International Journal of Number Theory

INDEX-DEPENDENT DIVISORS OF COEFFICIENTS OF MODULAR FORMS

B.K. MORIYA

Institute of Mathematical Sciences
IV Cross Road, CIT Campus
Chennai - 600 113
India
bhavinmoriya@gmail.com

C.J. SMYTH

School of Mathematics and Maxwell Institute for Mathematical Sciences
University of Edinburgh
Edinburgh EH9 3JZ
Scotland, U.K.
c.smyth@ed.ac.uk

Received 29 January 2013
Accepted 28 April 2013

We evaluate $\gcd_{m=1}^{\infty} a(nm)$ for a certain family of sequences, which include the Fourier coefficients of some modular forms. In particular, we compute $\gcd_{m=1}^{\infty} \tau(nm)$ for all positive integers n for Ramanujan's τ-function. As a consequence, we obtain many congruences – for instance that $\tau(1000m)$ is always divisible by 64000. We also determine, for a given prime number p, the set of n for which $\tau(p^{n-1})$ is divisible by n. Further, we give a description of the set $\{n \in \mathbb{N} : n \text{ divides } \tau(n)\}$.

We also survey methods for computing $\tau(n)$. Finally, we find the least n for which $\tau(n)$ is prime, complementing a result of D.H. Lehmer, who found the least n for which $|\tau(n)|$ is prime.

Keywords: Modular forms, Lucas sequence, Ramanujan τ-function

Mathematics Subject Classification 2010: 11B39, 11F03

1. Introduction

This paper has four main aims. In Section 2 we evaluate the gcd of every nth term of an integer sequence belonging to a certain family. This family includes those sequences coming from modular forms. In Section 3, we recall a recently-described method for specifying increasing sequences of integers. The method involves describing, for each number n of the sequence, the *multiplying set* $\mathcal{P}_n$ of those primes that can multiply n to produce another member of the sequence. Numbers in the sequence that cannot be produced in this way from smaller numbers of the sequence

are called *basic*. This method is applied to two increasing sequences coming from modular forms (Theorems 3.3 and 3.5). In Section 7, we survey methods for computing Ramanujan's τ-function, while in Section 8 we find the smallest n for which $\tau(n)$ is prime. Sections 4 contains the preliminaries for the proofs of the Theorems. The proofs themselves are in Section 5.

2. Sequences from modular forms

In this section we discuss sets of integers that arise when one considers divisibility properties of certain Fourier coefficients of a modular form. Our first theorem, however, can be stated for more general sequences having certain special properties. Our specific application will be to sequences of coefficients of modular forms.

2.1. *The greatest common divisor of every n^{th} term of special sequences*

Suppose that $k \in \mathbb{N}$ is given, and that $(a(n))_{n\in\mathbb{N}}$ is a sequence of integers, not all 0, with the following properties:

$$a(p) = 0 \text{ or } p^k \nmid a(p) \text{ for each prime } p; \tag{2.1}$$

$$a(nm) = a(n)a(m) \text{ for } n, m \in \mathbb{N} \text{ with } \gcd(n, m) = 1; \tag{2.2}$$

$$a(p^{r+1}) = a(p)a(p^r) - p^{2k-1}a(p^{r-1}) \text{ for each prime } p \text{ and } r \geq 1. \tag{2.3}$$

Note that these properties immediately imply that $a(1) = 1$, as is seen by choosing $a(n) \neq 0$ and $m = 1$ in (2.2). Also, $(a(n))_{n\in\mathbb{N}}$ is completely determined by its values $a(p)$ at primes p. A prime p is called *nonordinary for a* if $p \mid a(p)$. Further, if a sequence satisfies

$$|a(p)| \leq 2p^{k-\frac{1}{2}} \tag{2.4}$$

for a prime $p > 3$, then, as is easily seen, it satisfies (2.1) for that particular p. Thus it is sufficient for (2.1) to be true for all primes p that it holds for $p = 2$ and $p = 3$, and that (2.4) holds for primes $p \geq 5$.

Now for p prime and $a(p) \neq 0$ define $f_p \geq 0$ by $p^{f_p} || a(p)$. Also, define

$$C(n) = \gcd_{m=1}^{\infty} a(nm),$$

the gcd of the $a(nm)$ for $m \in \mathbb{N}$. Then we can state our first result.

Theorem 2.1. *Suppose that the sequence $(a(n))_{n\in\mathbb{N}}$ satisfies equations* (2.1), (2.2) *and* (2.3). *Then, writing $n = \prod_p p^{e_p}$, we have*

$$C(n) = \prod_{\substack{p|n \\ a(p)\neq 0}} p^{e_p f_p} \cdot \prod_{\substack{p|n \\ a(p)=0}} p^{e'_p(2k-1)}, \tag{2.5}$$

where $e'_p = \lfloor \frac{e_p+1}{2} \rfloor$.

2.2. *Modular forms*

Let k be a positive integer. A function $f : \mathcal{H} \to \mathbb{C}$ is called a *modular form of weight* $2k$ if it is holomorphic in $\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$ as well as at ∞ and satisfies $f(z+1) = f(z)$ and $f(-1/z) = z^{2k} f(z)$. From the periodicity we have a Fourier series expansion $f(z) = \sum_{n=0}^{\infty} a_n q^n$ for f, where $q = e^{2\pi i z}$. If $a_0 = 0$ (i.e., $f(\infty) = 0$) then f is called a *cusp form*.

For each $n \in \mathbb{N}$, there is an operator $T(n)$ called the *Hecke operator* that maps modular forms to modular forms and cusp forms to cusp forms. If there exists a modular form f such that

$$T(n)f = \lambda(n)f, \text{ for each } n \geq 1,$$

then f is called a *Hecke eigenform*, with eigenvalues $(\lambda(n))_{n\in\mathbb{N}}$.

Let $f(z) = \sum_{n=1}^{\infty} a_n q^n$ be a cuspform, and Hecke eigenform of weight $2k$, $k > 0$, with $a_1 = 1$. Then it is known [12, p. 102] that the sequence $(a_n)_{n\in\mathbb{N}}$ satisfies (2.2), (2.3) and (2.4).

Next, define Ramanujan's τ-function for $z \in \mathcal{H}$ by

$$\Delta(z) = q \prod_{j=1}^{\infty} (1-q^j)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n. \tag{2.6}$$

The function $(2\pi)^{12}\Delta(z)$ is the discriminant function for the complex elliptic curve $\mathbb{C}/\langle 1, z\rangle$. For $k \geq 2$ define (see Serre [12, p. 92])

$$E_{2k}(z) = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n,$$

where B_{2k} is the $(2k)$-th Bernoulli number, and $\sigma_{2k-1}(n) = \sum_{d|n} d^{2k-1}$. Then ([12, p. 105]) $E_{2k}(z)$ is a modular form of weight $2k$. Also, because $4k/B_{2k}$ is an integer for $2k = 4, 6, 8, 10$ and 14, the cusp forms $\Delta_{12} = \Delta$, $\Delta_{16} = \Delta E_4$, $\Delta_{18} = \Delta E_6$, $\Delta_{20} = \Delta E_8$, $\Delta_{22} = \Delta E_{10}$ and $\Delta_{26} = \Delta E_{14}$ all have integer coefficients. They are known to be Hecke eigenforms, of weights $12, 16, 18, 20, 22, 26$, respectively. Put $\Delta_{2k} = \sum_{n=1}^{\infty} \tau_{2k}(n) q^n$ so that, in particular, $\tau_{12}(n) = \tau(n)$. Then for $n \in \mathbb{N}$ and $2k = 12, 16, 18, 20, 22, 26$, the coefficients $\tau_{2k}(n)$ are integers, with $\tau_{2k}(1) = 1$. Thus the coefficient sequences of these cusp forms all satisfy (2.2), (2.3) and (2.4). This last bound was a conjecture of Ramanujan for the τ-function, generalised by Petersson (The Ramanujan-Petersson Conjecture), proved by Deligne [1] as a consequence of his proof of the Weil conjectures. (See also the Math Review by Nicholas Katz of this paper, where the connection between the τ-function and the Weil conjectures is clearly outlined.) Furthermore, from the tables in Gouvêa [4], all the τ_{2k} satisfy (2.1) for $p = 2$ and 3 and hence, by the remark in Section 2.1 above, for all primes p. This gives the following corollary.

Corollary 2.2. *Suppose that* $C_{2k}(n) = \gcd_{m=1}^{\infty} \tau_{2k}(nm)$, *where* $2k \in \{12, 16, 18, 20,$

$22, 26\}$, *and* $n = \prod_p p^{e_p}$. *Then*

$$C_{2k}(n) = \prod_{\substack{p|n \\ \tau_{2k}(p)\neq 0}} p^{e_p f_p} \cdot \prod_{\substack{p|n \\ \tau_{2k}(p)=0}} p^{e'_p(2k-1)}, \tag{2.7}$$

where $e'_p = \lfloor \frac{e_p+1}{2} \rfloor$.

Note that $C_{2k}(n)$ is a product of nonordinary primes for τ_{2k}. Of course its formula would be simpler if, as suspected, $\tau_{2k}(p)$ is never 0. Indeed, Atkin conjectured that, for any $\varepsilon > 0$, $|\tau_{2k}(p)| \gg_\varepsilon p^{(k-3)/2-\varepsilon}$ on simple heuristic grounds – see Serre [13, p. 15].

Corollary 2.3. *For* $n, m \in \mathbb{N}$ *and* $2k \in \{12, 16, 18, 20, 22, 26\}$ *with* $\tau_{2k}(n) \neq 0$ *we have*

$$\tau_{2k}(nm) \equiv 0 \pmod{\prod_{p|n} p^{e_p f_p}}.$$

2.3. *Nonordinary primes for* τ

We denote by $\mathcal{P}_{\text{non}}$ the set of so-called *nonordinary* primes for $\tau(n)$, namely those primes p for which $\tau(p)$ is divisible by p. It has been proved that there are only six primes less than 10^{10} in $\mathcal{P}_{\text{non}}$, namely, $2, 3, 5, 7, 2411, 7758337633$ – see [3,9]. Using the heuristic that $\tau(p)$ has 'probability' $1/p$ of being divisible by p, and the fact that $\sum_{p \text{ prime}} \frac{1}{p}$ is divergent, one might expect from the converse of the Borel-Cantelli Lemma that $\mathcal{P}_{\text{non}}$ is an infinite (albeit very sparse) set [9]. On the other hand, the convergence of $\sum_{p \text{ prime}} \frac{1}{p^2}$ suggests that there are only finitely many primes p for which $\tau(p)$ is divisible by p^2. For a nonordinary prime p with $\tau(p) \neq 0$, we have $f_p > 0$ where, as above, $p^{f_p} || \tau(p)$. Then for the six known nonordinary primes $f_2 = 3$, $f_3 = 2$, while $f_p = 1$ for the other four known nonordinary primes – see [9] for the factorization of $\tau(7758337633)$. Indeed, it may be that 2 and 3 are the only nonordinary primes p with $f_p > 1$.

For example, Corollary 2.2 shows that $(2k = 12)$, $\tau(1000m)$ is divisible by $2^{3\cdot 3} \cdot 5^{3\cdot 1} = 64000$ for all m, while $\tau(512m)$ is divisible by $2^{9\cdot 3} = 2^{27}$.

3. The subsequence of an increasing sequence that is divisible by its index

3.1. *Describing sequences*

To start with, we describe one way of specifying a strictly increasing sequence of positive integers, S say. This was first used in [14]. For each $s \in S$ we define a set $\mathcal{P}_s(S)$, the *multiplying set of* s, to be the set of primes p for which $ps \in S$. Further, we say that an element s of S is *basic* if there is no prime p such that s/p is in S. Denote the set of basic elements of S by $\mathcal{B}(S)$. The smallest element of S is clearly basic, so that $\mathcal{B}(S)$ is always nonempty. It is clear that then S is completely

specified by the sets $\mathcal{B}(S)$ and $\{\mathcal{P}_s(S)\}_{s\in S}$. It can be visualised as an edge-labelled directed graph whose vertices are the elements of S, with a directed edge $s \xrightarrow{p} s'$ from vertex s to vertex s' when s'/s is a prime p, with p the label for that edge. One can place the vertices at levels $0, 1, 2, \ldots$, with the basic elements at level 0. For $k \geq 1$ the elements of S at level k are those elements of S that are a product $bp_1p_2 \ldots p_k$, where $b \in \mathcal{B}(S)$, $p_1 \in \mathcal{P}_b(S)$, $p_2 \in \mathcal{P}_{bp_1}(S), \ldots, p_k \in \mathcal{P}_{bp_1p_2\ldots p_{k-1}}(S)$. (One should place a vertex s at the lowest possible level, by choosing b so that in the representation $s = bp_1p_2 \ldots p_k$ the level k is minimised.) One obtains a minimal spanning tree for this digraph by choosing, for a given nonbasic s', the unique edge pointing to s' as the edge $s \xrightarrow{p} s'$, where p is the largest prime factor of s' with the property that $p \in \mathcal{P}_s$ for some $s \in S$. One advantage of this way of describing a set S is that, for a given bound X, there is an obvious algorithm for finding all elements of S that do not exceed X. The algorithm uses two sets U and V, initialised by $U := \emptyset$ and $V := \{b \in \mathcal{B}(S) : b \leq X\}$. Then repeat the following until $V = \emptyset$:

- $U := U \cup V$ and then $V := \{np : n \in V, p \in \mathcal{P}_n \text{ and } p \leq X/n\}$.

Let $\mathcal{P}$ denote the set of all primes.

Example 3.1. Take S to be the set of squarefree integers. Then 1 is the only basic element, and for each $n \in S$ the set $\mathcal{P}_n(S) = \{p \in \mathcal{P} : p \nmid n\}$.

Example 3.2. Take S to be the set of nonsquarefree integers. Then $\mathcal{B}(S) = \{p^2 : p \in \mathcal{P}\}$, and for each $n \in S$ the set $\mathcal{P}_n = \mathcal{P}$.

The above description of our set S depends for its usefulness on the structure of the sets $\mathcal{B}(S)$ and $\mathcal{P}_n(S)$. For instance, for S the set of all squares, all elements of S are basic and all $\mathcal{P}_n(S)$ are empty, which tells us little about S.

3.2. *The operator $\mathcal{I}$: indices n that divide the n^{th} sequence element*

Given an integer sequence $S = (s(n))_{n\in\mathbb{N}}$, we define a new, increasing sequence $\mathcal{I}S$ by

$$\mathcal{I}S = \{n \in \mathbb{N} : n \text{ divides } s(n)\}.$$

3.3. *The sequence $\mathcal{I}\tau$*

Our next result concerns the sequence $\mathcal{I}\tau$ of those $n \in \mathbb{N}$ for which n divides $\tau(n)$.

Theorem 3.3. *The sequence $\mathcal{B}(\mathcal{I}\tau)$ of basic elements of $\mathcal{I}\tau$ is given by*

$$\mathcal{B}(\mathcal{I}\tau) = \{1, 4147, 14191, 23276, 28957, 29095, 40733, 52371, 186208, 552343, 625807, 727375, 867031, 983411, \ldots\}.$$

For n in $\mathcal{I}\tau$, the set $\mathcal{P}_n(\mathcal{I}\tau)$ is the set of primes p with the following property:

$$\begin{cases} p \mid \tau(n) \text{ or } p \mid \tau(p) & \text{if } p \nmid n; \\ n' \mid \tau(n') \text{ and } \left(p^{e+1} \mid \tau(n') \text{ or } p \mid \tau(p)\right) & \text{if } p \mid n. \end{cases}$$

Here $n = n'p^e$, where $p \nmid n'$.

The elements of $\mathcal{B}(\mathcal{I}\tau)$ listed are all those that are at most 10^6. The number 3246 of elements of $\mathcal{I}\tau$ that are at most 10^6 is much bigger than the 14 basic elements in that range, given above. We have, however, no reason to suppose that the set $\mathcal{B}(\mathcal{I}\tau)$ is finite.

A table of $\tau(n)$ for $n \le 10^6$ is available at

`http://www.maths.ed.ac.uk/~chris/tauout.out`

More generally, one can define $\mathcal{I}^{(j)}\tau$ to be the set of those $n \in \mathbb{N}$ for which n^j divides $\tau(n)$. Then $\mathcal{I}^{(2)}\tau$ has 333 elements not exceeding 10^6, of which three, 1, 66339 and 329280, are basic, while $\mathcal{I}^{(3)}\tau$ has 33 elements not exceeding 10^6, of which two, 1 and 276480, are basic. The number 1 is the only element of $\mathcal{I}^{(4)}\tau$ not exceeding 10^6.

3.4. *The sequence $\mathcal{I}C_{2k}$*

Now, for $2k \in \{12, 16, 18, 20, 22, 26\}$, let $\mathcal{I}C_{2k}$ be the set of all $n \in \mathbb{N}$ for which n divides $C_{2k}(n)$, defined by (2.7). Clearly $\mathcal{I}C_{12} \subset \mathcal{I}\tau$, since $C_{12}(n) \mid \tau(n)$.

Corollary 3.4. *The sequence $\mathcal{I}C_{2k}$ for $2k \in \{12, 16, 18, 20, 22, 26\}$ consists of all numbers that are a product only of (powers of) nonordinary primes for τ_{2k}.*

3.5. *The divisibility by their indices of Lucas sequences coming from $(a(n))_{n\in\mathbb{N}}$*

Given integers P and Q, let α and β be the roots of the equation

$$x^2 - Px + Q = 0.$$

Then the well-known *Lucas sequence of the first kind* $L(P, Q) = (u_n)_{n\ge 0}$ is given by $u_0 = 0, u_1 = 1$ and $u_{n+2} = Pu_{n+1} - Qu_n$ for $n \ge 0$, or explicitly by Binet's formula

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

when $D = (\alpha - \beta)^2 = P^2 - 4Q \ne 0$, and $u_n = n\alpha^{n-1}$ when $D = 0$.

Given a prime p, denote by $A(p, a)$ the sequence $(a(p^{n-1}))_{n\in\mathbb{N}} = \{1, a(p), \dots\}$. From (2.3) we see that this is the Lucas sequence $L(\tau(p), p^{2k-1})$. Our next result describes the sequence

$$\mathcal{I}A(p, a) = \{n \in \mathbb{N} : n \text{ divides } a(p^{n-1})\}$$

in the manner given in Section 3.1 above.

Theorem 3.5. *Let p be any prime. The only basic elements of $\mathcal{I}A(p, a))$ are*

- 1 *and* 6 *if* $a(p) \equiv 3 \pmod 6$, $p \neq 2$ *or* 3*;*
- 1 *and* 12 *if* $a(p) \equiv \pm 1 \pmod 6$, $p \equiv -1 \pmod 6$*;*
- 1 *only, otherwise.*

For n *in* $\mathcal{I}A(p,a))$*, the set* $\mathcal{P}_n(\mathcal{I}A(p,a)))$ *consists of the set of primes dividing* $a(p^{n-1})D$*, where* $D = a(p)^2 - 4p^{2k-1}$*.*

4. Preliminaries for the proofs

4.1. *Divisibility of terms in Lucas sequences by their index*

For all pairs (P,Q), let $\mathcal{I}L(P,Q)$ be the set of all $n \geq 1$ for which n divides u_n. The following are the propositions which we shall be using in the course of this note.

Proposition 4.1 (Smyth [14]).

(i) For $n \in \mathcal{I}L = \mathcal{I}L(P,Q)$*, the set* $\mathcal{P}_n(\mathcal{I}L)$ *is the set of primes dividing* $u_n D$*.*
(ii) Every element of $\mathcal{I}L$ *can be written in the form* $bp_1p_2\cdots p_r$ *for some* $r \geq 0$*, where* $b \in \mathcal{B}(\mathcal{I}L)$ *is basic and, for* $i = 1, 2, \cdots r$*, the number* $bp_1p_2\cdots p_{i-1}$ *are also in* $\mathcal{I}L$*, and* p_i *is in* $\mathcal{P}_{bp_1p_2\cdots p_{i-1}}(\mathcal{I}L)$
(iii) The basic elements of $\mathcal{I}L$ *are*

- 1 *and* 6 *if* $P \equiv 3 \pmod 6, Q \equiv \pm 1 \pmod 6$*;*
- 1 *and* 12 *if* $P \equiv \pm 1 \pmod 6, Q \equiv -1 \pmod 6$*;*
- 1 *only, otherwise.*

Note that the primes p_i in (ii) need not be distinct.

Proposition 4.2 ([14]). *If* $n \in \mathcal{I}L(P,Q)$ *and all prime factors of* m *divide* $u_n D$*, then* $nm \in \mathcal{I}L(P,Q)$*.*

Proposition 4.3 ([14]). *Let* $n \in \mathcal{I}L(P,Q)$, $n > 1$*, with* p_{max} *its largest prime factor. Then, except in the case that* P *is odd and* n *is of the form* $2^l \cdot 3$ *for some* $l \geq 1$*, we have* $n/p_{max} \in \mathcal{I}L(P,Q)$*.*

4.2. *A lemma needed for the proofs*

Lemma 4.4. *Let* $(a(n))_{n\in\mathbb{N}}$ *be a sequence satisfying* (2.1)*,* (2.2) *and* (2.3)*, and let* p *and* q *be primes.*

(i) If $q \neq p$ *and* $q \mid a(p^\ell)$ *for some* $\ell \geq 1$*, then* $q \nmid a(p^{\ell-1})$ *and* $q \nmid a(p^{\ell+1})$*;*
(ii) If $p \mid a(p^\ell)$ *for some* $\ell \geq 1$ *then* $p \mid a(p)$*;*
(iii) If $q \mid a(n)$ *then either*

- $q \mid n$ *and* $q \mid a(q)$
  or
- $q \nmid a(nm)$ *for some* $m \in \mathbb{N}$ *with* $m \mid n$*;*

(iv) If $a(p) \neq 0$ *and* $p^f \| a(p)$ *then* $p^{ef} \| a(p^e)$*.*
(v) If $a(p) = 0$ *then for all* $r \geq 0$ *we have* $a(p^{2r}) = (-1)^r p^{(2k-1)r}$ *and* $a(p^{2r+1}) = 0$*.*

Proof.

(i) Take $q \neq p$ with $q \mid a(p^\ell)$. Suppose that $q \mid a(p^{\ell-1})$, and that r is the greatest index in $\{0, 1, \ldots, \ell-2\}$ such that $q \nmid a(p^r)$. Then $\ell \geq 2$, as $q \nmid a(1)$. Further, because $q \mid a(p^{r+1})$, we have $q \mid a(p^{r+2})$ and so, using (2.3), obtain a contradiction. Hence $q \nmid a(p^{\ell-1})$ and so, using (2.3) again, we have $q \nmid a(p^{\ell+1})$.

(ii) From $a(1) = 1$ and (2.3) we have by induction that

$$a(p^r) \equiv a(p)^r \pmod{p}.$$

Hence if $p \mid a(p^r)$ then $p \mid a(p)$.

(iii) Assume $q \mid a(n)$, with $n = \prod_p p^{e_p}$ say, so that $q \mid a(p^{e_p})$ for p in a nonempty set, $\mathcal{Q}_q$ say, of primes. If $q \in \mathcal{Q}_q$ we have $q \mid n$ and $q \mid a(q)$ by (ii). If $q \notin \mathcal{Q}_q$ then, by (i), $q \nmid a(p^{e_p+1})$. Hence $q \nmid a(nm)$ with $m = \prod_{p \in \mathcal{Q}_q} p$.

(iv) Suppose $p^f || a(p)$, where $f \geq 0$. From (2.1) we know that $f < k$. We use induction on e. The result is true for $e = 0$ (as $a(1) = 1$) and for $e = 1$. Now take $e \geq 1$ and assume that the result is true for e and $e-1$. Now $p^{(e+1)f} || a(p)a(p^e)$ and $p^{2k-1+(e-1)f} || p^{2k-1}a(p^{e-1})$, with $2k-1+(e-1)f = (e+1)f+2k-1-2f > (e+1)f$. Hence, from (2.3) we have $p^{(e+1)f} || a(p^{e+1})$, so that the result is true for e and $e+1$. This completes the induction.

(v) This comes immediately from $a(1) = 1$, $a(p) = 0$ and $a(p^{r+2}) = -p^{2k-1}a(p^r)$ from (2.3). □

5. Proofs

5.1. *Proof of Theorem 2.1*

Proof. Suppose that $p \mid C(n)$. If $p \nmid n$ then by Lemma 4.4(iii), $p \nmid a(nm)$, for some $m \mid n$, which contradicts $p \mid C(n)$. If $p \nmid a(p)$, then by Lemma 4.4(ii), $p \nmid a(p^{e_p})$. Since $p \mid C(n)$, we get $p \mid a(n/p^{e_p})$. By Lemma 4.4(iii) there exists $m \mid (n/p^{e_p})$ such that $p \nmid a(nm/p^{e_p})$. Therefore, $p \nmid a(nm)$, which contradicts $p \mid C(n)$. Hence we have proved, if $p \mid C(n)$ then $p \mid n$ and $p \mid a(p)$.

Note that, given $n \in \mathbb{N}$, there is always a $m_0 \in \mathbb{N}$ such that $a(nm_0) \neq 0$. Specifically, we can take $m_0 = \prod_{\substack{p^e || n: \\ a(p^e)=0}} p$, and use Lemma 4.4(v). Thus not all the $a(nm)$ are 0, so that the definition of $C(n)$ makes sense. Also, note that $a(nm) = 0$ for all m with $m_0 \nmid m$, since, for such m, $p^e || nm$ for some prime p with $a(p^e) = 0$. Hence $C(nm_0) = C(n)$ and so, by replacing n by nm_0 in what follows, we can assume that $a(n) \neq 0$. Note that this new n has the same values of e_p, as the old one for $a(p^e) \neq 0$, and the values $e_p + 1$ in place of e_p, when $a(p^e) = 0$.

We distinguish two cases.

(a) **The case $a(p) \neq 0$.**
By Lemma 4.4(iv), we get $p^{e_p f_p} || a(p^{e_p})$, where $p^{f_p} || a(p)$. Hence $p^{e_p f_p} \mid C(n)$. If $p \mid a(n/p^{e_p})$ then by Lemma 4.4(iii), there exists $m \mid (n/p^{e_p})$ such that $p \nmid a(nm/p^{e_p})$. Therefore, $p^{e_p f_p + 1} \nmid a(nm)$. Hence we get $p^{e_p f_p} || C(n)$.

(b) **The case $a(p) = 0$.**
By Lemma 4.4(v), $p^{(2k-1)e'_p} \mid a(p^{e_p})$. Suppose e_p is odd. Then $p^{(2k-1)e'_p} || a(p^{e_p+1})$. By Lemma 4.4(v), $p^{(2k-1)e'_p} \mid C(n)$. If $p \mid a(n/p^{e_p})$ then by Lemma 4.4(iii), $p \nmid a(nm/p^{e_p})$, for some $m \mid (n/p^{e_p})$. Therefore, $p^{(2k-1)e'_p+1} \nmid a(nmp)$. Therefore, $p^{(2k-1)e'_p} || C(n)$

If e_p is even then $p^{(2k-1)e'_p} || a(p^{e_p})$. By Lemma 4.4(v), $p^{(2k-1)e'_p} \mid C(n)$. As in last paragraph we can show, $p^{(2k-1)e'_p} + 1 \nmid a(nm)$, for some $m \mid (n/p^{e_p})$. Hence again $p^{(2k-1)e'_p} || C(n)$. □

5.2. *Proof of Theorem 3.3*

Proof. Take $n \in \mathcal{I}\tau$, so that $n \mid \tau(n)$. To find the primes $p \in \mathcal{P}_n = \mathcal{P}_n(\mathcal{I}\tau)$, i.e., those for which $np \mid \tau(np)$, we distinguish three cases:

(a) **The case $p \nmid n$.** Then from (2.2) we have

$$\tau(np) = \tau(n)\tau(p),$$

so that if $p \mid \tau(np)$ then $p \mid \tau(n)$ or $p \mid \tau(p)$.

Conversely, if $p \mid \tau(n)$ or $p \mid \tau(p)$ then $p \mid \tau(np)$ and, since $n \mid \tau(n)$ and $p \nmid n$, we have that $np \mid \tau(n)$ if $p \mid \tau(n)$, while $np \mid \tau(n)\tau(p)$ if $p \mid \tau(p)$. So $np \mid \tau(n)\tau(p) = \tau(np)$ in either case.

(b) **The case $e \geq 1$, $n = n'p^e$, $p \nmid n'$, $p \mid \tau(p)$.** Then $\tau(n) = \tau(n')\tau(p^e)$. By Lemma 4.4(iv),(v), it follows that $p^e \mid \tau(p^e)$, and as $n \in \mathcal{I}\tau$, $n' \mid \tau(n')\tau(p^e)$. But if $n' \nmid \tau(n')$ then we have $q \mid \tau(p^e)$ for some $q \mid n'$ which, by Lemma 4.4(i), gives $q \nmid \tau(p^{e+1})$ and hence $n' \nmid \tau(np)$. So we must have $n' \mid \tau(n')$. Then $np = n'p^{e+1} \mid \tau(n'p^{e+1}) = \tau(n')\tau(p^{e+1})$, since $p^{e+1} \mid \tau(p^{e+1})$, again by Lemma 4.4(iv).

Conversely, suppose that $n' \mid \tau(n')$. Then $p^{e+1} \mid \tau(p^{e+1})$. Therefore, $np = n'p^{e+1} \mid \tau(n')\tau(p^{e+1}) = \tau(np)$. Hence $p \in \mathcal{P}_n$.

(c) **The case $e \geq 1$, $n = n'p^e$, $p \nmid n'$, $p \nmid \tau(p)$.** So $p^e \mid \tau(n')\tau(p^e)$, giving $p^e \mid \tau(n')$ by Lemma 4.4(ii). We assume that $np \mid \tau(np) = \tau(n')\tau(p^{e+1})$. As in Case (b) this implies that $n' \mid \tau(n')$. Also, since $p \nmid \tau(p^{e+1})$ by Lemma 4.4(ii), we in fact have $p^{e+1} \mid \tau(n')$.
Conversely, suppose $n' \mid \tau(n')$ and $p^{e+1} \mid \tau(n')$. Since $p \nmid n'$, we have $np = n'p^{e+1} \mid \tau(n')$ and $\tau(n') \mid \tau(n'p^{e+1}) = \tau(np)$. Hence $p \in \mathcal{P}_n$. □

5.3. *Proof of Corollary 3.4*

Proof. Since $C_{2k}(n)$ is a product of nonordinary primes for τ_{2k}, every element of $\mathcal{I}C_{2k}$) must also be a product of nonordinary primes for τ_{2k}. Let n be such a product, say $n = \prod_p p^{e_p}$, where $p^{f_p} || \tau_{2k}(p)$ with all $f_p \geq 1$. We need to show that $p^{e_p} \mid C_{2k}(n)$ for all such p. This is immediate from (2.7) when $\tau_{2k}(p) \neq 0$. For $\tau_{2k}(p) = 0$, we have

$$e_p \leq 2e'_p < (2k-1)e'_p,$$

as $2k \geq 12$. □

5.4. *Proof of Theorem 3.5*

Proof. The proof is a straightforward application of Proposition 4.1. Fix a prime p and consider the sequence $u_n = a(p^{n-1})$ for $n \geq 1$. So $u_1 = a(1) = 1$, $u_2 = a(p)$, $u_3 = a(p^2), \ldots$.

Therefore, we have from (2.3) that

$$u_{n+1} = a(p)u_n - p^{2k-1}u_{n-1} \text{ for } n > 1. \tag{5.1}$$

Put $P = a(p),\ Q = p^{2k-1}$ so that for $n \geq 3$

$$u_n = Pu_{n-1} - Qu_{n-2}.$$

Hence the sequence $(u_n)_{n\geq 1}$ is a Lucas sequence of the first kind with these parameters P, Q, and with $D = P^2 - 4Q = a(p)^2 - 4p^{2k-1}$. Also $p^{2k-1} \equiv \pm 1 \pmod 6$ except for $p = 2$ or 3, and $p^{2k-1} \equiv -1 \pmod 6$ if and only if $p \equiv -1 \pmod 6$. Hence Theorem 3.5 follows straight from Proposition 4.1(iii). □

6. Example

Example 6.1. The set $\mathcal{IA}(p, \tau)$. We take $a(n) = \tau(n)$, Ramanujan's τ-function. Note that $D = \tau(p)^2 - 4p^{11}$. Since $\tau(n) \equiv \sigma_{11}(n) \pmod{2^8}$ for all positive odd integers n, we see $\tau(p)$ is even for any odd prime p, and so D is even. Since $\tau(2) = -24$, $\tau(p)$ is even for every prime p. Therefore $2 \in \mathcal{P}_1(\mathcal{IA}(p, \tau))$, for any choice of p. Furthermore, by Theorem 4.3, the only basic element is 1. Note that $p \mid D$ if and only if $p \mid \tau(p)$, and so $p \in \mathcal{IA}(p, \tau)$ if and only if p is nonordinary for τ. Also, 4.1(i) $\mathcal{P}_1(\mathcal{IA}(p, \tau))$ contains precisely the prime factors of $\tau(1)D = D$.

Now restricting to the particular case $p = 2$, we have $D = -7616 = -2^6 \cdot 7 \cdot 17$. Hence $\mathcal{P}_1(\mathcal{IA}(2, \tau)) = \{2, 7, 17\}$. Therefore, by Proposition 4.2 it follows that $2^k 7^l 17^m \in S_\tau$ for any choice of $k, l, m \in \mathbb{N} \cup \{0\}$. One can easily observe using Proposition 4.3 that, if $n \in \mathcal{IA}(2, \tau)$ then the minimal prime divisor of n has to belong to the set $\{2, 7, 17\}$.

Proposition 4.3 is useful in the sense that if we know $n \in \mathcal{IA}(2, \tau)$ and neither 2 nor 7 divides n, then n is not divisible by any prime q with $7 < q < 17$.

7. Computation of $\tau(n)$

The efficient computation of $\tau(n)$ is an interesting question. To compute $\tau(n)$ for a particular value of n, one way is to use Niebur's formula [10]

$$\tau(n) = n^4\sigma(n) - 24\sum_{k=1}^{n-1} k^2(35k^2 - 52kn + 18n^2)\sigma(k)\sigma(n-k)$$

for all $n \geq 1$. Here $\sigma(n)$ is the sum of the divisors of n. We remark that, by averaging the summand over k and $n-k$, we readily get the formula

$$\tau(n) = n^4\sigma(n) - M - 24 \sum_{k=1}^{\lfloor (n-1)/2 \rfloor} \left(n^4 + 70k^2(n-k)^2 - 20n^2k(n-k)\right)\sigma(k)\sigma(n-k),$$

having only half the number of terms of Niebur's formula. Here

$$M = \begin{cases} \left(\frac{9}{2}\right) n^4 \sigma\left(\frac{n}{2}\right)^2 & \text{if } n \text{ is even;} \\ 0 & \text{if } n \text{ is odd.} \end{cases}$$

For formulas like Niebur's for computing $\tau_{2k}(n)$ for $2k = 16, 18, 20, 22$ and 26, see Gouvêa [4].

When composing a table of $\tau(n)$, for $1 \leq n \leq N$ say, one can use Ramanujan's first recursion [11, p. 152]: $\tau(1) = 1$ and

$$\tau(n) = -\frac{24}{n-1} \sum_{k=1}^{n-1} \sigma(n-k)\tau(k),$$

for $n > 1$. A more efficient ($O(N^{3/2})$) method is to use Ramanujan's second recursion.

Lemma 7.1 ([11, p. 152] – see also D. H. Lehmer [6, p. 145]). *We have* $\tau(1) = 1$ *and, for* $n > 1$,

$$\tau(n) = \frac{1}{n-1} \sum_{j=1}^{\lfloor \sqrt{2n} - \frac{1}{2} \rfloor} (-1)^j (2j+1) \left(\tfrac{9}{2} j(j+1) - n + 1\right) \tau\left(n - \tfrac{1}{2} j(j+1)\right). \quad (7.1)$$

We give some more details of the proof, since Ramanujan and Lehmer gave only the essential (cunning!) idea.

Proof. Write

$$f(x) = \Delta(x)/x = \prod_{k=1}^{\infty} (1-x^k)^{24} = \sum_{n=0}^{\infty} \tau(n+1) x^n,$$

and

$$f_3(x) = \prod_{k=1}^{\infty} (1-x^k)^3 = \sum_{n=0}^{\infty} (-1)^n (2n+1) x^{n(n+1)/2},$$

the latter equality being Jacobi's identity. Then on logarithmically differentiating the identity $f(x) = (f_3(x))^8$ we obtain $f'(x) f_3(x) = 8 f(x) f_3'(x)$. Next, comparing the coefficients of x^n of both sides, we readily obtain (7.1), albeit with j satisfying $j \geq 1$ and $j(j+1)/2 \leq n-1$. While the latter inequality gives $j \leq \frac{1}{2}(\sqrt{8n-7} - 1)$, we can replace this bound by the slightly simpler one $\sqrt{2n} - \frac{1}{2}$, since there are no integers in the half-open interval $(\frac{1}{2}(\sqrt{8n-7} - 1), \sqrt{2n} - \frac{1}{2}]$. □

7.1. *Computation of $\tau(p)$*

Lygeros and Rosier [9] gave an algorithm of similar order, which uses Hurwitz class numbers to compute $\tau(p)$ for p prime. We reproduce their impressively short PARI/GP code from [9] here:

```
tau(p) = {
    tmax=floor(2*sqrt(p)); s10=0;
    for (t=1, tmax, s10+=(t^10)*qfbhclassno(4*p-t*t));
    return (p+1)*(42*p^5-42*p^4-48*p^3-27*p^2-8*p-1)-s10;
}
```

Recently, in a major breakthrough, Edixhoven *et al.* [2] have described how to compute $\tau(p)$ in polynomial time (i.e., in time bounded by a power of $\log p$) for p prime.

8. The least n for which $\tau(n)$ is prime

D.H. Lehmer [8] in 1965 claimed that the smallest n for which $\tau(n)$ is prime is for $n_0 = 63001 = 251^2$, with $\tau(n_0) = p_0$, where $p_0 = 805616635278024062573217 47$ is prime. Actually n_0 is only the smallest value of n for which $|\tau(n)|$ is prime, because in fact $\tau(n_0) = -p_0$. In his proof he worked to exclude the possibility that $\tau(n_0) = -2$, so it is clear that he was in fact studying the primality of $|\tau(n)|$. His method can readily be used to solve the original problem, showing that the smallest n for which $\tau(n)$ is prime is for $n_1 = 47^4 = 4879681$, with $\tau(n_1) = p_1$, where $p_1 = 4705942878159923138262416607648599521$. Lehmer shows that the least n for which $\tau(n)$ is an odd prime is for n an even power of an odd prime. Thus we only needed to search through $\tau(n)$ for such increasing n until we encountered a prime.

To show that there is no smaller n for which $\tau(n) = 2$, Lehmer shows that any such n must be a prime $p \equiv 1 \pmod{32 \cdot 691}$. There are no primes of this form less than 63001, which is all Lehmer needs for his proof. We, however, need to extend this to primes less than 47^4. To do this we make use of some extra congruences. Firstly, we use the Lehmer's congruence $\tau(n) \equiv n\sigma_9(n) \pmod 7$ [7], [15, p.4] to give

$$2 = \tau(p) \equiv p\sigma_9(p) \equiv p(1 + p^9) \equiv p\left(1 + \left(\frac{p}{7}\right)\right) \pmod 7,$$

giving $p \equiv 1 \pmod 7$. Finally, we use the congruence $\tau(n) \equiv \sigma_{11}(n) \pmod{2^{11}}$ for $n \equiv 1 \pmod 8$ [5], [15, p.4] to give

$$2 = \tau(p) \equiv \sigma_{11}(p) \equiv 1 + p^{11} \pmod{2^{11}},$$

so that $p^{11} \equiv 1 \pmod{2^{11}}$. Combining this with $p^{2^{10}} \equiv 1 \pmod{2^{11}}$ (Euler) we get $p = p^{2^{10}-11\cdot 93} \equiv 1 \pmod{2^{11}}$. Hence $p \equiv 1 \pmod{7 \cdot 691 \cdot 2^{11}}$. Since $7 \cdot 691 \cdot 2^{11} > 47^4$, we have the result.

Acknowledgments

The work described here was stimulated by a talk on Ramanujan's work by Ram Murty at IMSc, Chennai, in December 2011. We would like to thank Sanoli Gun and Ramachandran Balasubramanian for fruitful discussions. Also, we thank Shaun Stevens for a helpful remark.

References

[1] P. Deligne, La conjecture de Weil, *I. Inst. Hautes Études Sci. Publ. Math.* **43** (1974), 273–307.

[2] B. Edixhoven (ed.), J.-M. Couveignes (ed.) (Edixhoven, Bas; Couveignes, Jean-Marc; de Jong, Robin; Merkl, Franz; Bosman, Johan), *Computational aspects of modular forms and Galois representations. How one can compute in polynomial time the value of Ramanujans tau at a prime.* (Annals of Mathematics Studies **176**, Princeton, NJ: Princeton University Press, 2011.)

[3] L. Gallardo, On some formulae for Ramanujan's tau function, *Rev. Colombiana Mat.* **44** (2010), no. 2, 103–112.

[4] F. Q. Gouvêa, Non-ordinary primes: a story, *Experiment. Math.* **6** (1997), no. 3, 195–205.

[5] O. Kolberg, Congruences for Ramanujan's function $\tau(n)$, *Arbok Univ. Bergen Mat.-Natur. Serie* **1962** (1962), No.11, 8pp.

[6] D.H. Lehmer, Computer technology applied to the theory of numbers, *Studies in Number Theory* (Math. Assoc. Amer., distributed by Prentice-Hall, Englewood Cliffs, N.J., 1969), pp. 117–151.

[7] D.H. Lehmer, *Notes on some arithmetical properties of elliptic modular functions.* (Duplicated notes, Univ. of California at Berkeley, undated).

[8] D.H. Lehmer, The primality of Ramanujan's tau-function, *Amer. Math. Monthly* **72** (1965) no. 2, part II, 15–18.

[9] N. Lygeros, O. Rozier, A new solution to the equation $\tau(p) \equiv 0 \pmod{p}$, *J. Integer Seq.* **13** (2010), no. 7, Article 10.7.4, 11 pp.

[10] D. Niebur, A formula for Ramanujan's τ-function, *Illinois J. Math.* **19** (1975), 448–449.

[11] S. Ramanujan, *Collected Papers.* (Cambridge, UK: Cambridge University Press, 1927. Reprinted New York, 1962).

[12] J.-P. Serre, *A course in arithmetic.* (GTM 7, Springer-Verlag New York-Heidelberg, 1973).

[13] J.-P. Serre, Divisibilité de certaines fonctions arithmétiques, *Séminaire Delange-Pisot-Poitou*, 16e année (1974/75), Théorie des nombres, Fasc. 1, Exp. No. 20, (Secrétariat Mathématique, Paris, 1975), 28pp.

[14] C. Smyth, The terms in Lucas sequences divisible by their indices, *J. Integer Seq.* **13** (2010), no. 2, Article 10.2.4, 18 pp.

[15] H. P. F. Swinnerton-Dyer, On l-adic representations and congruences for coefficients of modular forms, *Modular functions of one variable*, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973, pp. 1–55.