Lehmer's Conjecture on the Non-vanishing of Ramanujan's Tau Function

Will Y. Lee

Abstract

In this paper we prove Lehmer's conjecture on Ramanujan's tau function, namely $\tau(n) \neq 0$ for each $n \geq 1$ by investigating the additive group structure attached to $\tau(n)$ with the aid of unique factorization theorem.

[1] Let E_k $(k = 2, 4, \dots)$ be the normalized Eisenstein series ($[4 : 108 - 122]$) given by

$$E_k = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \tag{1}$$

where $q := e^{i2\pi z}$ $(\Im(z) > 0), B_k$ the Bernoulli number defined by

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}$$

and $\sigma_{k-1}(n)$ the divisor function:

$$\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}.$$

For an elliptic curve given by

$$y^2 = 4x^3 - g_2(z)x - g_3(z) \tag{2}$$

where $g_2(z) = 120\zeta(4)E_4(z), g_3(z) = 280\zeta(6)E_6(z)$ and $E_k(z)$ given by equation (1) and $\zeta(k)$ is Riemann zeta function:

$$\zeta(k) := \sum_{n=1}^{\infty} \frac{1}{n^k}.$$

[1]2000 Mathematics Subject Classification. Primary $11L40$; Secondary $11YXX$

A simple calculation ([1 : 14], [4 : 112]) shows the discriminant $\varDelta(z) := 4^4(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$, where x_1, x_2 and x_3 are the roots the right side of equation (2), is given by

$$\varDelta(z) = g_2(z)^3 - 27g_3(z)^2 = \frac{(2\pi)^{12}}{1728}(E_4(z)^3 - E_6(z)^2). \tag{3}$$

On the other hand Jacobi's theorem ([4 : 122]) asserts that

$$(2\pi)^{-12}\varDelta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}. \tag{4}$$

From equation (4), Ramanujan has defined his tau function $\tau(n)$ ([1], [2], [3], [4 : 122], [5]−[7]) by

$$q\prod_{n=1}^{\infty}(1-q^n)^{24} := \sum_{n=1}^{\infty}\tau(n)q^n. \tag{5}$$

Notice that each $\tau(n)$ $(n \geq 1)$ has an integer value. In a series of papers ([5] − [7]), D.H. Lehmer investigated the properties of $\tau(n)$ for $n \leq 300$, proved that $\tau(n) \neq 0$ for $n < 3316799$, later for $n < 214928639999$ ([1 : 22]). He also showed that if $\tau(n) = 0$ then n must be a prime. He then conjectured, what is nowadays known as Lehmer's conjecture ([6]) that

$$\tau(n) \neq 0 \text{ for } \text{ each } n \geq 1. \tag{6}$$

A simple calculation ([3 : 21 − 22], [4 : 122 − 123]) shows

$$\tau(n) = \frac{65}{756}\sigma_{11}(n) + \frac{691}{756}\sigma_5(n) - \frac{691}{3}\sum_{j=1}^{n-1}\sigma_5(j)\sigma_5(n-j). \tag{7}$$

Since Lehmer's conjecture is equivalent to $3\tau(n) \neq 0$ for each $n \geq 1$, we write

$$A(n) := \frac{65}{252}\sigma_{11}(n) + \frac{691}{252}\sigma_5(n);\ B(n) := 691\sum_{j=1}^{n-1}\sigma_5(j)\sigma_5(n-j). \tag{8}$$

Then $3\tau(n) = A(n) - B(n)$. Observe that $A(n)$ takes on integer value for each $n \geq 1$ since both $\tau(n)$ and $B(n)$ do. Now Lehmer's conjecture is, in view of equations (7), (8) and the unique factorization theorem, equivalent to:

$$A(n) \neq B(n) \text{ for each } n \geq 1. \tag{9}$$

Recent calculation by Bosman confirms Lehmer's conjecture for $n \leq 22798241520242687999$. In this paper we prove equation (9) by showing that $\{\sum_{k=0}^{q-1} k a_{i,k} \bmod q\}_{k=0}^{q-1}$ forms an additive group of order q modulo q for $q \mid A(p)$, $q > p$, $p \equiv -1 \bmod 691$, $[a_{i,k}]_{0\leq i,k\leq q-1}$ $q \times q$-matrix, with the aid of the unique factorization theorem, the pigeonhole principle and the remainder theorem. We prove equation (9) first for prime p then for $p^\alpha, \alpha \geq 2$ and finally for any composite number n. Since $11 \nmid 690$ and since $(p+1) \mid (p^{11}+1)$, the following Lemma 1 evidently holds.

Lemma 1 *Let $A(p)$ be given by equation* (8)*. Then the following two conditions* (10) *and* (11) *are equivalent:*

$$A(p) \equiv 0 \mod 691. \tag{10}$$

$$p \equiv -1 \mod 691. \tag{11}$$

If $691 \nmid A(p)$ or equivalently p does not satisfy equation (11) then we trivially have $A(p) \neq B(p)$ by equation (8). It suffices therefore to prove Lehmer's conjecture for prime p satisfying equation (10) or (11). In what follows, prime p satisfies either equation (10) or (11). We first prove:

Lemma 2 *Let p satisfy equation* (10) *or* (11)*. There is at least one prime $q \mid A(p)$ such that $q > p$.*

Proof. Write $x = [x] + \{x\}$, where $[x]$ stands for the integral part of x, $\{x\}$ non-integral part of x. Now

$$\begin{array}{rclllll} A(p) & = & \frac{65}{252}(1+p^{11}) & + & \frac{691}{252}(1+p^5) & & \\ & = & 3 & + & \frac{65}{252}p.p^{10} & + & \frac{691}{252}p^5 \\ & = & 3 & + & [\frac{65}{252}p]p^{10} & + & p\{\frac{65}{252}p\}p^9 \; + \; \frac{691}{252}p^5. \end{array}$$

Since $\{p\{\frac{65}{252}p^i\}\} = \{\frac{65}{252}p^{i+1}\}$, continuation of the above procedure leads us to:

$$\begin{array}{rl} A(p) = & 3 + \sum_{i=5}^{10} a_i p^i,\ a_5 = p\{\frac{65p^5}{252}\} + \frac{691}{252},\ a_i = [p\{\frac{65}{252}p^{10-i}\}] \\ & 7 < a_5 < p,\ 4 < a_i < p\ (6 \le i \le 10). \end{array} \tag{12}$$

For the last part of equation (12), notice that $p > a_5 \ge p/252 + 691/252 > 5 + 2 = 7$ and $p > a_i \ge p/252 > 4$, as $p = 1381$ is the smallest prime satisfying equation (11). Assume $A(p)$ has no prime factor greater than p. Write

$$A(p) = 2^{e_0} q_1^{e_1} q_2^{e_2} \dots q_m^{e_m},\ e_i \ge 1,\ q_i < p\ (1 \le i \le m). \tag{13}$$

Observe that $A(p)$ has an even factor 2^{e_0} which follows from substitution of equation (11) into equation (8). Since $0.25p^{11} < A(p) < 0.26p^{11}$ from equation (8), we have

$$\begin{array}{rclllll} A(p) & = & \frac{A(p)}{p^{10}}p^{10} & & & & \\ & = & [\frac{A(p)}{p^{10}}]p^{10} & + & p\{\frac{A(p)}{p^{10}}\}p^9 & & \\ & = & [\frac{A(p)}{p^{10}}]p^{10} & + & [p\{\frac{A(p)}{p^{10}}\}]p^9 & + & p\{\frac{A(p)}{p^9}\}p^8. \end{array}$$

Since $\{p\{\frac{A(p)}{p^i}\}\} = \{\frac{A(p)}{p^{i-1}}\}$ $(1 \le i \le 10)$, continuation of the above argument shows us:

$$A(p) = \sum_{i=0}^{10} b_i p^i,\ b_i = [p\{\frac{A(p)}{p^{i+1}}\}],\ 1 \le b_i < p\ \ (0 \le i \le 10). \tag{14}$$

$A(p)$ in equation (14) is given by equation (13). Since each $q_i < p$ $(1 \le i \le m)$ from equation (13) and since $\{\frac{A(p)}{p^{i+1}}\} = \{\frac{\sum_{j=0}^{i} b_j p^j}{p^{i+1}}\} < \{\frac{p^{i+1}}{p^{i+1}}\} = 1$ $(0 \le i \le 10)$ from the first part of equation (14), the last part of equation (14), namely $1 \le b_i < p$ $(1 \le i \le 10)$ follows from the following equivalent statements:

$$A(p) \not\equiv 0 \bmod p^i \Longleftrightarrow \frac{1}{p} < \{\frac{A(p)}{p^{i+1}}\} < 1 \Longleftrightarrow 1 < [p\{\frac{A(p)}{p^{i+1}}\}] = b_i < p\ \ (1 \le i \le 10).$$

Since $a_i \neq b_i$ $(1 \leq i \leq 10)$ from equations (12) and (14) respectively, equation (14) contradicts equation (12) by the unique representation theorem in the powers of p^i $(0 \leq i \leq 10)$ regardless of the value of $b_0 \geq 1$ in equation (14). This establishes Lemma 2.

Let q be an odd prime prime factor of $A(p)$. Construct matrix $[a_{i,k}]_{0\leq i,k\leq q-1}$ as follows:

$$a_{i,k} := \sum_{\substack{j = 1 \\ i691\sigma_5(j)\sigma_5(p-j) \equiv k \bmod q}}^{p-1} 1. \tag{15}$$

Since $\sigma_5(j)\sigma_5(p-j) = \sigma_5(p-j)\sigma_5(p-(p-j))$, we have from equation (15)

$$a_{i,k} = 2 \sum_{\substack{j = 1 \\ i691\sigma_5(j)\sigma_5(p-j) \equiv k \bmod q}}^{(p-1)/2} 1. \tag{16}$$

Then the matrix $[a_{i,k}]_{0\leq i,\, k\leq q-1}$ has the following properties:

$$a_{i,k} \equiv 0 \mod 2 \qquad (0 \leq i, k \leq q-1). \tag{17}$$

$$a_{0,0} = p-1,\ a_{0,k} = 0 \qquad (1 \leq k \leq q-1). \tag{18}$$

$$a_{i,0} = a_{j,0} \qquad (1 \leq i \neq j \leq q-1). \tag{19}$$

$$a_{i,k} = a_{q-i,q-k} \qquad (1 \leq i, k \leq q-1). \tag{20}$$

$$i691\sum_{j=1}^{p-1}\sigma_5(j)\sigma_5(p-j) \equiv \sum_{k=1}^{q-1} k a_{i,k} \mod q \qquad (1 \leq i \leq q-1). \tag{21}$$

$$\sum_{k=1}^{q-1} k a_{i,k} \equiv i\sum_{k=1}^{q-1} k a_{1,k} \mod q \quad (1 \leq i \leq q-1). \tag{22}$$

Notice that given $a_{1,k}$ $(1 \leq k \leq q-1)$, $a_{i,k}$ $(2 \leq i \leq q-1, 1 \leq k \leq q-1)$ are reshuffles of $a_{1,k}(1 \leq k \leq q-1)$ and vice versa determined by

$$a_{i,k} = a_{1,i^{-1}k \bmod q} \Longleftrightarrow a_{1,k} = a_{i,ik \bmod q} \quad (2 \le i \le q-1, 1 \le k \le q-1). \tag{23}$$

Let $q \mid A(p)$ with $q > p$. Such a prime q exists by Lemma 2. Write $f_j := 691\sigma_5(j)\sigma_5(p-j) \bmod q$ $(1 \le j \le (p-1)/2)$. Then $f_j = f_{p-j}$ $(1 \le j \le (p-1)/2)$. Define:

$$\begin{array}{rcl} S_{1,l} & := & \{k : a_{1,k} = 2l \ (0 \le l \le q_0)\} \\ & = & \{(j_1, j_2, \ldots, j_l) : 1 \le j_1 < j_2 < \cdots < j_l \le \frac{p-1}{2},\ f_{j_1} = f_{j_2} = \cdots = f_{j_l} \ (1 \le l \le q_0)\} \\ S_{1,l} & = & \varnothing \ \text{ for } l > q_0. \end{array} \tag{24}$$

The second identity of equation (24) follows from equation (15). Since $q > p$ and since $a_{i,k}$ $(0 \le i, k \le q-1)$ cannot be too large even number from equations (15) and (16), a positive integer $q_0 < q-1$ exists, depending on p and q, satisfying the last line of equation (24). We then have when $q \mid A(p)$ with $q > p$:

$$\textstyle\sum_{l=0}^{q_0} \mid S_{1,l} \mid \ = q. \tag{25}$$

$$\textstyle\sum_{k=1}^{q-1} a_{i,k} \ = \displaystyle\sum_{l=1}^{q_0} 2l \mid S_{1,l} \mid = p-1. \tag{26}$$

Equation (26) reads when $q \mid A(p)$ with $q < p$ that:

$$\sum_{k=0}^{q-1} a_{i,k} = p-1 \ (1 \le i \le q-1). \tag{27}$$

Equations (17) – (23) readily follow from equations (15) and (16). Equation (21) is a restatement of the remainder theorem in view of equations (15), (26) and (27). Equations (25) – (27) follow from the pigeonhole principle. Lehmer's conjecture therefore is equivalent via equation (21) for $i = 1$ to:

$$\sum_{k=0}^{q-1} k a_{1,k} \not\equiv 0 \mod q. \tag{28}$$

Since both $A(p)$ and $B(p)$ are even and divisible by 691, we have $(A(p), B(p)) \ge 1382$. Suppose q divides both $A(p)$ and $B(p)$. Then by equation (21), we have:

$$\sum_{k=0}^{q-1} ka_{i,k} \equiv 0 \mod q \ (0 \leq i \leq q-1). \tag{29}$$

Clearly equation (29) is equivalent by equation (22) to:

$$\sum_{k=0}^{q-1} ka_{1,k} \equiv 0 \mod q. \tag{30}$$

Since $\sum_{k=0}^{q-1} ka_{0,k} = 0 \equiv 0 \bmod q$ by equation (18), it follows that $\{\sum_{k=0}^{q-1} ka_{i,k} \bmod q\}_{i=0}^{q-1} = \{0\}$, the trivial additive group modulo q. Conversely, equation (29) or (30) implies both $q \mid A(p)$ and $q \mid B(p)$ by equation (21). On the other hand, since nonzero $a_{i,k}$ $(0 \leq i \leq q-1)$ is even and ≥ 2 from equation (17), with the aid of the unique factorization theorem, equation (29) or (30) is equivalent to:

$$\min_{1 \leq i < j \leq q-1} \left(\sum_{k=0}^{q-1} ka_{i,k}, \ \sum_{k=0}^{q-1} ka_{j,k}\right) = 2q. \tag{31}$$

Consequently equation (29), (30) or (31) completely characterizes common prime factors of both $A(p)$ and $B(p)$. We thus have:

Lemma 3 *The following conditions are equivalent:*

(i) q divides both $A(p)$ and $B(p)$.

(ii) $\sum_{k=0}^{q-1} ka_{i,k} \equiv 0 \mod q \ (0 \leq i \leq q-1)$.

(iii) $\sum_{k=0}^{q-1} ka_{1,k} \equiv 0 \mod q$.

(iv) $\{\sum_{k=0}^{q-1} ka_{i,k} \bmod q\}_{i=0}^{q-1} = \{\varnothing\}$, *the trivial additive group modulo q.*

(v) $\min_{1\le i<j\le q-1}(\sum_{k=0}^{q-1} ka_{i,k},\ \sum_{k=0}^{q-1} ka_{j,k}) = 2q.$

Lemma 4 *(Main Lemma) Let p satisfy equation (10) or (11) and let $q \mid A(p)$ with $q > p$. Then $\{\sum_{k=0}^{q-1} ka_{i,k} \bmod q\}_{i=0}^{q-1}$ forms an additive group of order q modulo q.*

Proof. Let $a_{i,k}$ $(0 \le i, k \le q-1)$ be defined by equation (15). We have for each $i = 1, 2, \ldots, q-1$:

$$\begin{array}{llll} & \sum_{k=0}^{q-1} ka_{i,k} & + \ \sum_{k=0}^{q-1} ka_{q-i,k} & \\ = & \sum_{k=1}^{q-1} ka_{i,k} & + \ \sum_{k=1}^{q-1} ka_{i,q-k} & \text{by (20)} \\ = & \sum_{k=1}^{q-1} ka_{i,k} & + \ \sum_{k=1}^{q-1}(q-k)a_{i,k} & \\ = & q\sum_{k=1}^{q-1} a_{i,k} & & \\ = & q\sum_{l=1}^{q_0} 2l \mid S_{1,l} \mid & \text{by (24)} & \\ = & q(p-1) & \text{by (26)} & \end{array} \tag{32}$$

Notice that equation (32) holds regardless of $\{\sum_{k=0}^{q-1} ka_{i,k} \bmod q\}_{i=0}^{q-1}$ being trivial or not. We claim that $\{\sum_{k=0}^{q-1} ka_{i,k}\}_{i=0}^{q-1}$ are all distinct. To show the claim observe that $\{S_{1,l}\}_{l=0}^{q_0}$ are disjoint from equation (24). Since $f_j = f_{p-j}$ $(1 \le j \le (p-1)/2)$, it follows that each k for which $a_{1,k} \neq 0$ $(1 \le k \le q-1)$, the corresponding values of j such that $k = f_j$ $(1 \le j \le (p-1)/2)$ appear pairwise, namely j and $p-j$. We first prove:

$$\mid S_{1,1} \mid > 2! \mid S_{1,2} \mid > 3! \mid S_{1,3} \mid > \cdots > q_0! \mid S_{1,q_0} \mid \tag{33}$$

Write $\nu_l := \mid S_{1,l} \mid$ $(1 \le l \le q_0)$. Since the same proof works for each $l = 2, 3, \ldots, q_0$, we prove inequality (33) for l $(2 \le l \le q_0)$ only. Let $(j_{1i}, j_{2i}, \ldots, j_{li})$ $(1 \le i \le \nu_l) \in S_{1,l}$ with $1 \le j_{1i} < j_{2i} < \cdots < j_{li} \le (p-1)/2$ such that $f_{j_{1i}} = f_{j_{2i}} = \cdots = f_{j_{li}}$ $(1 \le i \le \nu_l)$ from the second line of equation (24). Consider the map $\beta : S_{1,l-1} \mapsto S_{1,l-1}$ given by:

$$\begin{array}{rl} \beta(j_{1i}, j_{2i}, \ldots, j_{li}) := & ((\beta_1(j_{1i}), \beta_2(j_{1i}), \ldots, \beta_{l-1}(j_{1i})), (\beta_1(j_{2i}), \beta_2(j_{2i}), \ldots, \beta_{l-1}(j_{2i})), \ldots, \\ & (\beta_1(j_{1i}), \beta_2(j_{1i}), \ldots, \beta_{l-1}(j_{1i}))) \ (1 \le i \le \nu_l). \end{array} \tag{34}$$

$$\begin{array}{rl} a_{1,\beta_1(j_{mi})} & = l-1, \ \mid j_{mi} - \beta_1(j_{mi}) \mid = \text{ minimum}, \ \beta_1(j_{ui}) \neq \beta_1(j_{vi}) \\ & (1 \le m \le l, \ 1 \le u < v \le l, \ 1 \le i \le \nu_l). \end{array} \tag{35}$$

$$f_{\beta_1(j_{mi})} = f_{\beta_2(j_{mi})} = \cdots = f_{\beta_{l-1}(j_{mi})} \ (1 \le m \le l,\ 1 \le i \le \nu_l). \tag{36}$$

Notice that each $(\beta_1(j_{mi}), \beta_2(j_{mi}), \ldots, \beta_{l-1}(j_{mi}))$ $(1 \le m \le l,\ 1 \le i \le \nu_l)$ from equation (34) belongs to $S_{1,l-1}$ in view of equations (35) and (36). In equation (35), once $\beta_1(j_{1i})$ $(1 \le i \le \nu_l)$ is selected, $\beta_1(j_{mi})$ $(2 \le m \le l,\ 1 \le i \le \nu_l)$ is successively chosen to satisfy the last two conditions of equation (35). Given $\beta_1(j_{mi})$ $(1 \le m \le l,\ 1 \le i \le \nu_l)$ determined by equation (35), $\beta_k(j_{mi})$ $(2 \le k \le l-1,\ 1 \le m \le l,\ 1 \le i \le \nu_l)$ are uniquely determined by equation (36). Let k_l be the smallest integer for which $a_{1,k_l} = l$. From the first line of equation (24), there is at least one integer $k < k_l$ such that $a_{1,k} = l-1$ which is not represented by equation (34). It follows that the map $\beta : S_{1,l} \mapsto S_{1,l-1}$ given by equations (34) $-$ (36) maps $S_{1,l}$ into a proper subset of $S_{1,l-1}$ in a fashion of 1 to l (see equation (34)). Consequently we have:

$$\mid S_{1,l-1} \mid > \ l \mid S_{1,l} \mid \ \ (2 \le l \le q_0).$$

Notice that the above inequality is a strict one. Repetitive application of the above inequality for each $l = 2, 3, \ldots, q_0$ shows inequality (33). See Table 1 for examples of primes p with $q \mid A(p),\ q > p$, satisfying inequality (33), where $q_0 \le 4$. Since $a_{i,k} = a_{1,i^{-1}k \bmod q}$ from equation (23), we have for each $l = 1, 2, \ldots, q_0$:

$$\begin{array}{lcl} \sum\limits_{k \in S_{1,l}} k a_{i,k} & = & \sum\limits_{k \in S_{1,l}} k a_{1,i^{-1}k \bmod q} \quad = \\ \sum\limits_{k \in S_{1,l}} ik \pmod{q}\ a_{1,k} & = & 2l \sum\limits_{k \in S_{1,l}} ik \pmod{q}. \end{array} \tag{37}$$

It is evident for each $1 \le i \ne j \le q-1$ and each l $(1 \le l \le q_0)$ that:

$$\sum_{k \in S_{1,l}} ik \pmod{q} \ne \sum_{k \in S_{1,l}} jk \pmod{q}. \tag{38}$$

For each $1 \le i \ne j \le q-1$, conjunction of equations (33), (37) and (38) leads us to

$$\begin{array}{rl} & \sum_{k=0}^{q-1} ka_{i,k} \\ = & \sum_{l=1}^{q_0} 2l \sum_{k\in S_{1,l}} ik \pmod q \text{ by (26) \& (37)} \\ \neq & \sum_{l=1}^{q_0} 2l \sum_{k\in S_{1,l}} jk \pmod q \text{ by (33) \& (38)} \\ = & \sum_{k=0}^{q-1} ka_{j,k} \text{ by (26) \& (37).} \end{array} \tag{39}$$

Equation (39) establishes the claim. Since $\sum_{k=0}^{q-1} ka_{1,k} \bmod q$ is a generator for the additive group $\{\sum_{k=0}^{q-1} ka_{i,k} \bmod q\}_{i=0}^{q-1}$ from equation (22) if it is nontrivial, it suffices therefore to show that

$$\sum_{k=0}^{q-1} ka_{1,k} \not\equiv 0 \bmod q. \tag{40}$$

Write

$$C_i := \sum_{k=0}^{q-1} ka_{i,k} \ (1 \leq i \leq q-1). \tag{41}$$

Notice that $\{C_i\}_{i=1}^{q-1}$ are distinct from equation (39). Rename C_i $(1 \leq i \leq q-1)$ again as C_i $(1 \leq i \leq q-1)$ in ascending order as follows:

$$C_1 < C_2 < \cdots < C_{q-1}. \tag{42}$$

We claim that there is at least one pair $\{C_j, C_{j+1}\}$ $(1 \leq j \leq q-2)$ from equation (42) such that

$$C_{j+1} - C_j < q-1 \text{ for some } j \ (1 \leq j \leq q-2). \tag{43}$$

Assume equation (43) is false. We then have:

$$\begin{array}{rl} & C_{q-1} \\ := & \max\limits_{1\leq i\leq q-1} \sum_{k=1}^{q-1} ka_{i,k} \text{ by (42)} \\ := & \sum_{k=1}^{q-1} ka_{i_0,k} \text{ for some } i_0 \ (1 \leq i_0 \leq q-1) \\ = & C_1 + \sum_{k=1}^{q-2} (C_{k+1} - C_k) \\ \geq & C_1 + \sum_{k=1}^{q-2} (q-1) \text{ by assumption} \\ > & (q-2)(q-1). \end{array} \tag{44}$$

On the other hand, we estimate C_{q-1} from equations (15) and (26). Since each nonzero $a_{i_0,k}$ $(0 \leq i_0 \leq q-1)$ is even ≥ 2 from equation (17), there are at most $(p-1)/2$ -numbers of nonzero $a_{i_0,k} \geq 2$ $(0 \leq k \leq q-1)$. Notice that each nonzero $a_{i_0,k}$ is a small even number due to equations (24) and (26) with $2 \leq a_{i_0,k} \leq 2q_0$ $(0 \leq k \leq q-1)$. It follows that there are at least $(q-1-(p-1)/2)$ -numbers of $a_{i_0,k} = 0$ $(0 \leq k \leq q-1)$. We then have:

$$\begin{array}{rl} & C_{q-1} \\ = & \sum_{k=0}^{q-1} k a_{i_0,k} \\ = & \sum_{k=0}^{q-1} i_0 k \pmod{q}\ a_{1,k} \quad \text{by (23)} \\ = & \sum_{l=1}^{q_0} 2l \sum\limits_{k \in S_{1,l}} i_0 k \pmod{q} \text{ by (26)} \\ = & 2(\sum_{l=1}^{q_0} l(\sum\limits_{k \in S_{1,l}} i_0 k \pmod{q})) \\ < & 2(\sum_{k=1}^{(p-1)/2} (q-k)) \\ = & (q-(p+1)/4)(p-1) \\ < & (q-2)(q-1). \end{array} \tag{45}$$

In the last part of inequality (45), we use the assumption $q > p$ and $p \geq 1381$, the smallest prime satisfying $691 \mid A(p)$. Observe that the total number of $k's$ in the summation $2(\sum_{l=1}^{q_0} l(\sum\limits_{k \in S_{l,l}} i_0 k \pmod{q})))$ in the middle of inequality (45) is $\leq (p-1)/2$ from equation (26), with $i_0 k \pmod{q}$ counted twice for $k \in S_{1,2}$, $i_0 k \pmod{q}$ counted thrice for $k \in S_{1,3}$, etc. The last part of inequality (45) contradicts inequality (44). This establishes inequality (43). For j chosen from equation (43), since each nonzero $a_{i,k} \geq 2$ $(1 \leq i \leq q-1,\ 0 \leq k \leq q-1)$, we then have:

$$2 \leq (C_j,\ C_{j+1}) = (C_j,\ C_{j+1} - C_j) < q-1. \tag{46}$$

Equation (46) implies $C_j := \sum_{k=0}^{q-1} k a_{u,k}$ and $C_{j+1} := \sum_{k=0}^{q-1} k a_{v,k}$ for some u, v $(1 \leq u,\ v \leq q-1)$ have no common factor q, which leads to $q \nmid \sum_{k=0}^{q-1} k a_{1,k}$ in view of equation (22), thereby proving equation (40). Consequently, each $\sum_{k=0}^{q-1} k a_{i,k}$ $(1 \leq i \leq q-1)$ has no factor q from equations (22) and (40). We thus have:

$$\sum_{k=0}^{q-1} ka_{i,k} \not\equiv 0 \bmod q, \ 1 \le i \le q-1. \tag{47}$$

Equation (47) is equivalent that the map:

$$\{\sum_{k=0}^{q-1} ka_{i,k} \bmod q\}_{i=0}^{q-1} \longmapsto \mathbb{Z}/q\mathbb{Z}$$

is an isomorphism. Furthermore equations (32) and (47) reveal the structure of the additive group $\{\sum_{k=0}^{q-1} ka_{i,k} \bmod q\}_{i=0}^{q-1}$ which is nontrivial, namely

$$\sum_{k=0}^{q-1} ka_{i,k} + \sum_{k=0}^{q-1} ka_{q-i,k} \equiv 0 \bmod q, \ 1 \le i \le q-1. \tag{48}$$

Equations (47) and (48) show $\sum_{k=0}^{q-1} ka_{i,k} \bmod q$ and $\sum_{k=0}^{q-1} ka_{q-i,k} \bmod q$ are additive inverse to each other modulo q for each $i = 1, 2, \ldots q-1$. Needless to say from equation (18), $\sum_{k=0}^{q-1} ka_{0,k} = 0 \equiv 0 \pmod q$ is the additive identity modulo q. This completes the proof of Lemma 4.

Since $p \nmid A(p)$ from equation (12), conjunction of Lemma 3 and Lemma 4 leads us to:

Corollary 5 *Let* $691 \mid A(p)$*. An odd prime* q *divides both* $A(p)$ *and* $B(p)$ *only if* $q < p$*.*

From Lemma 4, we have in particular for $i = 1$:

$$B(p) = 691 \sum_{j=1}^{p-1} \sigma_5(j)\sigma_5(p-j) \equiv \sum_{k=0}^{q-1} ka_{1,k} \not\equiv 0 \bmod q \ \text{ by (21) \& (47).} \tag{49}$$

Equation (49) implies $q \nmid B(p)$ and hence $A(p) \neq B(p)$ and $\tau(p) = (A(p) - B(p))/3 \neq 0$ via the unique factorization theorem if $691 \mid A(p)$. If $691 \nmid A(p)$, then since $691 \mid B(p)$ from equation (8), we trivially have $A(p) \neq B(p)$ and $\tau(p) = (A(p) - B(p))/3 \neq 0$ via the unique factorization theorem in this case too. We thus have:

Theorem 6 *$\tau(p) \neq 0$ for each prime p.*

For $691 \mid A(p)$ and $q \mid A(p)$ with $q > p$, since $\{\sum_{k=0}^{q-1} ka_{i,k}\}_{i=0}^{q-1}$ are distinct from equation (39) and since $q \nmid \sum_{k=0}^{q-1} ka_{i,k}$ $(1 \leq i \leq q-1)$ from Lemma 4, we have $\sum_{k=0}^{q-1} ka_{i,k} = 2^s t$ $(s \geq 1,\ t = \text{odd},\ 1 \leq i \leq q-1)$, where $q \nmid t$ from Lemma 4. Since $q > p$, and since each nonzero $a_{i,k} \geq 2$ from equation (17), there is at least one i $(1 \leq i \leq q-1)$ such that $\sum_{k=0}^{q-1} ka_{i,k} = 2t,\ q \nmid t$. We thus have with the aid of unique factorization theorem:

Corollary 7 *Suppose p satisfies equation* (10) *or* (11)*. Let $q \mid A(p)$ with $q > p$. Then*

$$\min_{1 \leq i < j \leq q-1} \left(\sum_{k=0}^{q-1} ka_{i,k},\ \sum_{k=0}^{q-1} ka_{j,k}\right) = 2.$$

Now let $\alpha \geq 2$. Then equations (10) and (11) are no longer equivalent. As in the case of $\alpha = 1$, since $A(p^\alpha) \equiv 3 \bmod p^5$ and $p^{11\alpha-1} < A(p^\alpha) < p^{11\alpha}$ from equation (8), an almost identical proof of Lemma 2 works for $\alpha \geq 2$. However, the upper limit 10 in the summation of the representation of $A(p)$ in the powers of p^i $(0 \leq i \leq 11\alpha - 1)$ of equation (12) is replaced by $11\alpha - 1$ for $\alpha \geq 2$. We thus have:

Lemma 8 *Let $691 \mid A(p^\alpha)$ for $\alpha \geq 2$. There is at least one prime $q \mid A(p^\alpha)$ with $q > p^\alpha$.*

For $q \mid A(p^\alpha)$, construct matrix $[a_{i,k}]_{0 \leq i,\ k \leq q-1}$ exactly the same way as in equation (15). Then properties (17) – (23), (25) – (27) hold with p replaced by p^α. Likewise almost the same proof for Lemma 4 works for $\alpha \geq 2$. We thus have:

Lemma 9 *Let $691 \mid A(p^\alpha)$ for $\alpha \geq 2$. Let $q \mid A(p^\alpha)$ with $q > p^\alpha$. Then $\{\sum_{k=0}^{q-1} ka_{i,k} \bmod q\}_{i=0}^{q-1}$ forms an additive group of order q modulo q.*

In particular for $i = 1$ from Lemma 9 and equation (21), we have for $\alpha \geq 2$

$$B(p^\alpha) = 691 \sum_{j=1}^{p^\alpha - 1} \sigma_5(j)\sigma_5(p^\alpha - j) \equiv \sum_{k=0}^{q-1} k a_{1,k} \not\equiv 0 \mod q. \tag{50}$$

Equation (50) implies $q \nmid B(p^\alpha)$ and hence $A(p^\alpha) \neq B(p^\alpha)$ and $\tau(p^\alpha) = (A(p^\alpha) - B(p^\alpha))/3 \neq 0$ by the unique factorization theorem. If $691 \nmid A(p^\alpha)$, since $691 \mid B(p^\alpha)$ from equation (8), we then trivially have $A(p^\alpha) \neq B(p^\alpha)$ and $\tau(p^\alpha) = (A(p^\alpha) - B(p^\alpha))/3 \neq 0$ via the unique factorization theorem in this case too. We thus have:

Theorem 10 $\tau(p^\alpha) \neq 0$ *for each* $\alpha \geq 2$.

Finally we show that $\tau(n) \neq 0$ for any positive integer n.

Theorem 11 *(Lehmer's Conjecture)* $\tau(n) \neq 0$ *for each* $n \geq 1$.

Proof. Since $\tau(1) = 1$, it suffices to prove the theorem when n is composite from Theorem 6 and Theorem 10. Write

$$n = p_0^{s_0} p_1^{s_1} \dots p_u^{s_u},\ p_0 := 2,\ s_0 \geq 0,\ s_j \geq 1,\ 1 \leq j \leq u.$$

Since $\tau(n)$ is multiplicative, $A(n) - B(n)$ is also multiplicative ([1 : 92 − 93], [2 : 52 − 53], [4 : 122], [5], [6]). Thus

$$\begin{array}{rcl} \tau(n) & = & \prod_{j=0}^{u} \tau(p_j^{s_j}) \\ & = & \prod_{j=0}^{u} \frac{1}{3}(A(p_j^{s_j}) - B(p_j^{s_j})) \\ & = & \frac{1}{3^{(1)+u}} \prod_{j=0}^{u} (A(p_j^{s_j}) - B(p_j^{s_j})) \\ & \neq & 0. \end{array} \tag{51}$$

In equation (51), the denominator $3^{(1)+u}$ equals either 3^{1+u} or 3^u depending on $s_0 \geq 1$ or $s_0 = 0$, respectively. Now for each $j = 0, 1, \dots, u$, $A(p_j^{s_j})$ either has factor 691 or not. If $691 \nmid A(p_j^{s_j})$, then since $B(p_j^{s_j})$ has factor 691 from equation (8), we trivially have $A(p_j^{s_j}) - B(p_j^{s_j}) \neq 0$ via the unique factorization theorem. If $691 \mid A(p_j^{s_j})$, then by Theorem 6 or Theorem 10, we also have:

$$A(p_j^{s_j}) - B(p_j^{s_j}) \neq 0, \quad j = 0, 1, \ldots, u.$$

In summary we have for each factor $p_j^{s_j}$ $(0 \leq j \leq u)$ of n:

$$A(p_j^{s_j}) - B(p_j^{s_j}) \neq 0 \text{ for each j = 0,1,...,u.} \tag{52}$$

Substitution of equation (52) into equation (51) completes the proof.

Suppose for each $\alpha \geq 1$,

$$A(p^\alpha) \equiv 0 \mod 691. \tag{53}$$

Equation (53) is equivalent to:

$$p^{(\alpha+1)} \equiv 1 \mod 691 \text{ and } (p-1, \ 691) = 1. \tag{54}$$

Equation (54) implies the following periodicity theorem modulo 691:

Theorem 12 *(periodicity modulo 691) Suppose $691 \mid A(p^\alpha)$ for $\alpha \geq 1$. Then we have:*

$$A(p^{\alpha+k(\alpha+1)}) \equiv 0 \mod 691, \ k = 0, 1, 2, \ldots$$

The values of α satisfying the periodicity of $A(p^\alpha) \equiv 0 \bmod 691$ for each $\alpha \geq 1$ has gaps in view of equation (54) and Fermat's little theorem, namely $A(p^\alpha) \not\equiv 0 \bmod 691$ if and only if the factors of $\alpha+1$ do not divide $690 = 2.3.5.23$. Thus $A(p^\alpha) \not\equiv 0 \bmod 691$ for α in the following set S of numbers:

$$S := \{6, 10, 12, 16, 18, 28, 30, 36, 40, 42, 46, 48, 52, 58, \dots\}$$

Needless to say $A(p^\alpha) \neq B(p^\alpha)$ and hence $\tau(p^\alpha) \neq 0$ for each $\alpha \in S$ by equation (8) with the aid of the unique factorization theorem.

Remark 13 *If $q \mid A(p^\alpha)$, $\alpha \geq 1$ with $q < p^\alpha$, as long as $\{\sum_{k=0}^{q-1} k a_{i,k} \bmod q\}_{i=0}^{q-1}$ forms an additive group of order q modulo q, then $q \nmid B(p^\alpha)$ by Lemma 4 or Lemma 9. It follows that $A(p^\alpha) \neq B(p^\alpha)$ and hence $\tau(p^\alpha) = (A(p^\alpha) - B(p^\alpha))/3 \neq 0$ in this case too. For $691 \mid A(p)$, computer simulation reveals $A(p)$ has at least one odd prime factor $q \neq 691$, $q \mid A(p)$ with $q < p$ for which $q \nmid B(p)$ for each prime $p \leq 1100000$ except $p = 186569, 290219, 464351, 671651$. Let $691 \mid A(p)$ and let $A_1(p)$ be the product of prime divisors $q \mid A(p)$ for which $q < p$ with their respective powers and $A_2(p)$ the product of prime divisors $q \mid A(p)$ for which $q > p$ with their respective powers. Computer simulation shows $C_1 p^2 < A_1(p) < C_2 p^5$ and $C_3 p^6 < A_2(p) < C_4 p^{10}$ with absolute constants $C_1, C_2, C_3, C_4 < 1$ for primes $p \leq 1100000$.*

In Table 1, we list primes p such that both 691 and q divide $A(p)$ with $q > p$ and the cardinality $\mid S_{1,i} \mid$ $(1 \leq i \leq 5)$, thereby confirming inequality (33) with $q_0 \leq 4$. Notice that in Table 1, each prime p with the associated prime $q \mid A(p)$ with $q > p$, satisfies equations (25) and (26). Computer simulation reveals that the majority of respective relatively large odd prime factors less than p of both $A(p)$ and $B(p)$ are distinct. Likewise an overwhelming majority of common odd prime factors of both $A(p)$ and $B(p)$ for which $691 \mid A(p)$ are relatively small apart from 691 thereby confirming Corollary 5. In Table 2, we list primes $p \leq 3000000$ such that $691 \mid A(p)$ and the odd prime factors of $(A(p),\ B(p))$ are ≥ 11.

Acknowledgment. We are deeply grateful to the referee who pointed out the obscurity of the additive group structure of $\{\sum_{k=0}^{q-1} ka_{i,k} \bmod q\}_{i=0}^{q-1}$ in our original manuscript. We are thankful to S. Durbha, J. Gerver, H. Li and M. Nerurkar for many lively discussions.

Table 1

p	q	$\mid S_{1,0} \mid$	$\mid S_{1,1} \mid$	$\mid S_{1,2} \mid$	$\mid S_{1,3} \mid$	$\mid S_{1,4} \mid$	$\mid S_{1,5} \mid$
8291	216113	212008	4065	40	0	0	0
29021	1357091	1342657	14358	76	0	0	0
30403	1283839	1268731	15015	93	0	0	0
34549	789673	772578	16918	175	2	0	0
51133	112919	89995	20474	2267	174	9	0
53897	371549	345582	25014	925	28	0	0
96739	392957	347376	42917	2543	118	3	0

Table 2

p	$(A(p),\ B(p))$
547271	$2.3.11.691$
610843	$2.3.17.691$
988129	$2.3.5.13.691$
1112509	$2.3.5.23.691$
1336393	$2.3.101.691$
1405493	$2.3.113.691$
1716463	$2.3^2.23.691$
1875373	$2.23.691$
1940327	$2^2.3^2.13.691$
2126897	$2.3^3.19.691$
2128279	$2^2.5.11.691$
2161447	$2^2.23.691$
2198761	$2.43.691$
2447521	$2.23.691$
2479307	$2.23.691$
2538733	$2.11.691$
2542879	$2^4.3.5.23.691$
2956097	$2.23.691$

References

1. Apostol, Tom Modular Functions And Dirichlet Series, Springer (1997).

2. Berndt, B., Number Theory in the Spirit of Ramanujan, AMS (2006).

3. Iwaniec, H., Topics in Classical Automorphic Forms, AMS (1997), $13-22$.

4. Koblitz, N., Int. to Elliptic Curves And Modular Functions, Springer (1993), $108-123$.

5. Lehmer, D.H., Ramanujan's Function $\tau(n)$, Duke Math. J. 10 (1943), $483-492$.

6. Lehmer, D.H., The Vanishing of Ramanujan's Function $\tau(n)$, Duke Math. J. 14 (1947), $429-433$.

7. Lehmer, D.H., Note on the Distribution of Ramanujan's τ Function, Math. Comp.24 (1970), $741-743$.

8. Hua, L.K., Int. to Number Theory, Springer (1982) $204-216$.

Rutgers University-Camden

Camden, NJ 08102 USA