THE VANISHING OF RAMANUJAN'S FUNCTION $\tau(n)$

By D. H. Lehmer

The numerical function $\tau(n)$ of Ramanujan defined by

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

has been the subject of numerous investigations since Ramanujan in 1916 first discovered its remarkable properties (see [4; Chapters 9 and 10]). This function is generated by the 24-th and 8-th powers respectively of the lacunary power series of Euler and Jacobi

$$(2) \qquad \prod_{\nu=1}^{\infty} (1 - x^{\nu}) = \sum_{r=-\infty}^{\infty} (-1)^r x^{(3r^2+r)/2} ,$$

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

and it is natural to ask whether $\tau(n) = 0$ for any $n > 0$. The recent discovery of D. F. Ferguson (communicated by a letter of August 3, 1946) that the 53rd coefficient of the 15-th power of (2) is zero adds to the interest in the question of the possible vanishing of $\tau(n)$. Tables of $\tau(n)$ given in [6], which extend to $n = 300$ show no case of $\tau(n) = 0$. In this paper we show that $\tau(n) \neq 0$ for $n < 3316799$. Whether $\tau(3316799) = 0$ or not we cannot say. The methods of this paper would seem to be incapable of establishing that $\tau(n)$ is never zero. That such a simple question about a well-known function is apparently difficult to answer is due to the fact that no practicable formula for $\tau(p)$ (p a prime) has ever been discovered.

1. In our discussion we use the following formulas and congruence properties. The numbers in square brackets indicate items in the bibliography where the corresponding results are proved.

$$(3) \qquad \tau(m)\tau(n) = \tau(mn) \qquad (m, n \text{ coprime}) \qquad [7], [4]$$

$$(4) \qquad \tau(p^{\alpha}) = \tau(p)\tau(p^{\alpha-1}) - p^{11}\tau(p^{\alpha-2}) \qquad (p \text{ a prime}) \qquad [7], [4] \quad \text{A278577}$$

$$(5) \qquad \tau(p^{\alpha}) = p^{11/2} \csc \theta_p \sin (\alpha + 1)\theta_p \qquad [7], [4]$$

where $2 \cos \theta_p = \tau(p)p^{-11/2}$. If we use $\sigma_k(n)$ to denote the sum of the k-th powers of the divisors of n, we have

$$\tau(p) = \text{A76847}$$

(6) $\tau(n) \equiv \sigma_3(n)$ (mod 32)   (n odd)   [1]

(7) $\tau(n) \equiv \sigma_1(n)$ (mod 3)   ($n \not\equiv 0$ (mod 3))   [8], [3]

(8) $\tau(n) \equiv n\sigma_9(n)$ (mod 25)   [1]

(9) $\tau(n) \equiv n\sigma_3(n)$ (mod 7)   [2], [11], [8]

(10) $\tau(n) \equiv \sigma_{11}(n)$ (mod 691)   [9], [5].

To this list of congruences we add the following theorem for the modulus 23.

THEOREM 1.   *Let n be any integer and let $p_1, p_2, \cdots, p_t$ be those prime factors (if any) of n which are not of the form $u^2 + 23v^2$, but are quadratic residues of 23. Define n_1 by*

$$n = n_1 \prod_{i=1}^{t} p_i^{\alpha_i},$$

where α_i is the exponent of the highest power of p_i dividing n.   Then

$$\tau(n) \equiv \sigma_{11}(n_1) 2^t 3^{-t/2} \prod_{i=1}^{t} \sin \frac{2\pi}{3} (1 + \alpha_i) \qquad \text{(mod 23)}.$$

(A list of such primes $p_i < 1000$ will be found in [11], table II.)   Theorem 1 is equivalent to a theorem given by Wilton [11], who proved it by ideal theory. An elementary proof is sketched in §2 of the present paper.

THEOREM 2.   *Let n_0 be the least value of n for which $\tau(n) = 0$.   Then n_0 is a prime.*

Proof.   It is clear that n_0 is a power of a prime, for otherwise we could break n_0 into the product of two relatively prime factors each less than n_0 and apply (3) to discover an even smaller value of n than n_0 for which $\tau(n) = 0$.   Hence we may set $n_0 = p^\alpha$ where p is a prime.   We have to show that $\alpha = 1$.   Assuming the contrary, namely $\alpha > 1$, so that $\tau(p) \neq 0$, we may write (5) in the form

$$\tau(p^\alpha) = 0 = p^{11/2} \csc \theta_p \sin (\alpha + 1)\theta_p.$$

This shows that θ_p is a real number of the form

$$\theta_p = \pi k/(1 + \alpha),$$

where k is an integer.   Now the number

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

being twice the cosine of a rational multiple of 2π, is an algebraic integer.   On the other hand z is a root of the obviously irreducible quadratic

(12) $p^{11} z^2 - \tau^2(p) = 0.$

Hence p^{11} divides $\tau^2(p)$, or in other words z^2 is a positive non-square integer. By (11), $z^2 \leq 4$. Therefore $z^2 = 2$ or 3. In the former case (12) becomes

(13) $$\tau^2(p) = 2p^{11}.$$

The right member is a square only if $p = 2$. Hence (13) becomes

$$\tau(2) = \pm 2^6.$$

Similarly if $z^2 = 3$,

$$\tau(3) = \pm 3^6.$$

Both these conditions are false since $\tau(2) = -24$, and $\tau(3) = 252$. This completes the proof of Theorem 2.

If in formulas (6) to (10) we set $n = p$, and suppose that p is a prime greater than 7 for which $\tau(p) = 0$, we obtain the following congruential conditions on p:

$$0 \equiv 1 + p^3 \qquad \text{(mod 32)},$$

$$0 \equiv 1 + p \qquad \text{(mod 3)},$$

$$0 \equiv p(1 + p^9) \qquad \text{(mod 25)},$$

$$0 \equiv p(1 + p^3) \qquad \text{(mod 7)},$$

$$0 \equiv 1 + p^{11} \qquad \text{(mod 691)}.$$

The first three conditions imply

$$p \equiv -1 \qquad \text{(mod 2400)}.$$

and, since 11 is prime to 690,

$$p \equiv -1 \qquad \text{(mod 691)}.$$

The congruence modulo 7 implies that p is a quadratic non-residue of 7, that is

$$p \equiv 3, 5, 6 \qquad \text{(mod 7)}.$$

Combining these conditions we find

$$p \equiv 3316799, 4975199, 11608799 \qquad \text{(mod 11608800)}.$$

The following 5 numbers are the only numbers belonging to these forms under 20 millions:

$$3316799, \ 4975199, \ 11608799, \ 14925599, \ 16583999.$$

If we now apply Theorem 1 with n a prime p we find that $\tau(p)$ is divisible by 23 if and only if

$$1 + p^{11} \equiv 0 \qquad \text{(mod 23)}.$$

Hence p is a quadratic non-residue of 23 and thus belongs to one of the forms

$$p = 23m + 5, 7, 10, 11, 14, 15, 17, 19, 20, 21 \text{ or } 22.$$

Applying this to the above set of 5 numbers we exclude all but the first and last, but of these only $p = 3316799$ is a prime.

With the present state of our knowledge about the function $\tau(n)$ there seems to be no practical way of deciding whether $\tau(3316799)$ vanishes or not.

2. *Proof of Theorem* 1. This theorem is a simple consequence of (3), (4) and the following

LEMMA. *Let p be any prime. Then $\tau(p)$ is congruent, modulo 23, to*

0 *if p is a quadratic non-residue of* 23,

1 *if $p = 23$,*

2 *if p is of the form $u^2 + 23v^2$ ($u \neq 0$),*

-1 *otherwise.*

In fact it follows from (3) that

$$\tau(p^\alpha) \equiv \tau(p)\tau(p^{\alpha-1}) - (p/23)\tau(p^{\alpha-2}) \qquad \text{(mod 23)}.$$

In the four categories of p mentioned in the lemma we have respectively

$$\tau(p^\alpha) \equiv \tau(p^{\alpha-2}) \equiv \tfrac{1}{2}(1 + (-1)^\alpha) \equiv \sum_{\nu=0}^{\alpha} (-1)^\nu \equiv \sum_{\nu=0}^{\alpha} p^{11\nu} \equiv \sigma_{11}(p^\alpha) \quad \text{(mod 23)},$$

$$\tau(p^\alpha) \equiv \tau(p)\tau(p^{\alpha-1}) \equiv 1 \equiv \sigma_{11}(p^\alpha) \qquad \text{(mod 23)},$$

$$\tau(p^\alpha) \equiv 2\tau(p^{\alpha-1}) - \tau(p^{\alpha-2}) \equiv 1 + \alpha \equiv \sum_{\nu=0}^{\alpha} p^{11\nu} \equiv \sigma_{11}(p^\alpha) \qquad \text{(mod 23)},$$

$$\tau(p^\alpha) \equiv -\tau(p^{\alpha-1}) - \tau(p^{\alpha-2}) \equiv \frac{\sin(1+\alpha)2\pi/3}{\sin 2\pi/3} \qquad \text{(mod 23)}.$$

By (3) it follows that if

$$n = n_1 \prod_{i=1}^{t} p_i^{\alpha_i} = \prod_{i=1}^{t_1} q_i^{\beta_i} \prod_{i=1}^{t} p_i^{\alpha_i},$$

where $p_1, \cdots, p_t$ are primes of the fourth category, then

$$\tau(n) = \prod_{i=1}^{t_1} \tau(q_i^{\beta_i}) \prod_{i=1}^{t} \tau(p_i^{\alpha_i})$$

$$\equiv \prod_{i=1}^{t_1} \sigma_{11}(q_i^{\alpha_i})(\csc 2\pi/3)^t \prod_{i=1}^{t} \sin(1+\alpha_i)2\pi/3$$

$$\equiv \sigma_{11}(n_1)2^t 3^{-t/2} \prod_{i=1}^{t} \sin(1+\alpha_i)2\pi/3 \qquad \text{(mod 23)}.$$

It remains to prove the lemma.

A fairly straightforward proof of the lemma by elementary methods, though rather lengthy, may be made along the following lines.

The lemma may be verified for $p = 2$ and 3. Hence consider $p = 6m \pm 1$. Since

$$(1 - x^{\nu})^{23} = 1 - x^{23\nu} + 23P,$$

where P is a polynomial with integer coefficients it follows from (2) that

(14) $$\tau(p) \equiv \sum (-1)^{r+s} \qquad (\mathrm{mod}\ 23)$$

where the sum extends over all solutions (r, s) of

(15) $$24p = (6r \pm 1)^2 + 23(6s \pm 1)^2.$$

In case p is a quadratic non-residue of 23, (15) has no solutions and the sum in (14) is vacuous. Other primes p are representable by either of the forms

$$x^2 + 23y^2, \qquad 3x^2 + 2xy + 8y^2$$

in essentially one way. In these respective cases (15) contributes two solutions with $r + s$ even, and one solution with $r + s$ odd. In the former case the two solutions are distinct except when $p = 23$.

Bibliography

1. R. P. Bambah, *Two congruence properties of Ramanujan's function $\tau(n)$*, London Mathematical Society Journal, vol. 21(1946), pp. 91–93.
2. H. Gupta, *A congruence property of $\tau(n)$*, Indian Academy of Sciences, Section A, vol. 24(1946), pp. 441–442.
3. H. Gupta, *A congruence relation between $\tau(n)$ and $\sigma(n)$*, Journal of the Indian Mathematical Society, vol. 9(1945), pp. 59–60.
4. G. H. Hardy, *Ramanujan*, Cambridge University Press, 1940.
5. D. H. Lehmer, *Properties of the coefficients of the modular invariant $J(\tau)$*, American Journal of Mathematics, vol. 64(1942), pp. 488–502.
6. D. H. Lehmer, *Ramanujan's function $\tau(n)$*, this Journal, vol. 10(1943), pp. 483–492.
7. L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions*, Proceedings of the Cambridge Philosophical Society, vol. 19(1920), pp. 117–124.
8. K. G. Ramanathan, *Congruence properties of Ramanujan's function $\tau(n)$* (II), Journal of the Indian Mathematical Society, vol. 9(1945), pp. 55–59.
9. S. Ramanujan, *On certain arithmetical functions*, Transactions of the Cambridge Philosophical Society, vol. 22(1916), pp. 159–184; Collected Papers of Srinivasa Ramanujan, Cambridge University Press, 1927.
10. S. Ramanujan, *Congruence properties of partitions*, Proceedings of the London Mathematical Society (2), Records for 13 March, 1919, vol. 18(1919), pp. xix-xx.
11. J. R. Wilton, *Congruence properties of Ramanujan's function $\tau(n)$*, Proceedings of the London Mathematical Society (2), vol. 31(1930), pp. 1–10.

University of California.