\mathbb{Q}(\zeta_m)^+$ by E_m^+ and the subgroup of cyclotomic units by C_m^+ then $[E_m^+ : C_m^+] = h_m^+$; see [39, Theorem 8.2]. Hence in all our cases, $E_m^+ = C_m^+$, and is generated [39, Lemma 8.1] by -1 and $(1-\zeta_m^a)/(1-\zeta_m)$ with $1 < a < m/2$. Thus for all values of m under consideration we know the class group and unit group.

12 Concluding remarks

As noted in the introduction, it would likely be extremely challenging computationally to extend, for example, Corollary 1.1 to explicitly find all n with $\tau(n)$ odd and, say,

$$P(\tau(n)) \leq 17.$$

The bottleneck in our approach is related to the difficulty involved in classifying the primes p for which $P(\tau(p^2))$ and $P(\tau(p^4))$ are "small". For larger exponents m, finding the p with $P(\tau(p^m))$ bounded appears to be somewhat more tractable. By way of example, we may show, by direct application of the Thue-Mahler solver described in [17], the following result.

Proposition 12.1 *The equation*

$$\tau(p^6) = \pm 3^{b_1}5^{b_2}7^{b_3}11^{b_4}13^{b_5}17^{b_6}19^{b_7}23^{b_8}29^{b_9}31^{b_{10}}37^{b_{11}}41^{b_{12}},$$
$$p \text{ prime}, \quad b_i \in \mathbb{Z} \tag{62}$$

has no solutions.

This amounts to solving the Thue-Mahler equation

$$-X^3 + 6X^2Y - 5XY^2 + Y^3$$
$$= \pm 3^{b_1}5^{b_2}7^{b_3}11^{b_4}13^{b_5}17^{b_6}19^{b_7}23^{b_8}29^{b_9}31^{b_{10}}37^{b_{11}}41^{b_{12}}$$

and checking to see if any solutions have $X = p^{11}$ for some prime p. Appealing to [17], we find that all solutions in coprime integers X and Y have either $\max\{|X|, |Y|\} < 1000$, or satisfy

$$\pm(X, Y) \in \{(241, 1111), (303, 2675), (373, 1212), (383, 1243), (547, 1530), (578, 1171), (643, 1060), (839, 1305), (860, 1337), (870, 1499), (983, 1419), (1061, 3530), (1095, 4577), (1376, 4467), (1408, 347), (1715, 339), (1793, -634), (1855, 6023), (2069, 1766), (2313, 458), (2372, 4441), (2387, 1292), (2427, 6647), (2469, 3877), (3091, 4806), (3482, 5869), (4168, 6481), (4220, 6013)\}.$$

Acknowledgements Readers interested in these computations may contact us for further details. For technical publishing purposes, there is no "associated data".

References

1. Balakrishnan, J.S., Craig, W., Ono, K.: Variations of Lehmer's conjecture for Ramanujan's tau-function, J. Number Theory (to appear)
2. Balakrishnan, J.S., Craig, W., Ono, K., Tsai, W.-L.: Variants of Lehmer's speculation for newforms. (submitted for publication)
3. Barros, C.F.: On the Lebesgue-Nagell equation and related subjects, PhD thesis, University of Warwick, (2010)
4. Bennett, M.A.: Rational approximation to algebraic numbers of small height : the Diophantine equation $|ax^n - by^n| = 1$. J. Reine Angew. Math. **535**, 1–49 (2001)
5. Bennett, M.A., Skinner, C.: Ternary Diophantine equations via Galois representations and modular forms. Can. J. Math. **56**(1), 23–54 (2004)
6. Bennett, M.A., Dahmen, S., Mignotte, M., Siksek, S.: Shifted powers in binary recurrence sequences. Math. Proc. Camb. Philos. Soc. **158**, 305–329 (2015)
7. Bilu, Y., Hanrot, G., Voutier, P.: Existence of primitive divisors of Lucas and Lehmer numbers. J. Reine Angew. Math. **539**, 75–122 (2001)
8. Bosma, W., Cannon, J., Playoust, C.: The magma algebra system i: the user language. J. Symb. Comp. **24**, 235–265. (1997) (See also http://magma.maths.usyd.edu.au/magma/). Accessed July 2021
9. Bugeaud, Y.: On the greatest prime factor of $ax^m - by^n$ II. Bull. Lond. Math. Soc. **32**(6), 673–678 (2000)
10. Bugeaud, Y., Győry, K.: Bounds for the solutions of Thue–Mahler equations and norm form equations. Acta Arith. **74**, 273–292 (1996)
11. Bugeaud, Y., Mignotte, M., Siksek, S.: Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers. Ann. Math. **163**, 969–1018 (2006)
12. Carmichael, R.D.: On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. Ann. Math. **15**, 30–70 (1913)
13. Darmon, H., Merel, L.: Winding quotients and some variants of Ferma's Last Theorem. J. Reine Angew. Math. **490**, 81–100 (1997)
14. Deligne, P.: La conjecture de Weil I. Inst. Hautes Études Sci. Publ. Math. **43**, 273–307 (1974)
15. Dembner, S., Jain, V.: Hyperelliptic curves and newform coefficients. J. Number Theory **225**, 214–239 (2021)
16. Derickx, M., Van Hoeij, M., Zeng, Jinxiang: Computing Galois representations and equations for modular curves $X_H(\ell)$, arXiv:1312.6819v2
17. Gherga, A., von Känel, R., Matschke, B., Siksek, S.: Efficient resolution of Thue–Mahler equations. (to appear)
18. Hanada, M., Madhukara, R.: Fourier coefficients of level 1 Hecke eigenforms. Acta Arith. (to appear)
19. Kraus, A., Oesterlé, J.: Sur une question de B. Mazur. Math. Ann. **293**, 259–275 (2002)

20. Lehmer, D.H.: The vanishing of Ramanujan's function $\tau(n)$. Duke Math. J. **14**, 429–433 (1947)
21. Lenstra, H.W.: Algorithms in algebraic number theory. Bull. Am. Math. Soc. **26**, 211–244 (1992)
22. van der Linden, F.J.: Class number computations of real abelian number fields. Math. Comput. **39**, 693–707 (1982)
23. The LMFDB Collaboration, The L-functions and modular forms database (2021). http://www.lmfdb.org, Online; Accessed 7 July 2021
24. Luca, F., Mabaso, S., Stanica, P.: On the prime factors of the iterates of the Ramanujan τ-function. Proc. Edinburgh Math. Soc. Acta Arithmetica **63**, 1031–1047 (2020)
25. Luca, F., Shparlinski, I.E.: Arithmetic properties of the Ramanujan function. Proc. Indian Acad. Sci. (Math. Sci.) **116**, 1–8 (2006)
26. Lygeros, N., Rozier, O.: A new solution to the equation $\tau(p) \equiv 0 \ mod \ p$. J. Integer Seq. 13, Article 10.7.4 (2010)
27. Lygeros, N., Rozier, O.: Odd prime values of the Ramanujan tau function. Ramanujan J. **32**, 269–280 (2013)
28. Momose, F.: Isogenies of prime degree over number fields. Compos. Math. **97**, 329–348 (1995)
29. Mordell, L.J.: On Mr. Ramanujan's empirical expansions of modular functions. Proc. Camb. Philos. Soc. **19**, 117–124 (1917)
30. Ono, K., Taguchi, Y.: 2-adic properties of certain modular forms and their applications to arithmetic functions. Int. J. Number Theory **1**, 75–101 (2005)
31. Ram Murty, M., Kumar Murty, V.: Odd values of Fourier coefficients of certain modular forms. Int. J. Number Theory **3**, 455–470 (2007)
32. Ram Murty, M., Kumar Murty, V., Shorey, T.N.: Odd values of the Ramanujan τ-function. Bull. Soc. Math. France **115**, 391–395 (1987)
33. Ramanujan, S.: On certain arithmetical functions. Trans. Camb. Philos. Soc. **22**, 159–184 (1916)
34. Serre, J.-P.: Divisibilité de certaines fonctions arithmétiques. L'Ens. Math. **22**(176), 227–260 (1974)
35. Siksek S: The modular approach to diophantine equations. In: Belabas, et al. (eds.) Explicit Methods in Number Theory: Rational Points and Diophantine Equations. Panoramas et synthèses, vol. 36. (2012)
36. Smart, N.P.: The Algorithmic Resolution of Diophantine Equations. Cambridge University Press, Cambridg (1998)
37. Stewart, C.L.: On divisors of Lucas and Lehmer numbers. Acta Math. **211**, 291–314 (2013)
38. Swinnerton-Dyer, H.P.F.: On ℓ-adic representations and congruences for coefficients of modular forms, page 1–55 of W. Kuyk and J.-P. Serre (eds.), Modular functions of one variable, III, Lecture Notes in Mathematics 350, (1973)
39. Washington, L.C.: Introduction to Cyclotomic Fields. Springer, Berlin (1982)