The Primality of Ramanujan's Tau-Function

Author(s): D. H. Lehmer
Source: *The American Mathematical Monthly*, Vol. 72, No. 2, Part 2: Computers and Computing (Feb., 1965), pp. 15-18
Published by: Taylor & Francis, Ltd. on behalf of the Mathematical Association of America
Stable URL: https://www.jstor.org/stable/2313305
Accessed: 31-07-2025 05:58 UTC

THE PRIMALITY OF RAMANUJAN'S TAU-FUNCTION

D. H. LEHMER, University of California, Berkeley

Introduction. The function $\tau(n)$ introduced by Ramanujan in 1916 [1] as a natural outgrowth of the functions $\sigma_k(n)$, the sum of the kth powers of the divisors of n, has been the subject of numerous investigations ever since. It is defined most simply as the coefficient of X^n in the expansion of the product

$$X\prod_{m=1}^{\infty}(1-X^m)^{24}=\sum_{n=1}^{\infty}\tau(n)X^n=X-24X^2+252X^3+\cdots.$$

Although a number of remarkable properties of $\tau(n)$ have been established, some of which are cited below, there remains a number of unsolved questions about $\tau(n)$; for example: What is the exact order of magnitude of $\tau(n)$ (see [2])? Is $\tau(n)=0$ for some $n>0$ (see [3])? In this note we address ourselves to the question: Is $\tau(n)$ ever a prime? We answer this question by

THEOREM A. *The integer $\tau(n)$ is composite for $2\leqq n\leqq 63000$, but*

$$\tau(63001)=80561663527802406257321747$$

is a prime number.

Since published tables of $\tau(n)$, [4], extend to $n=1000$ and unpublished tables to $n=10000$, [5], it is clear that to prove Theorem A requires the use of some of the known properties of $\tau(n)$, namely the formulas and congruence properties listed below. Numbers in square brackets give references to papers where these results are established. In what follows p always designates a prime.

Required Properties.

(1) If $(a,b)=1$, then $\tau(ab)=\tau(a)\tau(b)$. [6]

(2) $\tau(p^{\alpha+1})=\tau(p)\tau(p^{\alpha})-p^{11}\tau(p^{\alpha-1})$, $(\alpha>0)$. [6]

As an immediate consequence of (1) and (2)

(3) If $p\mid\tau(p)$ then $p\mid\tau(np)$, $(n>0)$.

(4) If n is odd $\tau(n)\equiv\sigma(n)\pmod 8$. [7]

Setting $p=2$ in (3) and using (4) we easily derive

(5) $\tau(n)$ is odd if and only if n is an odd square.

(6) If n is odd, $\tau(n)\equiv\sigma_3(n)\pmod{32}$. [8]

(7) If $(n,3)=1$, $\tau(n)\equiv\sigma(n)\pmod 3$. [9]

(8) If $3p=u^2+23v^2$, $\tau(p)\equiv-1\pmod{23}$. [10], [3]

(9) $\tau(n)\equiv\sigma_{11}(n)\pmod{691}$. [2], [11]

Proof of Theorem A. We begin by assuming there exists a least integer $n_0\leqq 63000$ for which $\tau(n_0)$ is a prime. If n_0 is not a power of a prime then $n_0=ab$

with $1<a<b<n_0$ and $(a, b)=1$. By (1), either $\tau(a)$ or $\tau(b)$ is a prime, contrary to the minimal property of n_0; hence

$$n_0 = p^\alpha \qquad (\alpha \geqq 1). \tag{10}$$

We now separate two cases:

Case I. $|\tau(n_0)|=2$.

In this case it is clear that $p\neq 2$ because $\tau(2)=-24$ is a multiple of 8 and so, by (2), is $\tau(2^\alpha)$. Hence n_0 is odd but not an odd square, by (5). Therefore $n_0=p^{2\beta+1}$, $(p>2, \beta\geqq 0)$. Writing (2) in the form

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

we see, by induction on k, that $\tau(p)$ divides $\tau(p^{2\beta+1})=\pm 2$. Now $|\tau(p)|=1$ would contradict (5). Hence $|\tau(p)|=2$. Because n_0 is minimal this implies $n_0=p$. Now the case $\tau(p)=-2$ is impossible by (7). In fact, $p\neq 3$ because $\tau(3)=252\neq -2$. Hence (7) would give

$$-2 = \tau(p) \equiv \sigma(p) = 1 + p \pmod 3.$$

This implies $p=3$, a contradiction. Hence we are left with

$$\tau(p) = 2. \tag{12}$$

To complete Case I we have to show the impossibility of (12) with $p<63000$. This is easily done by using the congruences (6) and (9). In fact, (6) gives

$$2 = \tau(p) \equiv 1 + p^3 \pmod{32}$$

which implies

$$p \equiv p^{1+2\cdot 16} \equiv p^{33} \equiv (p^3)^{11} \equiv 1^{11} \equiv 1 \pmod{32}. \tag{13}$$

Also (9) gives $2=\tau(p)\equiv 1+p^{11} \pmod{691}$ which implies

$$p \equiv p^{1+4\cdot 690} \equiv p^{2761} \equiv (p^{11})^{251} \equiv 1 \pmod{691}.$$

Combining this with (13) gives $p=22112x+1$. Since 22113 and 44225 are not primes, $p>63000$. This disposes of Case I.

Case II. $|\tau(n_0)|>2$.

Since $|\tau(n_0)|$ is now an odd prime, (5) and (10) give $n_0=p^{2\beta}(p>2, \beta\geqq 1)$.

We show next that p does not divide $\tau(p)$, for otherwise by (2) p^2 would divide $\tau(p^2), \tau(p^3), \cdots$, so that $\tau(n_0)=\tau(p^{2\beta})$ could not be a prime. Since $p|\tau(p)$ for $p=3, 5, 7$ it follows that $p\geqq 11$. Since

$$63000 < 83521 = 17^4 < 1771561 = 11^6,$$

the case of $\beta>1$ reduces to the consideration of

$$\tau(11^4) = -815446775566671275778 95$$

and

$$\tau(13^4) = 152868044248899843598 4621.$$

Neither one of these numbers is a prime, the latter being divisible by 25741.

There remains the case $n_0=p^2$, $11\leqq p<251$. We see from (7) that if $p=6x+1$ then

$$\tau(p^2)\equiv\sigma(p^2)\equiv 1+p+p^2\equiv 0 \pmod 3.$$

This would imply $\tau(p^2)=\pm 3$. We would infer from (9) that

$$\pm 3\equiv\sigma_{11}(p^2)\equiv 1+p^{11}+p^{22} \pmod{691}.$$

Solving these two congruences gives the solutions $p\equiv 1, 21, 33, 348 \pmod{691}$. This disagrees with the assumption that p is a prime less than 251. Hence $p\neq 6x+1$.

Next suppose that

$$3p = u^2+23v^2. \tag{14}$$

Then

$$p^{11}\equiv\left(\frac{p}{23}\right)\equiv\left(\frac{3p}{23}\right)=\left(\frac{u^2}{23}\right)\equiv 1 \pmod{23}$$

so that (2) and (8) give $\tau(p^2)=(\tau(p))^2-p^{11}\equiv(-1)^2-1\equiv 0 \pmod{23}$. This would require $\tau(p^2)=\pm 23$. But then (9) would give

$$\pm 23\equiv\sigma_{11}(p^2)\equiv 1+p^{11}+p^{22} \pmod{691},$$

which has solutions $p\equiv 92, 340, 410, 432 \pmod{691}$ contrary to $p<251$. Hence the prime p is of the form $6x-1$ but not of the form (14). The fifteen such primes <251 are the arguments of Table 1. For each argument, we give one or more small factors q of $\tau(p^2)$ to show that $\tau(p^2)$ is not a prime. In those cases in which only one q is given $|\tau(p^2)|\neq q$ (see [**12**]).

TABLE I

p	q	p	q
17	842087·15936629	113	31
23	11·13	137	11
53	17	149	49139
59	137	167	137
83	61·71	173	89·1567·38833
89	33107	191	2357·308117
101	8731	227	51869
107	43·211		

Test for Primality of $\tau(251^2)$. To complete the proof of Theorem A we must establish the primality of $\tau(63001)$. The standard procedure for testing numbers N as large as this is to apply some valid converse of Fermat's theorem [**13**]. These require the knowledge of some large prime factor of $N-1$. In our case

$$N-1 = 2\cdot 397\cdot 1014630523020181439009 09,$$

where the large factor was found to be composite but rather difficult to decompose into its prime factors, but the factorization of $N+1$ is relatively easy, namely

$$N + 1 = 2^2 \cdot 3^2 \cdot 7 \cdot 23 \cdot 29 \cdot 1249 \cdot 1767401 \cdot 217122342553.$$

Hence the following Fibonacci type test was used [**14**].

THEOREM. *Let* $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$, *be the sequence of Fibonacci. If* F_n *is divisible by* N *for* $n = N+1$ *but not for* $n = (N+1)/p$, *where* p *ranges over the prime factors of* $N+1$, *then* N *is a prime.*

Although this theorem speaks of Fibonacci numbers that are incredibly large for $N = \tau(63001)$, one does not deal with such large numbers themselves but only their remainders on division by N. Furthermore, one does not use the defining recurrence to compute F_n modulo N but instead skips over all but O (log N) values of n by a duplication formula. All told, the application of the theorem represents an effort proportional to only log N. For $N = \tau(63001)$ the hypothesis of the theorem was verified in about twenty seconds. Hence $\tau(63001)$ is indeed the first prime value of $\tau(n)$.

References

1. S. Ramanujan, On certain arithmetical functions, Trans. Camb. Phil. Soc., 22 (1916) 159–184.
2. G. H. Hardy, Ramanujan, Cambridge, Ch. X (1940) 161–185.
3. D. H. Lehmer, The vanishing of Ramanujan's function $\tau(n)$, Duke Math. J., 14 (1947) 429–433.
4. G. N. Watson, A table of Ramanujan's function $\tau(n)$, Proc. London Math Soc., 51 (1949) 1–13.
5. D. H. Lehmer, Manuscript Table of $\tau(n)$; $n = 1$ (1) 10000.
6. L. J. Mordell, On Mr. Ramanujan's empirical expansions of modular functions, Proc. Camb. Phil. Soc., 19 (1920) 117–124.
7. H. Gupta, Congruence properties of $\tau(n)$, Proc. Benares Math. Soc., 5 (1943) 17–22.
8. R. P. Bambah, Two congruence properties of Ramanujan's function $\tau(n)$, J. London Math. Soc., 21 (1946) 91–93.
9. H. Gupta, A congruence relation between $\tau(n)$ and $\sigma(n)$, J. Indian Math. Soc., 9 (1945) 59–60.
10. J. R. Wilton, Congruence properties of Ramanujan's function $\tau(n)$, Proc. London Math. Soc., 31 (1930) 1–10.
11. D. H. Lehmer, Properties of the coefficients of the modular invariant $J(\tau)$, Amer. J. Math., 64 (1942) 488–502.
12. These factors were discovered by John Brillhart using the IBM 7090 at Stanford University's Department of Computer Sciences under grant No. NSF-GP948.
13. D. H. Lehmer, Tests for primality by the converse of Fermat's theorem, Bull. Amer. Math. Soc., 33 (1927) 327–340.
14. A brief discussion of such tests will appear elsewhere.