

On Some Inadmissible Values of the Fourier Coefficients of Some Cusp Forms with Level 1 or 2

後藤, 新裕

<https://hdl.handle.net/2324/7396163>

出版情報 : Kyushu University, 2025, 博士 (数理学), 課程博士
バージョン :
権利関係 :



On Some Inadmissible Values of the Fourier Coefficients of Some Cusp Forms with Level 1 or 2

AKIHIRO GOTO

Abstract

Let f be either the newform Δ of weight 12 and level 1, or the newform φ_8 of weight 8 and level 2. As a variation of Lehmer's conjecture, we prove that for all odd primes $\ell < 1000$, the Fourier coefficients $a_f(n)$ of f never take the values

$$\pm\ell, \pm 2\ell, \pm 4\ell, \pm 8\ell$$

except for those ℓ belonging to an explicit finite subset L of odd primes less than 1000.

Contents

Introduction and the main results	2
1 Modular Forms	8
1.1 Congruence Subgroups and Modular Curves	8
1.2 Modular forms and cusp forms	10
1.3 Hecke operators	14
1.4 Newforms and old forms	16
1.5 Fourier coefficients modulo some prime powers	16
2 Lucas sequences	19
2.1 Some basic properties of Lucas sequences	19
2.2 The Lucas sequences from a Hecke eigenform	22
3 Other methods	25
3.1 Thue equation	26
3.2 Dembner–Jain's method	27
4 Proofs	28
4.1 Part (a)	28
4.2 Part (b)	29
A Some congruences for $a_f(p^{d-1})$ at some prime powers	30

B	Tables	32
B.1		32
B.2		36

Introduction and the main results

Ramanujan's τ -function ([24]) is defined by

$$x \prod_{n=1}^{\infty} (1 - x^n)^{24} = \sum_{n=1}^{\infty} \tau(n) x^n.$$

For each $n \geq 1$, the value $\tau(n)$ is an integer. By setting $x = e^{2\pi iz}$, where z is any complex number with $\text{Im}(z) > 0$, this defines the newform Δ of weight 12 and level 1. Ramanujan computed many values of $\tau(n)$ and conjectured the following:

- Theorem 0.1** (Ramanujan's conjecture, 1916). (1) $\tau(nm) = \tau(n)\tau(m)$, $\gcd(n, m) = 1$,
(2) $\tau(p^{m+1}) = \tau(p)\tau(p^m) - p^{11}\tau(p^{m-1})$ for p prime and $m \geq 1$,
(3) $|\tau(p)| \leq 2p^{11/2}$ for p prime.

The first two assertions, (1) and (2), were proven by Mordell [21], who used operators now known as Hecke operators. The third statement (3) was proven by Deligne [8, 9] as a corollary of the Weil conjecture.

In 1947, Lehmer [17] conjectured that $\tau(n) \neq 0$ for all $n \geq 1$. This conjecture remains open. Lehmer [17] also proved that if there exists an integer n such that $\tau(n) = 0$, then there must exist a prime p for which $\tau(p) = 0$. Later, Serre [26] proved that the set of primes p satisfying $\tau(p) = 0$ has natural density zero among all primes. This result is now a corollary of the Sato–Tate conjecture (now a theorem) (0.1).

Since the value $\tau(p)$ is a real number (in fact, an integer), we may write

$$\tau(p) = 2p^{11/2} \cos \theta_p$$

for some real number $0 \leq \theta_p \leq \pi$. The Sato–Tate conjecture, proven by Barnett-Lamb, Geraghty, Harris, and Taylor [5], asserts that for any $0 \leq \alpha < \beta \leq \pi$, we have

$$\lim_{x \rightarrow \infty} \frac{\#\{p \leq x \mid p \text{ prime}, \alpha \leq \theta_p \leq \beta\}}{\#\{p \leq x \mid p \text{ prime}\}} = \frac{2}{\pi} \int_{\alpha}^{\beta} \sin^2 \theta d\theta. \quad (0.1)$$

This implies that the angles θ_p are most likely to occur near $\pi/2$. However, Lehmer's conjecture is equivalent to the statement that $\theta_p \neq \pi/2$ for all primes p .

Recently, Newton and Thorne [23] proved that the n -th symmetric power L -function of Δ (more generally, of any non-CM newform) coincides with the L -function of an automorphic representation of $\text{GL}_n(\mathbb{A}_{\mathbb{Q}})$ for any $n \geq 1$, where $\mathbb{A}_{\mathbb{Q}}$ denotes the ring of adèles over $\mathbb{Q}$. Using this result, Thorner [28] established an effective form of the Sato–Tate theorem (0.1):

$$\frac{\#\{p \leq x \mid p \text{ prime}, \alpha \leq \theta_p \leq \beta\}}{\#\{p \leq x \mid p \text{ prime}\}} = \frac{2}{\pi} \int_{\alpha}^{\beta} \sin^2 \theta d\theta + O\left(\frac{\log(12 \log x)}{\sqrt{\log x}}\right), x \rightarrow \infty,$$

for any $0 \leq \alpha < \beta \leq \pi$. Using this estimate, Gafni, Thorner, and Wong [11] proved that, outside a density zero subset $S(\Delta)$ of primes, the inequality

$$2p^{\frac{11}{2}} \cdot \frac{\log \log p}{\sqrt{\log p}} < |\tau(p)| \quad (0.2)$$

holds. This implies that the Atkin–Serre conjecture is true for all but a density zero subset of primes.

Conjecture 0.2 (Atkin–Serre [25]). For each $\varepsilon > 0$, there exist constants $c_\varepsilon, c'_\varepsilon > 0$ such that for all primes $p > c'_\varepsilon$, the inequality

$$|\tau(p)| \geq c_\varepsilon p^{\frac{9}{2}-\varepsilon}$$

holds.

The above breakthrough results are highly nontrivial, and the methods used in their proofs vary considerably. However, they provide no information about the individual values of $\tau(n)$. In recent years, therefore, there has been growing interest in studying the behavior of these individual values.

In particular, as a variation of Lehmer’s conjecture, one may ask whether there exists a nonzero integer that never appears as a value of $\tau(n)$. Murty, Murty, and Shorey [22] showed that for any odd integer a , the equation $\tau(n) = a$ holds for at most finitely many n . In 2013, Lygeros and Rozier [20] proved that $\tau(n) \neq \pm 1$ for any $n > 1$ (noting that $\tau(1) = 1$). In 2022–2023, Balakrishnan, Ono, Craig, and Tsai [2, 3] proved that the following integers are not values of $\tau(n)$:

$$\pm 3, \pm 5, \pm 7, \pm 13, \pm 17, -19, \pm 23, \pm 37, \pm 691.$$

Hanada and Madhukara [13] further proved that the following values also never occur as $\tau(n)$:

$$-9, \pm 15, \pm 21, -25, -27, -33, \pm 35, \pm 45, \pm 49, -55, \pm 63, \pm 77, -81, \pm 91$$

Dembner and Jain [10] proved that for any $n > 1$,

$$\tau(n) \notin \{\pm \ell \mid \ell < 100, \text{ odd prime}\} \cup \{\pm 5^m \mid m \geq 0\}. \quad (0.3)$$

Bennett, Gherga, Patel, and Siksek [6, Corollary 1.1 and Theorem 6] proved that for $n > 1$,

$$\tau(n) \neq \pm \ell^a, 3^b 5^c 7^d 11^e,$$

where ℓ is an odd prime less than 100, and $a, b, c, d, e \geq 0$. Lin and Ma [19, Corollary 1.3] proved that if $\tau(n)$ is odd and $n > 3$, then

$$|\tau(n)| > |\tau(3)| = 252.$$

These results concerning the odd values of $\tau(n)$ rely on the following congruence:

$$\Delta(z) \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod{2}, \quad (0.4)$$

which can be proven using Jacobi's triple product identity.

On the other hand, regarding even values of $\tau(n)$, Balakrishnan, Ono, and Tsai [4] proved that if $\ell < 100$ is an odd prime, then for all $n \geq 1$,

$$\tau(n) \notin \{\pm 2\ell\} \cup \{\pm 2\ell^2\} \cup \{\pm 2\ell^3 \mid \ell \neq 59\}. \quad (0.5)$$

As a general result concerning the number of prime divisors of $\tau(n)$, the following theorem was proved:

Theorem 0.3 ([3]). Let $\sigma_0(n)$ denote the number of positive divisors of n , as usual. Define $\omega(n)$ (resp. $\Omega(n)$) as the number of distinct prime divisors of n (resp. counted with multiplicity). Then for all $n \geq 1$, we have

$$\Omega(\tau(n)) \geq \sum_{i=1}^r (\sigma_0(d_i) - 1) \geq \omega(n),$$

where $n = p_1^{d_1-1} \cdots p_r^{d_r-1}$, and each p_i is an *ordinary prime*, meaning that $p_i \nmid \tau(p_i)$.

Remark 0.4. The inequality $\Omega(\tau(n)) \geq \omega(n)$ still holds even when $n \geq 1$ is divisible by some non-ordinary prime p , because for any prime power $q > 1$, we have $|\tau(q)| > 1$ (by (0.3)), and τ is multiplicative (Theorem 1.6 (1)).

In this paper, motivated by the above results, we investigate further integers that do not lie in the image of the τ -function. To state the main theorems, we define the following sets:

$$\begin{aligned} L(\Delta)_1^+ &:= \{461\}, & L(\Delta)_1^- &:= \{599\}, \\ L(\Delta)_2^+ &:= \emptyset, & L(\Delta)_2^- &:= \{587\}, \\ L(\Delta)_4^+ &:= \{23, 449, 569, 863\}, & L(\Delta)_4^- &:= \{241, 397, 811\}, \\ L(\Delta)_8^+ &:= \{457\}, & L(\Delta)_8^- &:= \{3, 293, 983\}. \end{aligned}$$

Let $\ell < 1000$ be an odd prime and let $\varepsilon = \pm$ be a sign. Then, the following theorem, together with Theorem B below, constitutes our main results:

Theorem A. Suppose $\tau(n) = \varepsilon t \ell$, where $t = 1, 2, 4$, or 8 .

(a) If $t = 1$, then $n = p^4$ for some prime p , and $\ell \in L_1^\varepsilon$.

(b) If $t = 2, 4$, or 8 , then one of the following holds:

- (1) There exists a prime $p \mid n$ such that $\tau(p) = 2$ and $\gcd(p, n/p) = 1$.
- (2) n is prime and $\ell \in L_t^\varepsilon$.

Remark 0.5. Let $\ell < 1000$ be an odd prime. By Theorem A, if $\tau(n) = \pm \ell$, then $\pm \ell$ must be either 461 or -599 , and $n = p^4$ for some prime p . For each of $\pm \ell = 461$ or -599 , [3, Theorem 1.1] implies that there is at most one prime p such that $\tau(p^4) = \pm \ell$.

Proposition 0.6 ([3, Theorem 1.1]). For any odd ordinary prime ℓ , if $\tau(n) = \pm \ell^m$, with $m \geq 1$, then $n = p^{d-1}$, where p and d are odd primes with $d \mid \ell(\ell^2 - 1)$.

In fact, we have

$$\begin{aligned}\tau(461) &= -729307946668938 = -2 \cdot 3 \cdot 7 \cdot 13 \cdot 17 \cdot 78572284709 \\ \tau(599) &= -1701984261329400 = -2^3 \cdot 3 \cdot 5^2 \cdot 31 \cdot 757 \cdot 1483 \cdot 81509,\end{aligned}$$

which shows that the primes 461 and 599 are ordinary, that is, primes ℓ such that $\ell \nmid \tau(\ell)$. Suppose, for contradiction, that there exist two distinct primes p_1 and p_2 such that $\tau(p_1^4) = \tau(p_2^4) = 461$. Then, by the multiplicativity of τ , we have $\tau(p_1^4 p_2^4) = 461^2$. However, by the above proposition, $\tau(n) = 461^2$ can occur only when n is a prime power, which contradicts the fact that $p_1^4 p_2^4$ is not a prime power. Therefore, we conclude that there is at most one prime p such that $\tau(p^4) = 461$. The case of $\pm\ell = -599$ can be treated in the same way.

In [3], the authors gave a proof of Theorem 1.1 (or Theorem 3.2) only in the case of $m = 1$, where m appears in the above proposition. It is unclear, however, at least to the present author, whether their argument works for the general case.

For example, if $\tau(n) = -4\ell$, then using distinct primes p_1, p_2, p_3 , we can write

$$n = \begin{cases} p_1 p_2 p_3^4 & \text{with } \tau(p_1) = \tau(p_2) = 2, \tau(p_3^4) = -599, \\ p_1 p_2 & \text{with } \tau(p_1) = 2, \tau(p_2) = -2 \cdot 587, \\ p_1 & \text{with } \ell = 241, 397, 811. \end{cases}$$

Remark 0.7. (1) In each case, certain congruence conditions must be satisfied by the relevant prime p . For example, if $\tau(p) = -2 \cdot 587$, then the prime p must satisfy

$$p \equiv \begin{cases} 1 & \text{mod } 3, \\ -7 & \text{mod } 16, \\ 2 & \text{mod } 5, \\ 1 & \text{mod } 7, \end{cases}$$

and additionally, $(p/23) = 1$ (where $(\cdot)$ denotes the Legendre symbol), and p cannot be written in the form $a^2 + 23b^2$ with $a, b \in \mathbb{Z}$. See also equation (1.5) or the more convenient Lemma A.2.

Among the values $\varepsilon t \ell$ in Theorem A, only $-8 \cdot 3 (= \tau(2))$ is confirmed to actually occur. The first examples of values of the form $\tau(n) = \pm 2\ell, \pm 4\ell, \pm 8\ell$, with ℓ an odd prime and $n > 2$, are as follows:

$$\begin{aligned}\tau(277) &= -2 \cdot 8209466002937, & \tau(1297) &= 2 \cdot 58734858143062873, \\ \tau(163) &= -4 \cdot 89458189897, & \tau(4603) &= 4 \cdot 56958468932026008713, \\ \tau(967) &= 8 \cdot 2311913038549627, & \tau(2647) &= 8 \cdot 1344910678663379137.\end{aligned}$$

Moreover, we also consider the function

$$\varphi_8(z) := q \prod_{n=1}^{\infty} (1 - q^n)^8 (1 - q^{2n})^8, \text{ where } q := e^{2\pi i z}.$$

This defines the newform of weight 8 and level 2. Let

$$\varphi_8(z) = \sum_{n=1}^{\infty} a_{\varphi_8}(n)q^n$$

be its Fourier expansion.

To state our second main theorem on inadmissible values of a_{φ_8} , we define the following sets:

$$LD(\varphi_8)_1^+ := \{(\ell, d) \mid d \in C(\ell) \setminus \{7, 11, 13, 17, 19, 23, 29, 31, 37\}\},$$

$$LD(\varphi_8)_1^- := \{(\ell, d) \mid d \in C(-\ell) \setminus \{7, 11, 13, 17, 19, 23, 29, 31, 37\}\},$$

$$L(\varphi_8)_2^+ := \{3, 13, 31, 43, 61, 73, 103, 151, 163, 181, 193, 211, 223, 241, 271, 283, 313, 331, 373, 421, \\ 433, 463, 523, 541, 571, 601, 613, 631, 643, 661, 673, 691, 733, 751, 811, 823, 853, 883, 991\},$$

$$L(\varphi_8)_2^- := \{7, 31, 37, 61, 67, 97, 127, 151, 157, 181, 211, 241, 271, 277, 307, 331, 337, 367, 397, 421, \\ 457, 487, 541, 547, 571, 577, 601, 607, 631, 661, 691, 727, 751, 757, 787, 811, 877, 907, 937, \\ 967, 991, 997\},$$

$$L(\varphi_8)_4^+ := \{3, 5, 23, 29, 53, 59, 83, 89, 113, 149, 173, 179, 233, 239, 263, 269, 293, 353, 359, 383, 389, 419, \\ 443, 449, 479, 503, 509, 563, 569, 593, 599, 653, 659, 683, 719, 743, 773, 809, 839, 863, 929, \\ 953, 983\},$$

$$L(\varphi_8)_4^- := \{7, 31, 37, 61, 67, 97, 127, 151, 157, 181, 211, 241, 271, 277, 307, 331, 337, 367, 397, 421, 457, \\ 487, 541, 547, 571, 577, 601, 607, 631, 661, 691, 727, 751, 757, 787, 811, 877, 907, 937, 967, \\ 991, 997\},$$

$$L(\varphi_8)_8^+ := \{7, 19, 37, 67, 79, 97, 109, 127, 139, 157, 199, 229, 277, 307, 337, 349, 367, 379, 397, 409, 439, \\ 457, 487, 499, 547, 577, 607, 619, 709, 727, 739, 757, 769, 787, 829, 859, 877, 907, 919, 937, \\ 967, 997\},$$

$$L(\varphi_8)_8^- := \{3, 5, 11, 23, 41, 53, 71, 83, 101, 113, 131, 173, 191, 233, 251, 263, 281, 293, 311, 353, 383, 401, \\ 431, 443, 461, 491, 503, 521, 563, 593, 641, 653, 683, 701, 743, 761, 773, 821, 863, 881, 911, \\ 941, 953, 971, 983\},$$

where the set $C(\pm\ell)$ consists of those odd primes d such that the equation $\tau(p^{d-1}) = \pm\ell$ satisfies the congruences given in Lemma A.1 (1).

Theorem B. Let $f = \varphi_8$. Suppose $a_f(n) = \varepsilon t \ell$, where $t = 1, 2, 4$, or 8 , $\varepsilon = \pm$, and $\ell < 1000$ is an odd prime.

(a) If $t = 1$, then $n = p^{d-1}$ for some prime p , and $(\ell, d) \in LD(\varphi_8)_1^\varepsilon$.

(b) If $t = 2, 4$, or 8 , then one of the following holds:

(1) There exists a prime $p \mid n$ such that $a_f(p) = 2, -4$, and $\gcd(p, n/p) = 1$.

(2) n is prime and $\ell \in L(\varphi_8)_t^\varepsilon$.

The proof of the main results combines several tools developed in previous works, including [2, 3, 4, 10]. For simplicity, we describe the argument in the case of the τ -function. If $\tau(n) = \pm\ell$, where $\ell < 1000$ is an odd prime, it suffices to consider only the values of τ at prime powers $n = p^{d-1}$, since τ is multiplicative. In many cases, the values of τ at prime powers form a *Lucas sequence*. By applying the propositions introduced in Chapter 2, we reduce to considering only finitely many pairs (ℓ, d) . Furthermore, Ramanujan's congruence (1.5) allows us to further eliminate certain pairs (ℓ, d) . Finally, we treat each remaining case individually: for $d > 5$, we apply methods solving Thue equations; for $d = 5$, we use the method of Dembner and Jain [10]. As a result of this case-by-case analysis, the only remaining possibilities are $\pm\ell = 461$ and -599 .

In the even case, if $\tau(n) = \pm 2\ell$, $\pm 4\ell$, or $\pm 8\ell$, we make use of the following lemma:

Lemma (Lemma 2.14). Let p and ℓ be primes with $\ell \neq 2$, and let $d \geq 1$. If

$$\tau(p^{d-1}) = \pm 2\ell, \pm 4\ell, \pm 8\ell,$$

we have

$$d = \begin{cases} 2, & \text{if } \tau(p^{d-1}) = \pm 2\ell, \pm 8\ell, \\ 2, 4, & \text{if } \tau(p^{d-1}) = \pm 4\ell. \end{cases}$$

Moreover, if $d = 4$, then we have

$$(\tau(p), \varepsilon, \ell) = (2, -, p^{11} - 2)$$

We now remark on the relationship between our main result and the Atkin–Serre conjecture. For simplicity, we focus on the case of Δ . The quantity

$$2p^{\frac{11}{2}} \cdot \frac{\log \log p}{\sqrt{\log p}}$$

in (0.2) increases monotonically with respect to p , and exceeds 42442 for all $p \geq 7$. Therefore, if $\tau(p) = \varepsilon t \ell$ for some $\ell \in L(f)_t^\varepsilon$ and some odd prime p , then p must lie in $S(\Delta)$, defined as the set of primes for which the inequality (0.2) fails.

Finally, based on our computations, the prime factorizations of $a_f(n)$ for $f = \Delta$ or φ_8 do not have a simple form. It appears that the factorizations typically involve a few small primes together with a single large prime.

Acknowledgments

First of all, I would like to express my deepest gratitude to my academic advisor, Professor Masanobu Kaneko. Although he began supervising me from the start of my doctoral course, he always treated me with respect and provided delicate and thoughtful guidance throughout the past three and a half years. At times, Professor Toshiki Matsusaka also kindly offered guidance on his behalf. Thanks to their support, I was able to significantly broaden the scope of my research methods and bring this thesis to completion.

I am also deeply grateful to Kyosuke Imanaka, a junior colleague from Doshisha University and Kyoto University. It was through him that I encountered this research topic. He not only

answered my questions about research methodologies but also presented valuable problems for exploration. Likewise, I am sincerely thankful to Mr. Keiichiro Nomoto, my senior colleague, who assisted me in resolving several technical challenges related to computation.

I extend my thanks to Katsumi Kina and Naoki Sugibayashi, my juniors in the laboratory. Through our voluntary study sessions, I was able to learn about a wide of topics. The knowledge I cultivated during those times are, I believe, lifelong assets.

Furthermore, I would like to express my gratitude to Ryota Shii, Taiga Adachi, Atsuki Kuramoto, Ryohei Fujii, Masaya Miyazaki, and Shoma Sueyoshi, who supported me in my personal life. The time we spent together in the graduate student office was truly meaningful, and I am grateful for the study sessions we held as a group.

I am also especially grateful to Yuka Mori*, who has been a constant source of support throughout my doctoral studies. We began our relationship six months after I entered the doctoral course and have spent the past three years together. She not only offered encouragement, but also provided honest feedback. Her unwavering support enabled me to remain disciplined and persevere through the challenges of the doctoral program.

Lastly, I would like to express my heartfelt gratitude to my family in my hometown of Nagoya: Morimasa Goto, Keiko Goto, Chieko Mizukoshi, Hajime Mizukoshi, Sakura Mizukoshi, and Haruka Mizukoshi. I sincerely apologize for not being able to return home often and for causing them concern. My family has always been my greatest source of understanding. The time I spent with my sisters, Sakura and Haruka, is truly irreplaceable and has been a continual of encouragement for my research.

This work was supported by JST SPRING, Japan Grant Number JPMJSP2136.

1 Modular Forms

In this chapter, we give a brief introduction to modular forms.

1.1 Congruence Subgroups and Modular Curves

Let N be a positive integer. The kernel of the group homomorphism

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod N$$

is called the *principal congruence subgroup of level N* , and is denoted by $\Gamma(N)$. That is,

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \bmod N, b \equiv c \equiv 0 \bmod N \right\}.$$

A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a *congruence subgroup* if there exists a positive integer N such that $\Gamma(N) \subset \Gamma$. In this case, Γ is said to be a congruence subgroup of *level N* . For example, the following subgroups of $\mathrm{SL}_2(\mathbb{Z})$ are easily seen to be congruence subgroups of

*She is not a researcher

level N :

$$\begin{aligned}\Gamma_0(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}, \\ \Gamma_1(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid a \equiv d \equiv 1 \pmod{N} \right\}.\end{aligned}$$

Note that $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_1(1) = \Gamma_0(1)$.

Here, we introduce modular curves for a congruence subgroup. We denote by

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

the (Poincaré) upper half-plane. For $z \in \mathbb{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$, we define

$$\gamma z := \frac{az + b}{cz + d}. \quad (1.1)$$

This action is well-defined and induces a transitive action on $\mathbb{H}$.

Let $\mathbb{P}^1(\mathbb{Q}) := \mathbb{Q} \cup \{\infty\}$ denote the projective line over $\mathbb{Q}$. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $s \in \mathbb{P}^1(\mathbb{Q})$, we define

$$\gamma s := \begin{cases} \frac{ap+bq}{cp+dq} & s = \frac{p}{q} \in \mathbb{Q} \text{ and } cp + dq \neq 0, \\ \frac{a}{c} & s = \infty \text{ and } c \neq 0, \\ \infty & s = \frac{p}{q} \in \mathbb{Q} \text{ and } cp + dq = 0 \text{ or } s = \infty \text{ and } c = 0. \end{cases} \quad (1.2)$$

Then, $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$. If Γ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with finite index, then Γ has finitely many orbits on $\mathbb{P}^1(\mathbb{Q})$. Each such orbit of Γ is called a *cusp* of Γ .

For any congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, the group Γ acts on the extended upper half-plane $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ via the actions defined in (1.1) and (1.2). We define the quotient space $\Gamma \backslash \mathbb{H}^*$ to be the set of orbits of elements of $\mathbb{H}^*$ under this action. We now endow $\Gamma \backslash \mathbb{H}^*$ with a topology. To do this, we first define the topology on $\mathbb{H}^*$ as follows. The neighborhood basis of a point $z \in \mathbb{H}$ is given by the usual open sets in the complex plane. For a point $a \in \mathbb{P}^1(\mathbb{Q})$, the neighborhoods are described as follows: If $a = \infty$, a neighborhood basis at a consists of sets of the form

$$\{\infty\} \cup \{z \in \mathbb{H} \mid \mathrm{Im}(z) > C\}$$

for some $0 \leq C \in \mathbb{R}$. If $a \in \mathbb{Q}$, a neighborhood basis at a consists of sets of the form

$$\{a\} \cup U,$$

where U is the interior of a circle lying in $\mathbb{H}$ and tangent to the real line at a . Having defined the topology on $\mathbb{H}^*$ in this way, we equip the quotient space $\Gamma \backslash \mathbb{H}^*$ with the quotient topology. Then, $\Gamma \backslash \mathbb{H}^*$ can be endowed with the structure of a compact Riemann surface, although we do not explain the details of this construction here. This space is denoted by $X(\Gamma)$ and is called the *modular curve* associated with Γ .

1.2 Modular forms and cusp forms

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$ and $k \in \mathbb{Z}$, the *weight- k slash operator* on functions $f : \mathbb{H} \rightarrow \mathbb{C}$ is defined by

$$(f|_k \gamma)(z) = (\det \gamma)^{k-1} (cz + d)^{-k} f(\gamma z).$$

Recall that $\gamma z \in \mathbb{H}$ ((1.1)).

Definition 1.1. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and let k be an integer. A function $f : \mathbb{H} \rightarrow \mathbb{C}$ is called a *modular form of weight k with respect to Γ* if the following conditions hold:

- (1) f is holomorphic on $\mathbb{H}$,
- (2) $f = f|_k \gamma$ for all $\gamma \in \Gamma$,
- (3) for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, the limit

$$a_0 = \lim_{\mathrm{Im}(z) \rightarrow \infty} (f|_k \alpha)(z)$$

exists in $\mathbb{C}$.

If, in addition,

- (4) $a_0 = 0$ for any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$,

then f is called a *cusp form* of weight k with respect to Γ .

The space of modular forms of weight k with respect to Γ is denoted by $M_k(\Gamma)$, and the space of cusp forms is denoted by $S_k(\Gamma)$. Any modular form f with respect to some congruence subgroup is periodic. In particular, when $\Gamma = \Gamma_0(N)$, the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$ implies that any $f \in M_k(\Gamma_0(N))$ is periodic with period 1. Therefore, f has a Fourier expansion:

$$f(z) = \sum_{n=0}^{\infty} a_n q^n,$$

where $q = e^{2\pi iz}$. In this thesis, we say that $f \in M_k(\Gamma_0(N))$ is *normalized* if $a_1 = 1$ (not $a_0 = 1$).

The Eisenstein series are classical examples of modular forms. For each even integer $k \geq 4$, the Eisenstein series of weight k is defined by

$$E_k(z) := \frac{1}{2} \sum_{\gcd(c,d)=1} (cz + d)^{-k} \left(= \sum_{\gamma \in \Gamma_{\infty} \backslash \mathrm{SL}_2(\mathbb{Z})} 1|_k \gamma \right),$$

where $\Gamma_{\infty} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c = 0 \right\}$. This series converges absolutely, and defines a modular form $E_k \in M_k(\mathrm{SL}_2(\mathbb{Z}))$. Moreover, its Fourier expansion is given by

$$E_k(z) = 1 - \frac{2k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

where $\sigma_l(n) = \sum_{d|n} d^l$ and B_n denotes the n -th Bernoulli number, defined by the generating function

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

The Eisenstein series are not cusp forms. To construct cusp forms, we recall the *Dedekind eta function*, defined by

$$\eta(z) = e^{\pi iz/12} \prod_{n=1}^{\infty} (1 - q^n),$$

which is holomorphic on $\mathbb{H}$. Then the function

$$\Delta(z) := \eta(z)^{24} = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

is a normalized cusp form of weight 12 with respect to $\mathrm{SL}_2(\mathbb{Z})$, and

$$\varphi_8(z) := \eta^8(z) \eta^8(2z) = q \prod_{n=1}^{\infty} (1 - q^n)^8 (1 - q^{2n})^8$$

is a normalized cusp form of weight 8 with respect to $\Gamma_0(2)$. Their Fourier expansions are given by

$$\Delta(z) = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + 84480q^8 - 113643q^9 - 115920q^{10} + \dots$$

and

$$\varphi_8(z) = q - 8q^2 + 12q^3 + 64q^4 - 210q^5 - 96q^6 + 1016q^7 - 512q^8 - 2043q^9 + 1680q^{10} + 1092q^{11} + \dots$$

See also Table 3 and Table 4. By definition, Δ and φ_8 are cusp forms with integer Fourier coefficients.

The form Δ is sometimes called the *discriminant function*. This name arises from the fact that, for $z \in \mathbb{H}$, it is related to the discriminant of the elliptic curve $E_z/\mathbb{C}$ given by

$$E_z : y^2 = 4x^3 - 60g_4(z)x - 140g_6(z),$$

where

$$g_4(z) = \sum_{(0,0) \neq (c,d) \in \mathbb{Z}^2} (cz + d)^{-4} \text{ and } g_6(z) = \sum_{(0,0) \neq (c,d) \in \mathbb{Z}^2} (cz + d)^{-6}.$$

The discriminant of E_z is then given by

$$(2\pi)^{12} \Delta = -8(-30g_4)^3 - 27(-140g_6)^2 = (2\pi)^{12} \frac{E_4^3 - E_6^2}{1728}.$$

Here, we use the identities

$$g_k(z) = 2\zeta(k)E_k(z) = (-1)^{k/2+1} \frac{(2\pi)^k}{k!} B_k E_k(z)$$

for $k = 4, 6$ and $B_4 = -1/30, B_6 = 1/42$.

It is known that the vector space $M_k(\Gamma)$ over $\mathbb{C}$ is finite-dimensional for any congruence subgroup Γ . To state the dimension formula, we first define elliptic points. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. A point $z \in \Gamma \backslash \mathbb{H}$ is called an *elliptic point* of $X(\Gamma)$ if the stabilizer

$$\Gamma_z = \{\gamma \in \Gamma \mid \gamma(z) = z\}$$

of z satisfies $\Gamma_z \not\subset \{\pm I\}$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. This definition is well-defined on the quotient. For each elliptic point z , a positive integer

$$h_z = |\{\pm I\}\Gamma_z/\{\pm I\}| = \begin{cases} |\Gamma_z|/2 & \text{if } -I \in \Gamma_z, \\ |\Gamma_z| & \text{if } -I \notin \Gamma_z \end{cases}$$

is called the *period* of z .

In the case of $X(\mathrm{SL}_2(\mathbb{Z}))$, the following is known:

Proposition 1.2. The point $\mathrm{SL}_2(\mathbb{Z}) \cdot i \in X(\mathrm{SL}_2(\mathbb{Z}))$ is the unique elliptic point of $X(\mathrm{SL}_2(\mathbb{Z}))$ with period 2, and the point $\mathrm{SL}_2(\mathbb{Z}) \cdot e^{2\pi i/3} \in X(\mathrm{SL}_2(\mathbb{Z}))$ is the unique elliptic point of $X(\mathrm{SL}_2(\mathbb{Z}))$ with period 3.

Then, the dimension formula is given as follows:

Theorem 1.3 (dimension formula). Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. For any even integer $k \in \mathbb{Z}$, then the dimensions of the spaces of modular and cusp forms are given by

$$\dim_{\mathbb{C}}(M_k(\Gamma)) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor \varepsilon_2 + \lfloor \frac{k}{3} \rfloor \varepsilon_3 + \frac{k}{2} \varepsilon_{\infty}, & \text{if } k \geq 2, \\ 1 & \text{if } k = 0, \\ 0 & \text{if } k < 0 \end{cases}$$

and

$$\dim_{\mathbb{C}}(S_k(\Gamma)) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor \varepsilon_2 + \lfloor \frac{k}{3} \rfloor \varepsilon_3 + (\frac{k}{2} - 1) \varepsilon_{\infty}, & \text{if } k \geq 4, \\ g & \text{if } k = 2, \\ 0 & \text{if } k \leq 0, \end{cases} \quad (1.3)$$

where g denotes the genus of the modular curve $X(\Gamma)$, and

$$\varepsilon_j = \begin{cases} \text{the number of elliptic points of } X(\Gamma) \text{ with period 2} & \text{if } j = 2, \\ \text{the number of elliptic points of } X(\Gamma) \text{ with period 3} & \text{if } j = 3, \\ \text{the number of cusps of } X(\Gamma) & \text{if } j = \infty. \end{cases}$$

We now compute the dimensions of the spaces $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ and $S_8(\Gamma_0(2))$ of cusp forms using the dimension formula. First, the genus g of a modular curve can be computed from the numbers of elliptic points and cusps:

Theorem 1.4. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Let

$$f : X(\Gamma) \longrightarrow X(\mathrm{SL}_2(\mathbb{Z})), \Gamma z \mapsto \mathrm{SL}_2(\mathbb{Z})z$$

be the natural projection, and let d denote its degree. Let $\varepsilon_j, j = 2, 3, \infty$ be as defined above. Then the genus g of $X(\Gamma)$ is given by

$$g = 1 + \frac{d}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}. \quad (1.4)$$

By Proposition 1.2, we have $\varepsilon_2 = \varepsilon_3 = 1$ for $\mathrm{SL}_2(\mathbb{Z})$. Also, $\varepsilon_\infty = 1$, since $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$. The map f in the theorem has degree 1 since it is the identity. Thus, by (1.4), the genus g of $X(\mathrm{SL}_2(\mathbb{Z}))$ is 0. Then, applying the dimension formula (1.3), we obtain

$$\dim_{\mathbb{C}}(S_{12}(\mathrm{SL}_2(\mathbb{Z}))) = 1.$$

Since $\Delta \neq 0$, we conclude that

$$S_{12}(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}\Delta.$$

Let p be a prime. For the modular curve $X_0(p) := X(\Gamma_0(p))$, the values of ε_j are given by

$$\begin{aligned} \bullet \quad \varepsilon_2 &= \#\{x \in \mathbb{F}_p \mid x^2 + 1 = 0 \text{ in } \mathbb{F}_p\} = \begin{cases} 1 & \text{if } p = 2, \\ 2 & \text{if } p \equiv 1 \pmod{4}, \\ 0 & \text{if } p \equiv 3 \pmod{4}, \end{cases} \\ \bullet \quad \varepsilon_3 &= \#\{x \in \mathbb{F}_p \mid x^2 - x + 1 = 0 \text{ in } \mathbb{F}_p\} = \begin{cases} 1 & \text{if } p = 3, \\ 2 & \text{if } p \equiv 1 \pmod{3}, \\ 0 & \text{if } p \equiv 2 \pmod{3}, \end{cases} \\ \bullet \quad \varepsilon_\infty &= 2. \end{aligned}$$

Thus, in the case of $\Gamma_0(2)$, we get

$$\varepsilon_\infty = 2, \varepsilon_2 = 1, \varepsilon_3 = 0.$$

In general, if $\Gamma_1 \subset \Gamma_2$ are congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, then the natural projection $f : X(\Gamma_1) \longrightarrow X(\Gamma_2)$ between the corresponding modular curves has degree

$$[\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1].$$

A right coset decomposition of $\mathrm{SL}_2(\mathbb{Z})$ with respect to $\Gamma_0(p)$ is given by

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{j=0}^{p-1} \Gamma_0(p) \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix} \cup \Gamma_0(p) \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Thus, the map $f : X_0(p) \longrightarrow X(\mathrm{SL}_2(\mathbb{Z}))$ has degree $p + 1$. Applying the genus formula (1.4) to the case $p = 2$, we find that the genus of $X_0(2)$ is 0. From the formula (1.3), we have

$$\dim_{\mathbb{C}}(S_8(\Gamma_0(2))) = 1.$$

We state a special case of Theorem 1.3 which will be used later.

Proposition 1.5. For any even integer $k \geq 4$, we have

$$M_k(\mathrm{SL}_2(\mathbb{Z})) = S_k(\mathrm{SL}_2(\mathbb{Z})) \oplus \mathbb{C}E_k$$

and

$$\dim_{\mathbb{C}}(S_k(\mathrm{SL}_2(\mathbb{Z}))) = \begin{cases} \lfloor \frac{k}{12} \rfloor - 1 & \text{if } k \equiv 2 \pmod{12}, \\ \lfloor \frac{k}{12} \rfloor & \text{otherwise.} \end{cases}$$

1.3 Hecke operators

In this section, we recall Hecke operators and prove the following theorem:

Theorem 1.6. Let $(k, N, f) = (12, 1, \Delta)$ or $(8, 2, \varphi_8)$, where the Fourier expansion of f is given by $f = \sum_{n=1}^{\infty} a_f(n)q^n$. Then the following hold:

(1) If $\gcd(n, m) = 1$, then

$$a_f(nm) = a_f(n)a_f(m).$$

(2) For any prime $p \nmid N$ and integer $m \geq 1$, we have

$$a_f(p^{m+1}) = a_f(p)a_f(p^m) - p^{k-1}a_f(p^{m-1}).$$

The map

$$\Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^*, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \pmod{N}$$

is a surjective group homomorphism with kernel $\Gamma_1(N)$. This shows that $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$ and induces an isomorphism of groups

$$\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^*.$$

This gives rise to a representation of $(\mathbb{Z}/N\mathbb{Z})^*$ on $M_k(\Gamma_1(N))$. For each $d \in (\mathbb{Z}/N\mathbb{Z})^*$, the corresponding *diamond operator* $\langle d \rangle$ is defined by

$$\langle d \rangle f = f|_k \alpha_d,$$

where $\alpha_d = \begin{pmatrix} a & b \\ c & d' \end{pmatrix} \in \Gamma_0(N)$ is any element satisfying $d \equiv d' \pmod{N}$. Therefore, as χ runs through the Dirichlet characters $(\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ satisfying $\chi(-1) = (-1)^k$, the diamond operators yield the following decompositions:

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi} M_k(N, \chi) \quad \text{and} \quad S_k(\Gamma_1(N)) = \bigoplus_{\chi} S_k(N, \chi),$$

where

$$M_k(N, \chi) = \{f \in M_k(\Gamma_1(N)) \mid \langle d \rangle f = \chi(d)f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^*\}$$

and

$$S_k(N, \chi) = \{f \in S_k(\Gamma_1(N)) \mid \langle d \rangle f = \chi(d)f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^*\}$$

are the χ -eigenspaces. Note that $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma_0(N)$. Hence, if $\chi : (\mathbb{Z}/N\mathbb{Z})^* \rightarrow \mathbb{C}^*$ satisfies $\chi(-1) \neq (-1)^k$, then

$$M_k(N, \chi) = S_k(N, \chi) = 0.$$

If $f \in M_k(N, \chi)$, then χ is called the *Nebentypus* character of f . If $\chi = \varepsilon$ is the trivial character, we have $M_k(N, \varepsilon) = M_k(\Gamma_0(N))$ and $S_k(N, \varepsilon) = S_k(\Gamma_0(N))$.

Let $f \in M_k(N, \chi)$ be a modular form whose Fourier expansion is given by

$$f = \sum_{m=0}^{\infty} a_f(m) q^m.$$

The Hecke operator T_n , for a positive integer n , is defined via its action on the Fourier expansion by

$$T_n f := \sum_{m=0}^{\infty} A(m) q^m,$$

where

$$A(m) = \sum_{d|\gcd(m,n)} \chi(d) d^{k-1} a_f\left(\frac{mn}{d^2}\right)$$

for $m \geq 0$. Here, we define $\chi(d) := 0$ if $\gcd(d, N) > 1$. Then $T_n f \in M_k(N, \chi)$ for any positive integer n .

The Hecke operators satisfy the following properties:

- (1) $T_1 = \text{id}_{M_k(N, \chi)}$,
- (2) $T_n T_m = T_m T_n$ for all positive integers n, m ,
- (3) $T_{p^{m+1}} = T_p T_{p^m} - \chi(p) T_{p^{m-1}}$ for any prime p and $m \geq 1$.

When $\dim_{\mathbb{C}}(S_k(N, \chi)) = 1$, as in the cases of $S_{12}(\text{SL}_2(\mathbb{Z}))$ and $S_8(\Gamma_0(2))$, any nonzero form $f \in S_k(N, \chi)$ is an eigenvector for all Hecke operators T_n . Such cusp forms are generally called a *Hecke eigenforms*. If f is a Hecke eigenform, then for each positive integer n , there exists an eigenvalue $\lambda_n \in \mathbb{C}$ such that

$$T_n f = \lambda_n f.$$

Comparing the Fourier coefficient of q , we have

$$\lambda_n a_f(1) = a_f(n).$$

Therefore, Δ and φ_8 are normalized Hecke eigenforms, and they satisfy Theorem 1.6 (1) and (2).

1.4 Newforms and old forms

Let k and N be fixed positive integers, and let χ be a Dirichlet character mod N satisfying $\chi(-1) = (-1)^k$. We define $S_k(N, \chi)_{\text{old}}$ as the $\mathbb{C}$ -vector subspace of $S_k(N, \chi)$ generated by

$$\bigcup_{N' | N, N' \neq N} \bigcup_{t | N/N'} \{g(tz) \mid g \in S_k(N', \chi)\}.$$

This space is called the space of *oldforms* in $S_k(N, \chi)$.

If $N' \mid N$, then $\Gamma_0(N) \subset \Gamma_0(N')$, and right coset representatives of $\Gamma_0(N')$ modulo $\Gamma_0(N)$ may be taken in $\Gamma_1(N')$. For $f \in S_k(N, \chi)$, where χ is a character mod N' , we define the *trace operator* by:

$$\text{Tr}_{N'}^N f = \sum_i f|_k R_i,$$

where $\{R_i\}_i \subset \Gamma_1(N')$ is a set of right coset representatives of $\Gamma_0(N) \setminus \Gamma_0(N')$. It is easy to check that $\text{Tr}_{N'}^N f$ does not depend on the choice of representatives $\{R_i\}_i$ and lies in $S_k(N', \chi)$. We define the space of *newforms* in $S_k(N, \chi)$ by

$$S_k(N, \chi)_{\text{new}} := \bigcap_q \{f \in S_k(N, \chi) \mid \text{Tr}_{N/q}^N(f) = 0 = \text{Tr}_{N/q}^N(f|_k W_N)\},$$

where the intersection is taken over all primes q dividing N such that χ is also a character mod N/q , and

$$W_N := \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

In general, the space $S_k(N, \chi)_{\text{new}}$ is defined as the orthogonal complement of $S_k(N, \chi)_{\text{old}}$ in $S_k(N, \chi)$ with respect to the Petersson inner product. Li [18] proved that this definition is equivalent to the one given above.

Theorem 1.7 ([18]). We have the decomposition:

$$S_k(N, \chi) = S_k(N, \chi)_{\text{old}} \oplus S_k(N, \chi)_{\text{new}}.$$

A *newform* $f \in S_k(N, \chi)$ is a normalized form in $S_k(N, \chi)_{\text{new}}$ which is a common eigenform of all T_p with p prime and $\gcd(p, N) = 1$.

Let $(k, N, f) = (12, 1, \Delta)$ or $(8, 2, \varphi_8)$. Then, f is a newform. In fact, when $N = 1$, it is immediate that $S_k(N, \chi)_{\text{old}} = 0$, and hence Theorem 1.7 implies $S_k(N, \chi) = S_k(N, \chi)_{\text{new}}$. Moreover, since $S_8(\text{SL}_2(\mathbb{Z})) = 0$ from Proposition 1.5, it follows that $S_8(\Gamma_0(2)) = S_8(\Gamma_0(2))_{\text{new}}$. Therefore, in both cases, f lies in the space of newforms. In the previous section, we also saw that f is a normalized eigenform. Then, f is indeed a newform.

1.5 Fourier coefficients modulo some prime powers

It is known that $\tau(n)$ is odd if and only if n is the square of an odd number. In fact, we have

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} \equiv q \prod_{n=1}^{\infty} (1 - q^{8n})^3 \pmod{2}.$$

On the other hand, we have

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

by Jacobi's triple product identity.

This implies that Δ has *trivial mod 2 residual Galois representation*. However, we omit the details of the Galois representations associated with modular forms.

Moreover, Ramanujan [24] and Swinnerton-Dyer [27] showed that for $n \geq 1$ and prime $p \neq 23$,

$$\begin{aligned} \tau(n) &\equiv \begin{cases} n\sigma_1(n) \bmod 3, \\ \sigma_3(n) \bmod 16 & \text{if } n \text{ is odd,} \\ n\sigma_1(n) \bmod 5, \\ n\sigma_3(n) \bmod 7, \end{cases} \\ \tau(p) &\equiv_{(23)} \begin{cases} 0, & \text{if } (p/23) = -1, \\ 2, & \text{if } p \neq 23 \text{ and } p = a^2 + 23b^2 \text{ with } a, b \in \mathbb{Z}, \\ 1 & \text{if } p = 23, \\ -1 & \text{otherwise.} \end{cases} \end{aligned} \tag{1.5}$$

On the other hand, $f = \varphi_8$ also satisfies the following congruences:

$$a_f(n) \equiv \begin{cases} n\sigma_1(n) \bmod 3, \\ \sigma_3(n) \bmod 16, \\ n\sigma_1(n) \bmod 5, \end{cases}$$

if n is odd.

Proof. By [15, Theorem 8.2], we have

$$a_f(p) \equiv p(p+1) \bmod \ell$$

for $\ell = 3, 5$. By the recursion in Theorem 1.6 (2) and induction on r , it can be shown that

$$a_f(p^r) \equiv p^r \sigma_1(p^r) \bmod \ell$$

for $r \geq 0$. Since both $a_f(n)$ and $n\sigma_1(n)$ are multiplicative for odd n , we have

$$a_f(n) \equiv n\sigma_1(n) \bmod 3, 5.$$

It is easy to see that

$$\begin{aligned} \Delta(z) &= q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q \prod_{n=1}^{\infty} (1 - q^n)^{16} \prod_{n=1}^{\infty} (1 - q^n)^8 \\ &\equiv_{\bmod 16} q \prod_{n=1}^{\infty} (1 - q^n)^{16} \prod_{n=1}^{\infty} (1 + q^n)^8 = \varphi_8(z) \end{aligned}$$

using the identity $(1 - x)^8 \equiv (1 + x)^8 \bmod 16$. □

Remark 1.8. For $p = 2$, we have $a_{\varphi_8}(2^r) = (-8)^r$ for $r \geq 0$.

Lemma 1.9. Let $(k, N, f) = (12, 1, \Delta)$ or $(8, 2, \varphi_8)$, and let p be a prime with $p \nmid N$.

(1) [6, Lemma 3.4] Assume $a_f(p) \neq 0$. Let $r = \text{ord}_p(a_f(p))$, which means that p divides $a_f(p)$ exactly r times. Then, we have $r \leq k/2 - 1$ and

$$\text{ord}_p(a_f(p^m)) = rm \quad (1.6)$$

for all $m \geq 0$.

(2) The following are equivalent:

(i) $a_f(p) = 0$.

(ii) There exists a positive integer m such that $a_f(p^m) = 0$.

If the above equivalent conditions hold, then we have

$$a_f(p^m) = \begin{cases} 0 & \text{if } m \text{ is odd,} \\ (-p^{k-1})^{m/2} & \text{if } m \text{ is even.} \end{cases} \quad (1.7)$$

Proof. (1) From Deligne's bound $|a_f(p)| \leq 2p^{(k-1)/2}$, we have $r \leq k/2 - 1$. The base cases $m = 0, 1$ are immediate. Assume the result holds for m . Then,

$$\text{ord}_p(a_f(p)a_f(p^m)) = r + rm = r(m+1),$$

and

$$\text{ord}_p(p^{k-1}a_f(p^{m-1})) = k-1 + r(m-1) = r(m+1) + (k-1) - 2r > r(m+1).$$

Hence, from the recursive relation (Theorem 1.6 (2)), we have $\text{ord}_p(a_f(p^{m+1})) = r(m+1)$.

(2) It is obvious that (i) implies (ii). Assume that (ii). Let α and β be roots of

$$X^2 - a_f(p)X + p^{k-1}.$$

Since $|a_f(p)| \leq 2p^{(k-1)/2}$, α and β are distinct complex conjugates. By induction on n , we can show

$$a_f(p^n) = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}$$

for $n \geq 0$ from the recursion (Theorem 1.6 (2)). Taking $\theta \in \mathbb{R}$ as $\alpha = p^{(k-1)/2}e^{i\theta}$, $\beta = p^{(k-1)/2}e^{-i\theta}$, we can write

$$a_f(p^n) = p^{n(k-1)/2} \frac{\sin(n+1)\theta}{\sin \theta}.$$

Therefore, $a_f(p^m) = 0$ if and only if there exists $l \in \mathbb{Z}$ such that $\theta = l\pi/(m+1)$. Then $z = 2\cos \theta \in \mathbb{Z}[e^{2\pi i/(m+1)}]$ is an algebraic integer. On the other hand, $z = e^{i\theta} + e^{-i\theta} = a_f(p)/p^{(k-1)/2} \in \mathbb{Q}$. Since $\mathbb{Z}$ is integrally closed, $z \in \mathbb{Z}$. Noting that $p^{(k-1)/2} \notin \mathbb{Q}$, we must have $z = 0$, that is, $a_f(p) = 0$.

If $a_f(p) = 0$, we can prove (1.7) using the recursion (Theorem 1.6 (2)). □

2 Lucas sequences

Let us begin by introducing Lucas sequences and recalling some of their properties.

2.1 Some basic properties of Lucas sequences

A *Lucas pair* is a pair (α, β) of algebraic integers such that $\alpha + \beta$ and $\alpha\beta$ are nonzero coprime integers and α/β is not a root of unity. Given a Lucas pair (α, β) , we define the sequence

$$u_n(\alpha, \beta) := \frac{\alpha^n - \beta^n}{\alpha - \beta}, n \geq 1,$$

which is called the *Lucas sequence* associated with the Lucas pair (α, β) . The sequence $\{u_n(\alpha, \beta)\}_{n=1}^{\infty}$ satisfies the following properties:

- (1) $u_1(\alpha, \beta) = 1$,
- (2) $u_{n+1}(\alpha, \beta) = (\alpha + \beta)u_n(\alpha, \beta) - \alpha\beta u_{n-1}(\alpha, \beta)$ for all $n \geq 1$.

For example, if we take $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$, then the associated Lucas sequence $\{u_n(\alpha, \beta)\}_{n=1}^{\infty}$ is the Fibonacci sequence.

Let (α, β) be a Lucas pair, and let $\{u_n(\alpha, \beta)\}_{n=1}^{\infty}$ denote the associated sequence. A prime number $p \mid u_n$ is called *primitive prime divisor* of u_n if p does not divide $(\alpha - \beta)^2 u_1 \cdots u_{n-1}$. For $n > 2$, the term u_n is said to be *defective* if it does NOT have any primitive prime divisors. For example, in the case of the Fibonacci sequence,

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

the underlined terms are defective.

A classical problem in the theory of Lucas sequences is the following:

Main problem. List all defective Lucas numbers.

This problem was solved by Bilu, Hanrot, and Voutier [7] and Abouzaid [1]. As a result, defective Lucas numbers are now completely classified. In particular, Bilu, Hanrot, and Voutier proved the following remarkable theorem:

Theorem 2.1 ([7, Theorem 1.4.]). For any Lucas sequence $\{u_n\}_{n=1}^{\infty}$, if $n > 30$, then u_n has a primitive prime divisor.

We will recall some classical facts about Lucas sequences.

Lemma 2.2 ([7, Proposition 2.1 (ii)]). For any Lucas sequence $\{u_n\}$, we have $u_d \mid u_n$ whenever $d \mid n$.

Remark 2.3. Note that [7, Proposition 2.1 (ii)] is originally stated for the Lehmer sequence which is defined as follows:

$$\tilde{u}_n(\alpha, \beta) = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n : \text{odd} , \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n : \text{even}, \end{cases}$$

where (α, β) is a Lehmer pair, that is, a pair of algebraic integers such that $(\alpha + \beta)^2, \alpha\beta \in \mathbb{Z}$ are nonzero coprime and α/β is not a root of unity. Note that any Lucas pair is also a Lehmer pair. By definition, for a Lucas pair (α, β) , we have:

$$\tilde{u}_n(\alpha, \beta) = \begin{cases} u_n(\alpha, \beta) & \text{if } n \text{ is odd,} \\ (\alpha + \beta)^{-1} u_n(\alpha, \beta) & \text{if } n \text{ is even.} \end{cases}$$

Thus, the conclusion of Lemma 2.2 follows from Proposition 2.1 (ii) in [7], noting that if $d \mid n$, then the pair (d, n) never satisfies $(d, n) \equiv (0, 1) \pmod{2}$.

For any prime ℓ , define

$$m_\ell(\alpha, \beta) := \min\{m \geq 1 \mid \ell \text{ divides } u_m\}.$$

Note that $m_\ell(\alpha, \beta) > 1$, since $u_1(\alpha, \beta) = 1$. Moreover, if ℓ is an odd prime that does not divide $\alpha\beta$, then $m_\ell(\alpha, \beta) < \infty$ by [7, Corollary 2.2]. The following proposition follows from [7, Corollary 2.2]. Although [7, Corollary 2.2] is stated in terms of a Lehmer pair (α, β) , it also applies to a Lucas pair. Indeed, for a Lucas pair (α, β) , if $\ell \nmid (\alpha + \beta)$, then the condition $\ell \mid u_n(\alpha, \beta)$ is equivalent to $\ell \mid \tilde{u}_n(\alpha, \beta)$ (see Remark 2.3).

Proposition 2.4 ([7, Corollary 2.2]). Let (α, β) be a Lucas pair, and let ℓ be an odd prime such that ℓ does not divide $\alpha\beta(\alpha + \beta)$. Then the following hold:

- (1) If $\ell \mid (\alpha - \beta)^2$, then $m_\ell(\alpha, \beta) = \ell$.
- (2) Otherwise, $m_\ell(\alpha, \beta)$ divides either $\ell - 1$ or $\ell + 1$.

We note that $\ell \mid (\alpha + \beta)$ is equivalent to $m_\ell(\alpha, \beta) = 2$, since $u_2(\alpha, \beta) = \alpha + \beta$.

Proposition 2.5 ([7, Corollary 2.2]). Assume that the notation is as in Proposition 2.4. Then, for any $m \geq 1$, the following conditions are equivalent:

- (1) $\ell \mid u_m(\alpha, \beta)$,
- (2) $m_\ell(\alpha, \beta) \mid m$.

Remark 2.6. Corollary 2.2 of [7] is originally stated for the Lehmer sequence. However, under the assumption that $\ell \nmid (\alpha + \beta)$, we have $\ell \mid u_m(\alpha, \beta)$ if and only if $\ell \mid \tilde{u}_m(\alpha, \beta)$. Thus, the value of m_ℓ in Corollary 2.2 of [7] coincides with our definition of m_ℓ .

As an application of the theory of Lucas sequences to solving certain Diophantine equations, we present the following lemma.

Lemma 2.7 ([12, Lemma 2.7]). Let ℓ and p be prime numbers with ℓ odd, let $\varepsilon = \pm 1$, and let $d \geq 3$ be an odd integer. Let $j, r \geq 0$ be integers.

- (1) If

$$p^2 - \varepsilon p + 1 = 3^r,$$

we must have $(\varepsilon, p, r) = (1, 2, 1)$.

(2) If

$$2\ell^j = p^d + \varepsilon,$$

we must have $(p, \varepsilon) = (3, -1)$.

(3) If

$$8\ell^j = p^d + \varepsilon$$

we must have $(p, \varepsilon) = (7, 1)$.

Proof. (1) We have $r > 0$ immediately. If $r = 1$, then a straightforward computation gives:

$$\varepsilon p(\varepsilon p - 1) = 2,$$

which implies $p = 2, \varepsilon = 1$.

Now assume $r \geq 2$, and let $\rho := e^{2\pi i/3}$. Then we have the following identity of ideals in $\mathbb{Z}[\rho]$:

$$(\varepsilon p + \rho)(\varepsilon p + \bar{\rho}) = (1 - \rho)^{2r},$$

where $\bar{(\cdot)}$ denotes the complex conjugation. Thus, there exists a unit $u \in \mathbb{Z}[\rho]^\times (= \{\pm 1, \pm \rho, \pm \bar{\rho}\})$ such that

$$\varepsilon p + \rho = u(1 - \rho)^r, \varepsilon p + \bar{\rho} = \bar{u}(1 - \bar{\rho})^r.$$

Since $\varepsilon p \in \mathbb{Z}$, it follows that $\varepsilon p - \bar{\varepsilon} \bar{p} = 0$. However, $\varepsilon p - \bar{\varepsilon} \bar{p} = u(1 - \rho)^r - \bar{u}(1 - \bar{\rho})^r - \bar{\rho} \equiv -\rho(1 - \rho) \pmod{(1 - \rho)^2}$. This is a contradiction, noting $(1 - \rho)$ is a prime ideal in $\mathbb{Z}[\rho]$.

(2) and (3) We first observe that p must be odd. The pair $(\alpha, \beta) := (p, -\varepsilon)$ is a Lucas pair. Note that d is odd, we can write:

$$u_d(\alpha, \beta) = \frac{\alpha^d - \beta^d}{\alpha - \beta} = \frac{p^d + \varepsilon}{p + \varepsilon}.$$

Thus,

$$(p + \varepsilon)u_d(\alpha, \beta) = 2\ell^j, 8\ell^j. \quad (2.1)$$

Since $u_d(\alpha, \beta) = \sum_{i=0}^{d-1} \alpha^{d-1-i} \beta^i$ is odd and $p + \varepsilon$ is even, it follows from (2.1) that:

$$p + \varepsilon = 2\ell^s, 8\ell^s, u_d(\alpha, \beta) = \ell^{j-s},$$

for some integer $0 \leq s \leq j$. We claim that $s = 0$. Suppose for contradiction that $s > 0$. Then $\ell \mid (p + \varepsilon)$, and hence $u_d(\alpha, \beta) = \ell^{j-s}$ is a defective term. Then, we must have $d = 3$. Indeed, since d is odd, we have $d = 3, 5, 7, 13$. However, since $b = (p + \varepsilon)^2$ is a square, we have $d \neq 5, 7, 13$ by Table 1, 3 in [7] and Table 4.1 in [1]. Now, since ℓ does not divide $p - \varepsilon$ but ℓ divides $p + \varepsilon$, we have $m_\ell(\alpha, \beta) = 3$. But Proposition 2.4 (1) implies $m_\ell(\alpha, \beta) = \ell$, so we must have $\ell = 3$. Then, $u_3(p, -\varepsilon) = 3^{j-s}$. By the claim (1) of this lemma, this implies $p = 2$, which contradicts the assumption that p is odd. Therefore, we have $s = 0$. In the case (2), we have $p + \varepsilon = 2$, so $(p, \varepsilon) = (3, -1)$. In the case (3), we similarly have $(p, \varepsilon) = (7, 1)$. $\square$

2.2 The Lucas sequences from a Hecke eigenform

Let $k \geq 4$ be an even integer, and let $f \in M_k(\Gamma_0(N))$ be a newform with integer Fourier coefficients. If p is a prime such that $p \nmid a_f(p)N$, then the sequence $\{a_f(p^{n-1})\}_{n=1}^{\infty}$ forms a Lucas sequence. Indeed, consider α and β as the roots of the following polynomial:

$$X^2 - a_f(p)X + p^{k-1} = (X - \alpha)(X - \beta).$$

Then it can be seen that (α, β) is a Lucas pair and for all $n \geq 1$, we have

$$a_f(p^{n-1}) = \frac{\alpha^n - \beta^n}{\alpha - \beta}. \quad (2.2)$$

Lemma 2.8. Let $k \geq 2$ be an integer, and let $A \in \mathbb{Z}$. Suppose that (α, β) is a Lucas pair such that α and β are the roots of the polynomial

$$X^2 - AX + p^{2k-1},$$

where p is a prime satisfying $p \nmid A$ and $|A| \leq 2p^{(2k-1)/2}$. Then for $n > 2$, if $u_n(\alpha, \beta) \in \{\pm 4\ell^j, \pm 8\ell^j \mid j \geq 0, \ell : \text{an odd prime}\}$, one of the following hold:

(1) There exists a primitive prime divisor of u_n .

(2) We have $n = 4$, and

$$\ell^{2j} = \begin{cases} \frac{3^{2k-1}-1}{2} & \text{if } u_n = \pm 4\ell^j, \\ \frac{7^{2k-1}+1}{8} & \text{if } u_n = \pm 8\ell^j. \end{cases} \quad (2.3)$$

Proof. Assume that u_n has no primitive prime divisor; that is, u_n is defective. It is known that the only elements of the set $\{\pm 4\ell^j, \pm 8\ell^j \mid \ell \text{ odd prime}, j \geq 0\}$ that can occur as defective values appear in exactly four rows of Table 2 in [3]. From this, we conclude that $n = 4$. The information of the table implies that if $u_n = \pm 4\ell^j$, we have

$$m^2 = 2p^{2k-1} + \varepsilon 2,$$

where $m = 2\ell^j$, $\varepsilon = \pm 1$. Thus, we have

$$2\ell^{2j} = p^{2k-1} + \varepsilon.$$

By Lemma 2.7 (2), we have $p = 3, \varepsilon = -1$. Therefore, the first case of (2.3) holds.

Similarly, if $u_n = \pm 8\ell^j$, we have

$$8\ell^{2j} = p^{2k-1} + \varepsilon.$$

By Lemma 2.7 (3), we obtain $p = 7, \varepsilon = 1$. Therefore, the second case of (2.3) also follows. $\square$

Remark 2.9. If $k = 3, \ell = 11, j = 1$, then the first equation in (2.3) holds. On the other hand, for $k < 10000$, the second equation in (2.3) does not hold. Of course, if $(k, j) = (1, 0)$, then both equations in (2.3) are satisfied for any prime ℓ .

Proposition 2.10. Let p be a prime such that $p \nmid \tau(p)$, and let α, β be the roots of the integral polynomial

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

Then, we have $u_i(\alpha, \beta) = \tau(p^{i-1})$ for all $i \geq 1$, and the sequence $\{u_i(\alpha, \beta)\}$ satisfies following properties:

- (1) ([2, Lemma 2.1]) For $n > 2$, if $u_n(\alpha, \beta) \in \{\pm 1, \pm \ell \mid \ell \text{ odd prime}\}$, then $u_n(\alpha, \beta)$ is not defective.
- (2) ([4, Lemma 2.1]) For $n > 2$, if $u_n(\alpha, \beta) \in \{\pm 2\ell^j \mid \ell \text{ odd prime}, j \geq 0\}$, then $u_n(\alpha, \beta)$ is not defective.
- (3) ([12, Proposition 2.10]) For $n > 2$, if $u_n(\alpha, \beta) \in \{\pm 4\ell^j, \pm 8\ell^j \mid \ell \text{ odd prime}, j \geq 0\}$, then $u_n(\alpha, \beta)$ is not defective.

Proposition 2.11. Let p be a prime such that $p \nmid a_f(p)$, and let α, β be the roots of the integral polynomial

$$X^2 - a_f(p)X + p^7 = (X - \alpha)(X - \beta).$$

Then, we have $u_i(\alpha, \beta) = a_f(p^{i-1})$ for all $i \geq 1$, and the sequence $\{u_i(\alpha, \beta)\}_{i=1}^{\infty}$ satisfies following properties:

- (1) For $n > 2$, if $u_n(\alpha, \beta) \in \{\pm 1, \pm \ell \mid \ell \text{ odd prime less than } \underline{10000}\}$, then $u_n(\alpha, \beta)$ is not defective.
- (2) ([4, Lemma 2.1]) For $n > 2$, if $u_n(\alpha, \beta) \in \{\pm 2\ell^j \mid \ell \text{ odd prime}, j \geq 0\}$, then $u_n(\alpha, \beta)$ is not defective.
- (3) For $n > 2$, if $u_n(\alpha, \beta) \in \{\pm 4\ell^j, \pm 8\ell^j \mid \ell \text{ odd prime}, j \geq 0\}$, then $u_n(\alpha, \beta)$ is not defective.

Proof. By [2, Lemma 2.1], if $u_n(\alpha, \beta) \in \{\pm 1, \pm \ell \mid \ell \text{ odd prime}\}$, then necessarily $n = 4$, $u_4(\alpha, \beta) = \pm \ell$, and $a_f(p) = \pm \ell$, with

$$\ell^2 = 2p^7 - 1.$$

However, this equation has no solution for $\ell < 10000$.

- (3) If $2k - 1 = 7$, the equation (2.3) has no solution. □

For $k \geq 1$, it remains an open question whether $\tau(n)$ can be equal to 2^k . However, the following lemma holds:

Lemma 2.12 (see also [16]). Let k be an integer such that $k \in \{1, \dots, 8\}$. The the equation

$$\tau(n) = -2^k$$

has no solutions. Moreover, if $\tau(n) = 2^k$, then we must have $n = p_1 \cdots p_k$, where $p_1, \dots, p_k$ are distinct primes satisfying $\tau(p_1) = \cdots = \tau(p_k) = 2$.

Proof. We first consider the equation

$$|\tau(p^{d-1})| = 2^j, \quad p \text{ prime}, d \geq 1$$

for $j = 1, \dots, 8$. Then we will show that this implies $d = 2$ and $\tau(p) = 2$.

We will first show that the sequence $\{\tau(p^{i-1})\}_{i=1}^{\infty}$ forms a Lucas sequence.

Clearly, $d \geq 2$ must hold. Suppose $p = 2$. Then $d \geq 4$ is necessary since $\tau(2) = -24$ and $\tau(4) = -1472$. However, from (1.6), we know that $2^9 \mid 2^{3(d-1)} \mid \tau(2^{d-1})$ if $d \geq 4$, which contradicts $|\tau(p^{d-1})| = 2^j$ with $j \leq 8$. Therefore, $p \neq 2$.

Next, suppose $p \mid \tau(p)$. Then by (1.6), we have $p^{d-1} \mid \tau(p^{d-1})$. Since p is odd, we must have $d = 1$. However, $\tau(1) = 1$, a contradiction. Thus, $p \nmid \tau(p)$. By (2.2), the sequence $\{\tau(p^{i-1})\}_{i=1}^{\infty}$ is a Lucas sequence.

Since $\tau(p)$ is even, if $d > 2$, then $\tau(p^{d-1})$ is defective term. However, by Proposition 2.11, there is no such defective number. Therefore, $d = 2$. By the congruences in Lemma A.2 for odd primes p , we conclude that $\tau(p) = 2$.

Now assume $|\tau(n)| = 2^k$ for some positive integer n . We write

$$n = q_1 \cdots q_r,$$

where $q_1, \dots, q_r > 1$ are powers of distinct primes. By Theorem 1.6 (1), we have

$$|\tau(n)| = |\tau(q_1)| \cdots |\tau(q_r)|.$$

Since $|\tau(q_i)| > 1$ for all i (by (0.3)), we can write

$$|\tau(q_i)| = 2^{j_i}$$

for some $j_i \geq 1$. From the argument above, we know that each q_i must be a prime and satisfy $\tau(q_i) = 2$. Hence, $r = k$. $\square$

In the case of $f = \varphi_8$, we can prove the following theorem by slight modification in the proof of previous lemma:

Lemma 2.13. Let $f = \varphi_8$, and let $a \in \{2, \pm 4, \pm 8\}$. Assume that $a_f(n) = a$. Then the possible values of n are as follows:

- (1) If $a = 2$ or -4 , then $n = p$, where p is prime.
- (2) If $a = 4$, then $n = p_1 p_2$, where p_1 and p_2 are distinct primes such that $a_f(p_1) = a_f(p_2) = 2$.
- (3) If $a = 8$, then $n = p_1 p_2 p_3$, where p_1, p_2, p_3 are distinct primes such that $a_f(p_1) = a_f(p_2) = a_f(p_3) = 2$.
- (4) If $a = -8$, then 2 or $p_1 p_2$, where p_1 and p_2 are distinct primes such that $a_f(p_1) = 2$ and $a_f(p_2) = -4$.

There is no solution to the equation $a_f(n) = -2$.

Lemma 2.14. Let p and ℓ be primes with $\ell \neq 2$ and let $d \geq 1$. Let

$$a_f(p^{d-1}) = \varepsilon t \ell,$$

where $\varepsilon = \pm$, $t = 2, 4, 8$, and $f = \Delta$ or φ_8 . Then, we have

$$d = \begin{cases} 2 & \text{if } t = 2, 8, \\ 2, 4 & \text{if } t = 4 \end{cases}$$

if $f = \Delta$,

$$d = \begin{cases} 2 & \text{if } t = 2, \\ 2, 4 & \text{if } t = 4, 8 \end{cases}$$

if $f = \varphi_8$. If $d = 4$, then we have

$$(a_f(p), \varepsilon, \ell) = \begin{cases} (2, -, p^{11} - 2) & \text{if } f = \Delta, \\ (2, -, p^7 - 2), (-4, +, p^7 - 8) & \text{if } f = \varphi_8. \end{cases} \quad (2.4)$$

Proof. We prove for $f = \Delta$, we can prove similarly in the case of $f = \varphi_8$. We put $\tau(p^{d-1}) = n$, where $n = \varepsilon t \ell$. Clearly, $d > 1$.

We will show that d is even. If $p = 2$, then by $\text{ord}_2(\tau(2)) = \text{ord}_2(-24) = 3$ and Lemma 1.9 (1), we have $2^{3(d-1)} \mid \tau(2^{d-1}) = n$. We must have $d = 2$. Thus, we may assume that $p \neq 2$. Since n is even, (0.4) implies that d is even.

Note that Lemma 1.9 (2) implies $\tau(p) \neq 0$. We will consider whether $p \nmid \tau(p)$ or not. If $p \mid \tau(p)$, we have $p^{d-1} \mid \tau(p^{d-1}) = n$ by Lemma 1.9 (1). In this case, we must have $d = 2$. Therefore, we may assume that $p \nmid \tau(p)$. As we noted before Lemma 2.8, $\{1, \tau(p), \dots\}$ is a Lucas sequence. Let $u_i = \tau(p^{i-1})$ for $i \geq 1$.

We assume that u_d does not have primitive prime divisor ℓ . If $d > 2$, we have that u_d does not have primitive prime divisor 2 since we have $2 \mid u_2$ by (0.4). This is a contradiction by Proposition 2.10. Thus we have $d = 2$.

If u_d has primitive prime divisor ℓ , we have $\ell \nmid u_1 \cdots u_{d-1}$. Since d is even, we can put $m := d/2$. Then $\ell \nmid u_m$. By Lemma 2.2, $u_m \mid u_d$. Therefore, $u_m = \pm 1, \pm 2, \pm 4, \pm 8$. By Lemma 2.12, we must have $(m, u_m) = (2, 2), (1, 1)$. Thus $d = 2, 4$. If $d = 4$, $\tau(p) = u_2 = 2$. Since we can write $\tau(p^3) = \tau(p)(\tau(p)^2 - 2p^{11})$, we have $\tau(p^3) = 4(2 - p^{11})$. Since p is odd, we have $u_4 = \tau(p^3) \neq \pm 2\ell, \pm 8\ell$. By $2 - p^{11} < 0$, we get (2.4) for $f = \Delta$. $\square$

3 Other methods

Let $f = \Delta$ or φ_8 . If

$$a_f(n) = \varepsilon \ell,$$

where $\varepsilon = \pm$ and odd prime ℓ , then $n = p^{d-1}$, where p, d are primes such that d is odd and divides $\ell(\ell^2 - 1)$ by Proposition 0.6. Moreover, we do not need to consider all such d for each ℓ , applying Lemma A.1. However, in the case that it satisfies Lemma A.1, we need to consider individually. In this chapter, we will introduce two methods used in such situation.

3.1 Thue equation

For $a = \pm\ell$, we consider the equation

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

Thanks to Proposition 0.6, there are only finitely many cases of possible values of d . For each such d , applying the congruence (1.5), more explicitly, Lemma A.1, we can rule out many cases of the pair (ℓ, d) . When we cannot rule out (ℓ, d) by the congruences, we use the theory of Thue equation.

Let $F(X, Y)$ be a homogeneous polynomial with degree ≥ 3 and $a \in \mathbb{Z}$. An equation of the form

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

is called a *Thue equation*.

Comparing the Euler factor of the L -function of Δ -function:

$$L(s, \Delta) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \prod_{p:\text{prime}} \frac{1}{1 - \tau(p)p^{-s} + p^{11}p^{-2s}},$$

we define

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

Then, by simple calculation, for a nonnegative integer m , we have that $F_{2m}, F_{2m+1}/\sqrt{Y} \in \mathbb{Z}[X, Y]$ is a homogeneous polynomial with degree m and $\tau(p^{2m}) = F_{2m}(p^{11}, \tau(p)^2)$. Some of the first of them are as follows:

$$F_1(X, Y) = \sqrt{Y}, F_2(X, Y) = Y - X, F_3(X, Y) = \sqrt{Y}(Y - 2X), F_4(X, Y) = X^2 - 3XY + Y^2, \dots$$

Proposition 3.1 ([3, Lemma 5.1]). Let $(k, N, f) = (12, 1, \Delta)$ or $(8, 2, \varphi_8)$, and p be prime with $p \nmid N$. If $a_f(p^4) = a$, then $(x, y) = (p, 2a_f(p)^2 - 3p^{k-1})$ is an integer point on

$$y^2 = 5x^{2(k-1)} + 4a. \quad (3.1)$$

Calculating by PARI/GP, for $d > 5$, we can know whether the Thue equation

$$F_{d-1}(X, Y) = \pm\ell$$

has any solution (X, Y) which can be written as $(X, Y) = (p^{11}, \tau(p)^2)$ or not.

Lemma 3.2. Let p be a prime. If $(\ell, d) \in LD_1^\varepsilon$, then

$$\tau(p^{d-1}) \neq \varepsilon\ell,$$

where

$$\begin{aligned} LD_1^+ &:= \{(277, 23), (421, 7), (631, 79), (827, 23), (827, 59), (967, 7), (967, 11), (967, 23)\}, \\ LD_1^- &:= \{(367, 23), (443, 17), (643, 23), (643, 107), (827, 59), (829, 23), (829, 83), (919, 17)\}. \end{aligned}$$

3.2 Dembner–Jain’s method

When $d = 5$, the equation

$$\tau(p^{d-1}) = a \quad (3.2)$$

for $a = -139, -179, 281, 461, -599, -919$ cannot be ruled out by the congruences. In this subsection, we will show that Dembner–Jain’s method [10] makes it possible ruling out $-139, -179, 281, -919$.

Lemma 3.3. For any prime p , we have $\tau(p^4) \neq -139, -179, 281, -919$.

Proof. We apply Dembner–Jain’s method. Let $\tau(p^4) = \varepsilon\ell$, where $(\varepsilon, \ell) = (1, 281), (-1, 919)$. Let the real quadratic field $K := \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_K := \mathbb{Z}[\omega]$ the ring of integers of K , where $\omega = (1 + \sqrt{5})/2$. Then, $\mathcal{O}_K^\times = \{\pm\omega^n \mid n \in \mathbb{Z}\}$. Two prime ideals $281\mathbb{Z}$ and $919\mathbb{Z}$ in $\mathbb{Z}$ are totally decomposition over K as follows:

$$281\mathcal{O}_K = (19 + 4\sqrt{5})(19 - 4\sqrt{5}), 919\mathcal{O}_K = (42 + 13\sqrt{5})(42 - 13\sqrt{5}).$$

When $\ell = 281$, by (3.1),

$$(19 + 4\sqrt{5})(19 - 4\sqrt{5}) = \frac{y + p^{11}\sqrt{5}}{2} \cdot \frac{y - p^{11}\sqrt{5}}{2},$$

where $y = 2\tau(p)^2 - 3p^{11}$. Let $\alpha = \frac{y + p^{11}\sqrt{5}}{2}$, then there exists $u \in \mathcal{O}_K^\times$ such that

$$\alpha = u(19 + 4\sqrt{5}) \text{ or } u(19 - 4\sqrt{5}).$$

For simplicity, we assume the former case. Then, taking its conjugate, we have

$$\bar{\alpha} = \frac{y - p^{11}\sqrt{5}}{2} = \bar{u}(19 - 4\sqrt{5}).$$

We can write $u = \pm\omega^n, n \in \mathbb{Z}$. Taking $\pm(\alpha - \bar{\alpha})$, we have

$$(\pm p)^{11} = 19 \cdot \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}} + 4(\omega^n + \bar{\omega}^n) \quad (3.3)$$

Here, we define the Fibonacci numbers and Lucas numbers

$$F_n := \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}}, L_n := \omega^n + \bar{\omega}^n$$

for $n \in \mathbb{Z}$. (Note that "Lucas numbers" means specific numbers in this paper. This is different to the notion of Lucas sequence. In fact, the sequence of Lucas numbers $\{L_n\}_{n \geq 1}$ is not a Lucas sequence.) The sequences F_n, L_n satisfy

$$F_{n+1} = F_n + F_{n-1}, L_{n+1} = L_n + L_{n-1},$$

for all $n \in \mathbb{Z}$. The sequences $F_n, L_n \bmod 89$ has period 44 (we can see this from Dembner–Jain’s page <https://github.com/sdembner/tauvalues>), therefore, so is $x_n = 19F_n + 4L_n$.

There are no perfect 11-th power mod 89 in $x_0, \dots, x_{43} \bmod 89$ by using computer. Thus, the equation (3.3) has no solution.

When $\ell = 919$, instead of (3.3),

$$(\pm p)^{11} = 42F_n + 13L_n \quad (3.4)$$

The sequence $x_n := 42F_n + 13L_n$ has period 44 mod 89, 22 mod 199. Then, x_n is perfect 11-th power mod 89 if and only if $n \equiv 1, 12, 23, 34 \bmod 44$. x_n is perfect 11-th power mod 199 if and only if $n \equiv 11 \bmod 22$. For any $n \in \mathbb{Z}$, these two condition can not be satisfied simultaneously. Thus, the equation (3.4) has no solution.

Similarly, for $a = -139, -179$, we can see that the equation (3.2) has no solution. $\square$

Let $f = \varphi_8$. For some $\pm \ell$ marked in Table 2 in Chapter B, we can check that the equation (3.2) has no solution by Dembner-Jain's method. The point is that $F_n, L_n \bmod 113$ has period 76.

4 Proofs

4.1 Part (a)

Proof of part (a) in Theorem A. By [3, Theorem 3.2], if $\tau(n) = \pm \ell$, then we have $n = p^{d-1}$, $d \mid \ell(\ell^2 - 1)$ is odd prime. It is trivial that $\tau(p) \neq 0$ from Lemma 1.9 (2). If $p \mid \tau(p)$, we have $p^{d-1} \mid \tau(p^{d-1})$ by Lemma 1.9 (1). However, this is a contradiction by $d \geq 3$. Therefore, we have that $p \nmid \tau(p)$. Taking α, β as Proposition 2.11, the sequence $\{u_i(\alpha, \beta) := \tau(p^{i-1})\}_{i \geq 1}$ is a Lucas sequence.

Now, u_d is not defective by Proposition 2.11 (1) and $d \geq 3$. In other words, ℓ is unique primitive prime divisor of u_d . By definition, we have $\ell \nmid (\alpha - \beta)^2 u_1 \cdots u_{d-1}$. In particular, $\ell \nmid (\alpha - \beta)^2$ and $\ell \nmid u_2 = \alpha + \beta$. We can check $\ell \nmid \alpha\beta (= p^{11})$ since we have $p \neq \ell$ by noting $p \nmid \tau(p)$. Then, Proposition 2.4 implies $d \mid (\ell^2 - 1)$. By Lemma A.1, $\tau(p^{d-1}) = \varepsilon \ell$ has no solution except for (ℓ, d) are as follows:

$$(277, 23), (281, 5), (421, 7), (461, 5), (631, 79), (827, 23), (827, 59), (967, 7), (967, 11), (967, 23),$$

if $\varepsilon = +$,

$$(139, 5), (179, 5), (367, 23), (443, 17), (599, 5), (643, 23), (643, 107), (827, 59), (829, 23), (829, 83),$$

$$(919, 5), (919, 17),$$

if $\varepsilon = -$. When $d > 5$, we can rule out (ℓ, d) by Lemma 3.2, $(281, 5)$ (when $\varepsilon = +$), $(139, 5), (179, 5), (919, 5)$ (when $\varepsilon = -$) by Lemma 3.3. $\square$

In the case of $f = \varphi_8$, we can prove similarly.

We consider solving Thue equation

$$F_{d-1}(X, Y) = \pm \ell$$

for $d \in C(\pm\ell)$ in Table 1 in Chapter B. If $7 \leq d \leq 37$, this equation has no solution such that $(X, Y) = (p^7, a_f(p)^2)$. When $d = 5$, we apply Dembner–Jain’s method to solve

$$y^2 = 5x^{14} \pm 4\ell.$$

Then we can rule out $-59, 101, 641, -659, 941$ (see Table 2 in Chapter B).

4.2 Part (b)

We may consider only the value of $a_f(p)$ for $f = \Delta$ or φ_8 . By Ramanujan’s congruences, we can restrict the value of $a_f(p)$ to the element of $L(f)_t^\pm, t = 2, 4, 8$. More precisely, this lemma is true:

Lemma 4.1. Let $f = \Delta$ or φ_8 . We take an odd prime $\ell < 1000$, and let $\varepsilon = \pm, t = 2, 4, 8$.

(1) For any prime p , if

$$a_f(p) = \varepsilon t \ell,$$

we must have $\ell \in L(f)_t^\varepsilon$.

(2) For any prime p ,

$$a_f(p^3) \neq \pm 4\ell.$$

Proof. (1) For any $(\varepsilon, \ell) \notin L_t^\varepsilon$, $\tau(p) = \varepsilon t \ell$ never happen by Lemma A.2. Here, note that when $f = \Delta$ and $t = 2$, we may assume that $100 < \ell$ by (0.5).

(2) If $\tau(p^3) = \varepsilon 4\ell, \varepsilon = \pm$, by Lemma 2.14, we have $(\tau(p), \varepsilon, \ell) = (2, -, p^{11} - 2)$. Now, $\ell < 1000$ and $|2 - p^{11}| \geq 2046$, therefore, this is a contradiction. Similarly, we get the claim $a_f(p^3) \neq \pm 4\ell$ also. $\square$

Proof of part (b) in Theorem A. We assume that $\tau(n) = \pm 2^j \ell$ for an odd prime $\ell < 1000$ and $j = 1, 2, 3$.

We consider when $2 \leq \omega(n) =: m$. Then, we can write $n = p_1^{d_1-1} \cdots p_m^{d_m-1}$, where $p_1, \dots, p_m$ are distinct primes and $d_1, \dots, d_m \geq 2$. We put $q_i := p_i^{d_i-1}$ for $i = 1, \dots, m$. From the multiplicity of τ , we have

$$\prod_{i=1}^m |\tau(q_i)| = 2^j \ell.$$

Then, there exists i such that $\ell \nmid |\tau(q_i)|$ because $m \geq 2$. Then $|\tau(q_i)| = 1, 2, \dots, 2^j$. By (0.3), $|\tau(q_i)| \neq 1$ and by Lemma 2.12, $d_i = 2$ and $\tau(q_i) = 2$. Therefore, $n/q_i (= n/p_i)$ is coprime to $q_i (= p_i)$. The case (1) of Theorem A (b) is true.

If $\omega(n) = 1$, so that we can write $n = p^{d-1}$, where p is prime, $d \geq 2$ is an integer. By Lemma 2.14 and Lemma 4.1 (2), we have $d = 2$. By Lemma 4.1 (1), we have $\ell \in L_{2j}^\varepsilon$. Thus, the case (2) of Theorem A (b) is true. $\square$

We can prove the part (b) in Theorem B also similarly.

A Some congruences for $a_f(p^{d-1})$ at some prime powers

Lemma A.1. Let f be Δ or φ_8 and d an odd integer.

(1) For p is an odd prime, we have

$$\begin{aligned}
 a_f(p^{d-1}) &\equiv_{(3)} 0, 1, d, \\
 a_f(p^{d-1}) &\equiv_{(16)} \begin{cases} 1 & \text{if } d \equiv 1 \pmod{16}, \\ 1, 3, 5, 7, 9, 11, 13, 15 & \text{if } d \equiv 3, 7, 11, 15 \pmod{16}, \\ 1, 5, 9, 13 & \text{if } d \equiv 5, 13 \pmod{16}, \\ 1, 9 & \text{if } d \equiv 9 \pmod{16}, \end{cases} \\
 a_f(p^{d-1}) &\equiv_{(5)} \begin{cases} 0, 1, d & \text{if } d \equiv 1, \\ 0, 1, 2, 3, d & \text{if } d \equiv 3. \end{cases}
 \end{aligned}$$

(2) If $f = \Delta$, moreover we have

$$\begin{aligned}
 a_\Delta(p^{d-1}) = \tau(p^{d-1}) &\equiv_{(7)} \begin{cases} 0, 1, d & \text{if } d \equiv 1, \\ 0, 1, 2, 4, d, 2d, 4d & \text{if } d \equiv 3, 5, \end{cases} \\
 a_\Delta(p^{d-1}) = \tau(p^{d-1}) &\equiv_{(23)} \begin{cases} 1, d & \text{if } d \equiv 1, \\ 0, 1, d & \text{if } d \equiv 3, \\ 1, -1, d & \text{if } d \equiv 5, \end{cases}
 \end{aligned}$$

for any prime p .

Lemma A.2. Let f be Δ or φ_8 and $d \geq 2$ an even integer.

(1) For any odd prime p , we have

$$\begin{aligned}
 a_f(p^{d-1}) &\equiv_{(3)} 0, d, \\
 a_f(p^{d-1}) &\equiv_{(16)} \begin{cases} 0, 2, 4, 6, 8, 10, 12, 14 & \text{if } d \equiv 2, 6, 10, 14 \pmod{16}, \\ 0, 4, 8, 12 & \text{if } d \equiv 4, 12 \pmod{16}, \\ 0, 8 & \text{if } d \equiv 8 \pmod{16}, \end{cases} \\
 a_f(p^{d-1}) &\equiv_{(5)} \begin{cases} 0, d & \text{if } d \equiv 0, \\ 0, 1, 2, d & \text{if } d \equiv 2. \end{cases}
 \end{aligned}$$

(2) If $f = \Delta$, moreover we have

$$a_\Delta(p^{d-1}) = \tau(p^{d-1}) \equiv_{(7)} \begin{cases} 0, d, 2d, 4d & \text{if } d \equiv 0, 2, \\ 0, d & \text{if } d \equiv 4, \end{cases}$$

for any prime p and

$$a_{\Delta}(p^{d-1}) = \tau(p^{d-1}) \equiv_{(23)} \begin{cases} 0, d & \text{if } d \equiv 0, \\ 0, -1, d & \text{if } d \equiv 2, \\ 0, 1, d & \text{if } d \equiv 4, \end{cases} \pmod{6}$$

for any prime $p \neq 23$. When $p = 23$, $\tau(p^{d-1}) \equiv_{(23)} 1$ for any integer $d \geq 1$.

Proof. The congruence mod 3, 16, 5, 7 in the lemma can be showed by the same method. Here, for example, in the case of that d is odd, we give the proof of the congruence mod 7. Substituting $n = p^{d-1}$ in (1.5), we have

$$\tau(p^{d-1}) \equiv p^{d-1}(1 + p^3 + \cdots + p^{3(d-1)}) \pmod{7}.$$

Since $p^3 \equiv 0, \pm 1 \pmod{7}$, $1 + p^3 + \cdots + p^{3(d-1)} \equiv 0, d \pmod{7}$ (note that d is odd). If $d \equiv 3, 5 \pmod{6}$, p^{d-1} is congruent to 0, 1, 2, 4 since p^{d-1} is square. If $d \equiv 1 \pmod{6}$, p^{d-1} is congruent to 0, 1 modulo 7.

We can prove the congruence mod 23 due to the recursion relation (Theorem 1.6 (2)) and induction on d . For example, suppose d is even and $(p/23) = -1$, in other words, $p^{11} \equiv -1 \pmod{23}$. By (1.5), $\tau(p) \equiv 0 \pmod{23}$. Therefore, from the recursion relation, we have

$$\tau(p^{m+1}) \equiv \tau(p^{m-1}) \pmod{23}$$

for $m \geq 1$. In particular, $\tau(p^{d-1}) \equiv \tau(p) \equiv 0 \pmod{23}$. In the case of that p is a quadratic residue mod 23, it can be proved similarly. If $p = 23$, use $\tau(23) = 18643272 \equiv 1 \pmod{23}$. $\square$

B Tables

B.1

The following table, for each odd prime ℓ , lists the odd prime divisors d of $\ell^2 - 1$ in the second column. The third (resp. the fourth) column of the table shows the values that satisfy the congruence conditions Lemma A.1 (1) when $a_f(p^{d-1}) = \ell$ (resp. $a_f(p^{d-1}) = -\ell$). An asterisk (*) indicates that the condition Lemma A.1 (2) for $\tau(p^{d-1}) = \pm\ell$ is also satisfied.

Table 1: congruence

ℓ	$d \mid (\ell^2 - 1)$	$C(\ell)$	$C(-\ell)$
3	$\emptyset$	$\emptyset$	$\emptyset$
5	$[3]$	$\emptyset$	$[3]$
7	$[3]$	$[3]$	$\emptyset$
11	$[3, 5]$	$\emptyset$	$\emptyset$
13	$[3, 7]$	$[3, 7]$	$\emptyset$
17	$[3]$	$\emptyset$	$[3]$
19	$[3, 5]$	$\emptyset$	$[5]$
23	$[3, 11]$	$[11]$	$[3^*, 11]$
29	$[3, 5, 7]$	$\emptyset$	$[3, 7]$
31	$[3, 5]$	$[3]$	$\emptyset$
37	$[3, 19]$	$[3, 19]$	$\emptyset$
41	$[3, 5, 7]$	$[5]$	$\emptyset$
43	$[3, 7, 11]$	$[3, 7, 11]$	$[11]$
47	$[3, 23]$	$[23]$	$[3, 23^*]$
53	$[3, 13]$	$\emptyset$	$[3]$
59	$[3, 5, 29]$	$\emptyset$	$[3, 5, 29]$
61	$[3, 5, 31]$	$[3, 5, 31]$	$\emptyset$
67	$[3, 11, 17]$	$[3, 11]$	$[11]$
71	$[3, 5, 7]$	$\emptyset$	$\emptyset$
73	$[3, 37]$	$[3]$	$\emptyset$
79	$[3, 5, 13]$	$\emptyset$	$[5]$
83	$[3, 7, 41]$	$\emptyset$	$[3, 7]$
89	$[3, 5, 11]$	$\emptyset$	$[3^*, 11]$
97	$[3, 7]$	$[3, 7]$	$\emptyset$
101	$[3, 5, 17]$	$[5]$	$\emptyset$
103	$[3, 13, 17]$	$[3]$	$\emptyset$
107	$[3, 53]$	$\emptyset$	$[3, 53]$
109	$[3, 5, 11]$	$\emptyset$	$[11]$
113	$[3, 7, 19]$	$\emptyset$	$[3, 7, 19]$
127	$[3, 7]$	$[3, 7]$	$\emptyset$
131	$[3, 5, 11, 13]$	$[11]$	$\emptyset$

ℓ	$d \mid (\ell^2 - 1)$	$C(\ell)$	$C(-\ell)$
137	[3, 17, 23]	[23*]	[3*, 23]
139	[3, 5, 7, 23]	$\square$	[5*, 23*]
149	[3, 5, 37]	$\square$	[3]
151	[3, 5, 19]	[3, 19]	$\square$
157	[3, 13, 79]	[3, 79]	$\square$
163	[3, 41]	[3]	$\square$
167	[3, 7, 83]	[83]	[3, 7, 83]
173	[3, 29, 43]	$\square$	[3, 43]
179	[3, 5, 89]	$\square$	[3, 5*]
181	[3, 5, 7, 13]	[3, 5, 7, 13]	$\square$
191	[3, 5, 19]	$\square$	[19]
193	[3, 97]	[3]	$\square$
197	[3, 7, 11]	[11]	[3, 7, 11]
199	[3, 5, 11]	$\square$	[5, 11]
211	[3, 5, 7, 53]	[3, 7]	$\square$
223	[3, 7, 37]	[3, 7]	$\square$
227	[3, 19, 113]	$\square$	[3*, 19]
229	[3, 5, 19, 23]	[19]	[23*]
233	[3, 13, 29]	$\square$	[3]
239	[3, 5, 7, 17]	$\square$	[3, 5, 7, 17]
241	[3, 5, 11]	[3, 5, 11]	$\square$
251	[3, 5, 7]	$\square$	$\square$
257	[3, 43]	$\square$	[3, 43]
263	[3, 11, 131]	[11, 131]	[3, 11, 131]
269	[3, 5, 67]	$\square$	[3, 67]
271	[3, 5, 17]	[3]	$\square$
277	[3, 23, 139]	[3*, 23*, 139]	[23]
281	[3, 5, 7, 47]	[5*, 47]	$\square$
283	[3, 47, 71]	[3, 47, 71]	[47, 71]
293	[3, 7, 73]	$\square$	[3, 7]
307	[3, 7, 11, 17]	[3, 7, 11]	[11]
311	[3, 5, 13, 31]	$\square$	$\square$
313	[3, 13, 157]	[3, 13]	$\square$
317	[3, 53, 79]	$\square$	[3, 79]
331	[3, 5, 11, 83]	[3, 11, 83]	$\square$
337	[3, 7, 13]	[3, 7]	$\square$
347	[3, 29, 173]	$\square$	[3, 173]
349	[3, 5, 7, 29]	[29]	$\square$
353	[3, 11, 59]	[11, 59]	[3, 11, 59]
359	[3, 5, 179]	[179]	[3, 5, 179]
367	[3, 23, 61]	[3, 23]	[23*]

ℓ	$d \mid (\ell^2 - 1)$	$C(\ell)$	$C(-\ell)$
373	[3, 11, 17, 31]	[3, 11, 31]	[11]
379	[3, 5, 7, 19]	[19]	[5]
383	[3, 191]	[191]	[3, 191]
389	[3, 5, 13, 97]	$\emptyset$	[3]
397	[3, 11, 199]	[3, 11, 199]	[11]
401	[3, 5, 67]	[5]	$\emptyset$
409	[3, 5, 17, 41]	$\emptyset$	$\emptyset$
419	[3, 5, 7, 11, 19]	$\emptyset$	[3, 5, 7, 11, 19]
421	[3, 5, 7, 211]	[3, 5, 7*, 211]	$\emptyset$
431	[3, 5, 43]	$\emptyset$	$\emptyset$
433	[3, 7, 31]	[3, 7, 31]	$\emptyset$
439	[3, 5, 11, 73]	$\emptyset$	[5, 11]
443	[3, 13, 17, 37]	$\emptyset$	[3, 37]
449	[3, 5, 7]	$\emptyset$	[3, 7]
457	[3, 19, 229]	[3, 19]	$\emptyset$
461	[3, 5, 7, 11, 23]	[5*, 11, 23]	$\emptyset$
463	[3, 7, 11, 29]	[3*, 7, 11]	[11]
467	[3, 13, 233]	$\emptyset$	[3, 13]
479	[3, 5, 239]	[239]	[3, 5, 239]
487	[3, 61]	[3]	$\emptyset$
491	[3, 5, 7, 41]	$\emptyset$	$\emptyset$
499	[3, 5, 83]	$\emptyset$	[5, 83]
503	[3, 7, 251]	[251]	[3*, 7, 251]
509	[3, 5, 17, 127]	$\emptyset$	[3, 127]
521	[3, 5, 13, 29]	[5, 29]	$\emptyset$
523	[3, 29, 131]	[3, 131]	[131]
541	[3, 5, 271]	[3, 5, 271]	$\emptyset$
547	[3, 7, 13, 137]	[3, 7]	$\emptyset$
557	[3, 31, 139]	$\emptyset$	[3, 31, 139]
563	[3, 47, 281]	[47]	[3, 47]
569	[3, 5, 19, 71]	$\emptyset$	[3, 19, 71]
571	[3, 5, 11, 13, 19]	[3, 11, 19]	$\emptyset$
577	[3, 17]	[3, 17]	$\emptyset$
587	[3, 7, 293]	$\emptyset$	[3, 7, 293]
593	[3, 11, 37]	[11]	[3, 11]
599	[3, 5, 13, 23]	$\emptyset$	[3, 5*, 13, 23]
601	[3, 5, 7, 43]	[3*, 5, 7, 43]	$\emptyset$
607	[3, 19, 101]	[3, 19]	$\emptyset$
613	[3, 17, 307]	[3, 307]	$\emptyset$
617	[3, 7, 11, 103]	[11]	[3, 7, 11, 103]
619	[3, 5, 31, 103]	$\emptyset$	[5]
631	[3, 5, 7, 79]	[3, 7, 79*]	$\emptyset$
641	[3, 5, 107]	[5, 107]	$\emptyset$

ℓ	$d \mid (\ell^2 - 1)$	$C(\ell)$	$C(-\ell)$
643	[3, 7, 23, 107]	[3, 7, 23, 107]	[23*, 107*]
647	[3, 17, 19]	$\square$	[3, 19]
653	[3, 109, 163]	$\square$	[3, 163]
659	[3, 5, 7, 11, 47]	$\square$	[3, 5, 7, 11, 47]
661	[3, 5, 11, 331]	[3, 5, 11, 331]	$\square$
673	[3, 7, 337]	[3, 7]	$\square$
677	[3, 13, 113]	$\square$	[3]
683	[3, 11, 19, 31]	[11]	[3, 11, 19, 31]
691	[3, 5, 23, 173]	[3*, 23]	$\square$
701	[3, 5, 7, 13]	[5]	$\square$
709	[3, 5, 59, 71]	[59]	[59, 71]
719	[3, 5, 359]	[359]	[3, 5, 359]
727	[3, 7, 11, 13]	[3, 7, 11]	[11]
733	[3, 61, 367]	[3, 367]	$\square$
739	[3, 5, 37, 41]	$\square$	[5]
743	[3, 7, 31, 53]	$\square$	[3, 7, 31]
751	[3, 5, 47]	[3, 47]	$\square$
757	[3, 7, 379]	[3, 7, 379]	$\square$
761	[3, 5, 19, 127]	[5]	[19]
769	[3, 5, 7, 11]	$\square$	[11]
773	[3, 43, 193]	$\square$	[3, 43]
787	[3, 131, 197]	[3, 131]	[131]
797	[3, 7, 19, 199]	$\square$	[3, 7, 19, 199]
809	[3, 5, 101]	$\square$	[3]
811	[3, 5, 7, 29]	[3, 7]	[29]
821	[3, 5, 41, 137]	[5]	$\square$
823	[3, 103, 137]	[3, 103]	[137]
827	[3, 7, 23, 59]	[23*, 59*]	[3*, 7, 23, 59*]
829	[3, 5, 23, 83]	$\square$	[23*, 83*]
839	[3, 5, 7, 419]	[419]	[3, 5, 7, 419]
853	[3, 7, 61, 71]	[3, 7, 71]	[71]
857	[3, 11, 13, 107]	[11, 107]	[3, 11, 107]
859	[3, 5, 11, 13, 43]	$\square$	[5, 11]
863	[3, 431]	[431]	[3, 431]
877	[3, 73, 439]	[3*, 439]	$\square$
881	[3, 5, 7, 11]	[5, 11]	$\square$
883	[3, 7, 13, 17]	[3, 7]	$\square$
887	[3, 37, 443]	[443]	[3, 443]
907	[3, 151, 227]	[3, 151, 227]	[227]
911	[3, 5, 7, 13, 19]	$\square$	[19]
919	[3, 5, 17, 23]	$\square$	[5*, 23]
929	[3, 5, 29, 31]	[29]	[3, 31]
937	[3, 7, 13, 67]	[3, 7, 67]	$\square$

ℓ	$d \mid (\ell^2 - 1)$	$C(\ell)$	$C(-\ell)$
941	[3, 5, 47, 157]	[5, 47]	$\square$
947	[3, 11, 43, 79]	[11]	[3, 11, 43, 79]
953	[3, 7, 17, 53]	[53]	[3, 7]
967	[3, 7, 11, 23]	[3*, 7*, 11*, 23*]	[11, 23]
971	[3, 5, 97]	$\square$	$\square$
977	[3, 61, 163]	$\square$	[3, 163]
983	[3, 41, 491]	[491]	[3, 491]
991	[3, 5, 11, 31]	[3, 11, 31]	$\square$
997	[3, 83, 499]	[3, 83, 499]	[83]

B.2

The following table lists the entries from the above table in which 5 appears. We apply Dembner–Jain’s method to these.

Table 2: Dembner–Jain’s method

ℓ	$a_f(p^4) = \ell$	$a_f(p^4) = -\ell$	ℓ	$a_f(p^4) = \ell$	$a_f(p^4) = -\ell$
19	$\square$	[5(inad φ_8)]	479	$\square$	[5]
41	[5]	$\square$	499	$\square$	[5]
59	$\square$	[5(inad φ_8)]	521	[5]	$\square$
61	[5]	$\square$	541	[5]	$\square$
79	$\square$	[5]	599	$\square$	[5*]
101	[5(inad φ_8)]	$\square$	601	[5]	$\square$
139	$\square$	[5*(inad Δ)]	619	$\square$	[5]
179	$\square$	[5*(inad Δ)]	641	[5(inad φ_8)]	$\square$
181	[5]	$\square$	659	$\square$	[5(inad φ_8)]
199	$\square$	[5]	661	[5]	$\square$
239	$\square$	[5]	701	[5]	$\square$
241	[5]	$\square$	719	$\square$	[5]
281	[5*(inad Δ)]	$\square$	739	$\square$	[5]
359	$\square$	[5]	761	[5]	$\square$
379	$\square$	[5]	821	[5]	$\square$
401	[5]	$\square$	839	$\square$	[5]
419	$\square$	[5]	859	$\square$	[5]
421	[5]	$\square$	881	[5]	$\square$
439	$\square$	[5]	919	$\square$	[5*(inad Δ)]
461	[5*]	$\square$	941	[5(inad φ_8)]	$\square$

The equation $a_f(p^4) = -19$ has no solution by [3, Theorem 1.3. (3)]. All other items marked with (inad f) show that the equation

$$a_f(p^4) = \pm \ell$$

has no solution by the Dembner–Jain’s method.

Table 3: $\tau(p)$ and its prime divisor decomposition

n	$\tau(n)$	prime divisor decomposition of $ \tau(n) $
2	-24	[<2, 3>, <3, 1>]
3	252	[<2, 2>, <3, 2>, <7, 1>]
5	4830	[<2, 1>, <3, 1>, <5, 1>, <7, 1>, <23, 1>]
7	-16744	[<2, 3>, <7, 1>, <13, 1>, <23, 1>]
11	534612	[<2, 2>, <3, 1>, <13, 1>, <23, 1>, <149, 1>]
13	-577738	[<2, 1>, <7, 1>, <29, 1>, <1423, 1>]
17	-6905934	[<2, 1>, <3, 2>, <7, 1>, <23, 1>, <2383, 1>]
19	10661420	[<2, 2>, <5, 1>, <7, 2>, <11, 1>, <23, 1>, <43, 1>]
23	18643272	[<2, 3>, <3, 1>, <617, 1>, <1259, 1>]
29	128406630	[<2, 1>, <3, 1>, <5, 1>, <11, 1>, <389111, 1>]
31	-52843168	[<2, 5>, <7, 2>, <67, 1>, <503, 1>]
37	-182213314	[<2, 1>, <23, 1>, <3961159, 1>]
41	308120442	[<2, 1>, <3, 1>, <7, 1>, <521, 1>, <14081, 1>]
43	-17125708	[<2, 2>, <23, 1>, <186149, 1>]
47	2687348496	[<2, 4>, <3, 1>, <7, 1>, <7998061, 1>]
53	-1596055698	[<2, 1>, <3, 3>, <23, 1>, <1285069, 1>]
59	-5189203740	[<2, 2>, <3, 1>, <5, 1>, <7, 1>, <29, 1>, <89, 1>, <4787, 1>]
61	6956478662	[<2, 1>, <7, 1>, <23, 1>, <59, 1>, <366169, 1>]
67	-15481826884	[<2, 2>, <23, 1>, <47, 1>, <3580441, 1>]
71	9791485272	[<2, 3>, <3, 2>, <61, 1>, <2229391, 1>]
73	1463791322	[<2, 1>, <7, 1>, <104556523, 1>]
79	38116845680	[<2, 4>, <5, 1>, <23, 1>, <1721, 1>, <12037, 1>]
83	-29335099668	[<2, 2>, <3, 1>, <7, 1>, <23, 1>, <283, 1>, <53653, 1>]
89	-24992917110	[<2, 1>, <3, 2>, <5, 1>, <7, 1>, <19, 1>, <23, 2>, <3947, 1>]
97	75013568546	[<2, 1>, <7, 2>, <23, 1>, <163, 1>, <204173, 1>]
101	81742959102	[<2, 1>, <3, 1>, <7, 1>, <1946260931, 1>]
103	-225755128648	[<2, 3>, <7, 1>, <23, 1>, <175275721, 1>]
107	90241258356	[<2, 2>, <3, 3>, <23, 1>, <53, 1>, <685453, 1>]
109	73482676310	[<2, 1>, <5, 1>, <23, 1>, <29, 1>, <59, 1>, <186727, 1>]
113	-85146862638	[<2, 1>, <3, 1>, <23, 1>, <617006251, 1>]
127	-262717201024	[<2, 7>, <18049, 1>, <113717, 1>]
131	631528759932	[<2, 2>, <3, 1>, <7, 1>, <659, 1>, <11408497, 1>]
137	-297198746214	[<2, 1>, <3, 1>, <23, 1>, <71, 1>, <30332593, 1>]
139	596793577940	[<2, 2>, <5, 1>, <7, 1>, <31, 1>, <1873, 1>, <73417, 1>]
149	-1115433620850	[<2, 1>, <3, 1>, <5, 2>, <23, 1>, <337, 1>, <959389, 1>]
151	-824447297848	[<2, 3>, <69191, 1>, <1489441, 1>]
157	1315116754406	[<2, 1>, <7, 1>, <13, 1>, <23, 2>, <1721, 1>, <7937, 1>]
163	-357832759588	[<2, 2>, <89458189897, 1>]
167	2754833892216	[<2, 3>, <3, 1>, <7, 1>, <16397820787, 1>]
173	-950387449578	[<2, 1>, <3, 1>, <7, 1>, <311, 1>, <72759719, 1>]
179	1681384224780	[<2, 2>, <3, 2>, <5, 1>, <13, 1>, <3319, 1>, <216493, 1>]

Table 4: Fourier coefficients of φ_8 and its prime divisor decomposition

p	$a_{\varphi_8}(p)$	prime divisor decomposition of $ a_{\varphi_8}(p) $
2	-8	[<2, 3>]
3	12	[<2, 2>, <3, 1>]
5	-210	[<2, 1>, <3, 1>, <5, 1>, <7, 1>]
7	1016	[<2, 3>, <127, 1>]
11	1092	[<2, 2>, <3, 1>, <7, 1>, <13, 1>]
13	1382	[<2, 1>, <691, 1>]
17	14706	[<2, 1>, <3, 2>, <19, 1>, <43, 1>]
19	-39940	[<2, 2>, <5, 1>, <1997, 1>]
23	68712	[<2, 3>, <3, 1>, <7, 1>, <409, 1>]
29	-102570	[<2, 1>, <3, 1>, <5, 1>, <13, 1>, <263, 1>]
31	227552	[<2, 5>, <13, 1>, <547, 1>]
37	160526	[<2, 1>, <80263, 1>]
41	10842	[<2, 1>, <3, 1>, <13, 1>, <139, 1>]
43	-630748	[<2, 2>, <137, 1>, <1151, 1>]
47	472656	[<2, 4>, <3, 1>, <43, 1>, <229, 1>]
53	-1494018	[<2, 1>, <3, 3>, <73, 1>, <379, 1>]
59	2640660	[<2, 2>, <3, 1>, <5, 1>, <11, 1>, <4001, 1>]
61	827702	[<2, 1>, <557, 1>, <743, 1>]
67	-126004	[<2, 2>, <17, 2>, <109, 1>]
71	-1414728	[<2, 3>, <3, 2>, <7, 2>, <401, 1>]
73	980282	[<2, 1>, <31, 1>, <97, 1>, <163, 1>]
79	-3566800	[<2, 4>, <5, 2>, <37, 1>, <241, 1>]
83	5672892	[<2, 2>, <3, 1>, <472741, 1>]
89	-11951190	[<2, 1>, <3, 2>, <5, 1>, <19, 1>, <29, 1>, <241, 1>]
97	8682146	[<2, 1>, <11, 1>, <394643, 1>]
101	-10079538	[<2, 1>, <3, 1>, <7, 1>, <17, 1>, <19, 1>, <743, 1>]
103	3747992	[<2, 3>, <468499, 1>]
107	-17985564	[<2, 2>, <3, 4>, <55511, 1>]
109	12257030	[<2, 1>, <5, 1>, <1225703, 1>]
113	16594962	[<2, 1>, <3, 1>, <67, 1>, <41281, 1>]
127	1168256	[<2, 7>, <9127, 1>]
131	-7923828	[<2, 2>, <3, 1>, <11, 1>, <60029, 1>]
137	-315654	[<2, 1>, <3, 1>, <52609, 1>]
139	39203780	[<2, 2>, <5, 1>, <7, 1>, <11, 1>, <25457, 1>]
149	-21886050	[<2, 1>, <3, 1>, <5, 2>, <59, 1>, <2473, 1>]
151	-29415448	[<2, 3>, <3676931, 1>]
157	60554966	[<2, 1>, <31, 1>, <97, 1>, <10069, 1>]
163	57085292	[<2, 2>, <11, 1>, <1297393, 1>]
167	-87726504	[<2, 3>, <3, 1>, <3655271, 1>]
173	8569542	[<2, 1>, <3, 1>, <1428257, 1>]
179	18804060	[<2, 2>, <3, 2>, <5, 1>, <11, 1>, <9497, 1>]

References

- [1] Mourad Abouzaid. Les nombres de Lucas et Lehmer sans diviseur primitif. *J. Théor. Nombres Bordeaux*, 18(2):299–313, 2006.
- [2] Jennifer S. Balakrishnan, William Craig, and Ken Ono. Variations of Lehmer’s conjecture for Ramanujan’s tau-function. *J. Number Theory*, 237:3–14, 2022.
- [3] Jennifer S. Balakrishnan, William Craig, Ken Ono, and Wei-Lun Tsai. Variants of Lehmer’s speculation for newforms. *Adv. Math.*, 428:Paper No. 109141, 31, 2023.
- [4] Jennifer S. Balakrishnan, Ken Ono, and Wei-Lun Tsai. Even values of Ramanujan’s tau-function. *Matematica*, 1(2):395–403, 2022.
- [5] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy II. *Publ. Res. Inst. Math. Sci.*, 47(1):29–98, 2011.
- [6] Michael A. Bennett, Adela Gherga, Vandita Patel, and Samir Siksek. Odd values of the Ramanujan tau function. *Math. Ann.*, 382(1-2):203–238, 2022.
- [7] Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001.
- [8] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.
- [9] Pierre Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980.
- [10] Spencer Dembner and Vanshika Jain. Hyperelliptic curves and newform coefficients. *J. Number Theory*, 225:214–239, 2021.
- [11] Ayla Gafni, Jesse Thorner, and Peng-Jie Wong. Almost all primes satisfy the Atkin-Serre conjecture and are not extremal. *Res. Number Theory*, 7(2):Paper No. 31, 5, 2021.
- [12] Akihiro Goto. On some values which do not belong to the image of ramanujan’s tau-function, 2024.
- [13] Mitsuki Hanada and Rachana Madhukara. Fourier coefficients of level 1 Hecke eigenforms. *Acta Arith.*, 200(4):371–388, 2021.
- [14] Michael Harris, Nick Shepherd-Barron, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy. *Ann. of Math. (2)*, 171(2):779–813, 2010.
- [15] Masatake Hirao, Hiroshi Nozaki, and Koji Tasaka. Spherical designs and modular forms of the D_4 lattice. *Res. Number Theory*, 9(4):Paper No. 77, 18, 2023.

- [16] Kaya Lakein and Anne Larsen. Some remarks on small values of $\tau(n)$. *Arch. Math. (Basel)*, 117(6):635–645, 2021.
- [17] D. H. Lehmer. The vanishing of Ramanujan’s function $\tau(n)$. *Duke Math. J.*, 14:429–433, 1947.
- [18] Wen Ch’ing Winnie Li. Newforms and functional equations. *Math. Ann.*, 212:285–315, 1975.
- [19] Wenwen Lin and Wenjun Ma. On values of Ramanujan’s tau function involving two prime factors. *Ramanujan J.*, 63(1):131–155, 2024.
- [20] Nik Lygeros and Olivier Rozier. Odd prime values of the Ramanujan tau function. *Ramanujan J.*, 32(2):269–280, 2013.
- [21] L.J. Mordell. On Mr. Ramanujan’s empirical expansions of modular functions. *Proc. Camb. Philos. Soc.*, (19):117–124, 1917.
- [22] M. Ram Murty, V. Kumar Murty, and T. N. Shorey. Odd values of the Ramanujan τ -function. *Bull. Soc. Math. France*, 115(3):391–395, 1987.
- [23] James Newton and Jack A. Thorne. Symmetric power functoriality for holomorphic modular forms, I, II. *Publ. Math. Inst. Hautes Études Sci.*, 134:1–152, 2021.
- [24] S. Ramanujan. On certain arithmetical functions [Trans. Cambridge Philos. Soc. **22** (1916), no. 9, 159–184]. In *Collected papers of Srinivasa Ramanujan*, pages 136–162. AMS Chelsea Publ., Providence, RI, 2000.
- [25] Jean-Pierre Serre. Divisibilité de certaines fonctions arithmétiques. *Enseign. Math. (2)*, 22(3-4):227–260, 1976.
- [26] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.
- [27] H. P. F. Swinnerton-Dyer. 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, 1972)*, volume Vol. 350 of *Lecture Notes in Math.*, pages 1–55. Springer, Berlin-New York, 1973.
- [28] Jesse Thorner. Effective forms of the Sato-Tate conjecture. *Res. Math. Sci.*, 8(1):Paper No. 4, 21, 2021.