PAPERS

PUBLISHED IN THE

PROCEEDINGS OF THE LONDON MATHEMATICAL SOCIETY

CONGRUENCE PROPERTIES OF RAMANUJAN'S FUNCTION $\tau(n)$

By J. R. WILTON.

[Received 19 November, 1928.—Read 13 December, 1928.]

1. The function $\tau(n)$ is the coefficient of x^n in the expansion of the modular function

$$f(x) = x\{(1-x)(1-x^2)(1-x^3)\ldots\}^{24} = \Sigma\,\tau(n)\,x^n.$$

It was stated by Ramanujan[*] that

$$(1.1)\qquad \tau(5n) \equiv 0 \pmod 5,$$

$$(1.2)\qquad \tau(7n) \equiv \tau(7n+3) \equiv \tau(7n+5) \equiv \tau(7n+6) \equiv 0 \pmod 7,$$

and that

$$(1.3)\qquad \tau(23n+\nu) \equiv 0 \pmod{23},$$

if ν is any one of the quadratic non-residues of 23, namely,

$$5,\ 7,\ 10,\ 11,\ 14,\ 15,\ 17,\ 19,\ 20,\ 21,\ 22.$$

Of these relations (1.1) is a consequence[†] of the result that

$$\tau(5) = 4830 \equiv 0 \pmod 5,$$

and $\tau(7n) \equiv 0 \pmod 7$ is a consequence of

$$\tau(7) = -16744 \equiv 0 \pmod 7;$$

and the remaining congruences have been proved by Mordell[‡].

[*] *Proc. London Math. Soc.* (2), 18 (1920), *Records* for 13th March, 1919. Ramanujan's *Collected papers*, No. 28.

[†] The formulae (5.1) and (5.2) show this immediately.

[‡] L. J. Mordell, *Proc. London Math. Soc.* (2), 20 (1922), 408-416 (413). In the last two lines of p. 413 for "2, 4, 6" read "3, 5, 6". The relation (1.1) was proved by H. B. C. Darling, *Proc. London Math. Soc.* (2), 19 (1921), 350-372, Equation (98).

In this note I give straightforward algebraic proofs of (1 . 2) and (1 . 3), and I have little doubt that the method is that by which Ramanujan established all these congruences*. I prove, in fact, a good deal more than (1 . 2) and (1 . 3). In the case of the modulus 23 the results obtained may be summarised in the following theorem:

Let p, q, r typify, respectively, (p) prime quadratic non-residues of 23, (q) *prime quadratic residues of* 23 *not expressible in the form* a^2+23b^2, *and* (r) *primes expressible in the form* a^2+23b^2; *let*

$$n = 23^h \prod_p p^k \prod_q q^l \prod_r r^m.$$

Then $\tau(n) \equiv 0 \pmod{23}$ *if any* k *is odd, or if any* $l \equiv 2 \pmod 3$, *or if any* $m \equiv 22 \pmod{23}$. *If none of these conditions is satisfied*

$$\tau(n) \equiv (-)^\lambda \prod (m+1) \pmod{23},$$

where λ *is the number of the indices* l *which are congruent to* 1 (mod 3).

The only point at which the theorem is incomplete is that there seems to be no simple rule by means of which to distinguish between the primes q and r. In Table III are given the twenty-five primes $r < 1000$ (together with the two which lie between 3800 and 3900).

Proof of (1 . 2)†.

2. Let

$$\psi(x) = \{(1-x)(1-x^2)(1-x^3)\dots\}^3$$
$$= 1-3x+5x^3-7x^6+9x^{10}-\dots,$$

* Cf. the posthumous paper, "Congruence properties of partitions", *Math. Zeitschrift*, 9 (1921), 147-153. *Collected papers*, No. 30.

† A Referee remarks "The method employed can probably be extended to find congruence properties among the coefficients of the terms of the various positive integral powers of a power series (of certain types) with integral coefficients, though the number of moduli which can be used for any given power of the series appears to be very limited." In agreement with this remark it may be observed that, if

$$\Sigma \tau_k(n) x^n = \{\Sigma \tau(n) x^n\}^k,$$

the congruences

$$\tau_2(n) \pmod{47},\quad \tau_3(n) \pmod{23},\quad \tau_3(n) \pmod{71},\quad \tau_4(n) \pmod{31},$$
$$\tau_6(n) \pmod{47},\quad \tau_7(n) \pmod{167},\quad \tau_8(n) \pmod{191},\quad \tau_9(n) \pmod{71},$$
$$\tau_{10}(n) \pmod{79},\quad \tau_{10}(n) \pmod{239},\ \text{etc.},\quad \tau_{\frac12}(n) \pmod{11},\ \text{etc.},$$

where $\tau_{\frac12}(x)$ is defined by $\Sigma \tau_{\frac12}(n) x^{2n-1} = \{f(x^2)\}^{\frac12}$, have very remarkable properties which may be established by the method of this paper. It is, moreover, evident that, in the case of any power series with integral coefficients, the method will determine, among the coefficients of the $(p+1)$-th power of the series (p prime), congruence relations (mod p)—which may or may not be interesting.

then, since
$$\{\psi(x)\}^7-\psi(x^7)\equiv 0 \pmod 7,$$
we have
$$f(x) = x\{\psi(x)\}^8 \equiv x\psi(x)\,\psi(x^7) \pmod 7.$$
But
$$x\psi(x)\,\psi(x^7) = x\sum_0^\infty b_n x^n \sum_0^\infty b_n x^{7n} = \sum_1^\infty d_n x^n,$$
where
$$b_n = (-)^m(2m+1) \text{ if } n = \tfrac{1}{2}m(m+1),$$
and otherwise $b_n = 0$; and
$$d_n = b_{n-1}+b_1 b_{n-8}+b_2 b_{n-15}+\ldots+b_h b_{n-1-7h},$$
where $h = [(n-1)/7]$. Now let
$$n = 7k+l \quad (k \geqslant 0,\ n \geqslant 1);$$
then (i) if $l > 0$, $b_{n-1} = 0$ unless there are positive integers l and m such that
$$7k+l-1 = \tfrac{1}{2}m(m+1),$$
i.e.
$$(2m+1)^2 = 56k+8l-7 \equiv l \equiv n \pmod 7.$$
Hence $d_n = 0$ if n is a quadratic non-residue of 7.

(ii) If $l = 0$, we have $b_{7n-1} = 0$ unless
$$7n-1 = \tfrac{1}{2}m(m+1), \quad \textit{i.e.} \quad (2m+1)^2 = 56n-7,$$
in which case
$$b_{7n-1} = (-)^m(2m+1) \equiv 0 \pmod 7.$$
Hence
$$\tau(7n) \equiv d_{7n} \equiv 0 \pmod 7.$$
This completes the proof of (1.2).

A simple application of the method of § 4 will show that, when p is a prime quadratic residue of 7,
$$\tau(p) \equiv 2p \pmod 7;$$
and equations (5.1) and (5.2) may then be employed to prove the following theorem analogous to that stated in § 1 for modulus 23.

If p typifies prime quadratic non-residues of 7, *and q typifies prime quadratic residues of* 7, *and if*
$$n = 7^h \prod_p p^k \prod_q q^l,$$
then $\tau(n) \equiv 0 \pmod 7$ *if $h > 0$, or if any k is odd, or if any $l \equiv 6 \pmod 7$; in all other cases*
$$\tau(n) \equiv n\Pi(l+1) \pmod 7.$$

Proof of (1 . 3).

3. Let $\phi(x) = (1-x)(1-x^2)(1-x^3)\ldots$, then

$$(3\,.\,1)\qquad \phi(x) = 1-x-x^2+x^5+x^7-\ldots = 1+\sum_{n=1}^{\infty}(-)^n\left\{x^{\frac{1}{2}n(3n-1)}+x^{\frac{1}{2}n(3n+1)}\right\},$$

and, as in the case of modulus 7,

$$(3\,.\,2)\qquad f(x) = x\{\phi(x)\}^{24} \equiv x\phi(x)\,\phi(x^{23}) \pmod{23}.$$

But

$$x\phi(x)\,\phi(x^{23}) = x\sum_0^{\infty} a_n x^n \sum_0^{\infty} a_n x^{23n} = \sum_1^{\infty} c_n x^n,$$

where

$$(3\,.\,3)\qquad a_n = (-1)^m \quad \text{if} \quad n = \tfrac{1}{2}m(3m\pm 1),$$

and otherwise $a_n = 0$; and

$$(3\,.\,4)\qquad c_n = a_{n-1}+a_1 a_{n-24}+a_2 a_{n-47}+\ldots+a_h a_{n-1-23h},$$

where $h = [(n-1)/23]$. It follows from (3 . 2) that

$$\tau(n) \equiv c_n \pmod{23}.$$

Let $n = 23k+l$ ($k \geqslant 0$, $n \geqslant 1$); then $a_{n-1} = 0$ unless, for some positive integers l and m,

$$23k+l-1 = \tfrac{1}{2}m(3m\pm 1),$$

i.e.

$$36m^2 \pm 12m = 552k+24l-24,$$

i.e.

$$(6m\pm 1)^2 \equiv l \equiv n \pmod{23}.$$

Hence $c_n = 0$ if n is a quadratic non-residue of 23. This completes the proof of (1 . 3).

Determination of c_p.

4. When the prime p is a quadratic residue of 23, we have from (3 . 3) and (3 . 4)

$$(4\,.\,1)\qquad c_p = \Sigma\, a_{\frac{1}{2}m(3m\pm 1)}\, a_{p-1-23\{\frac{1}{2}m(3m\pm 1)\}} = \Sigma(-1)^{m+n},$$

summed over those values of m and n for which

$$p-1-23\left\{\tfrac{1}{2}m(3m\pm 1)\right\} = \tfrac{1}{2}n(3n\pm 1),$$

i.e.

$$(4\,.\,11)\qquad (6n\pm 1)^2+23(6m\pm 1)^2 = 24p,$$

so that the value of c_p depends upon the character of the integers u and v which satisfy the Diophantine equation

$$u^2+23v^2 = 24p. \tag{4.2}$$

Let ω denote $\sqrt{(-23)}$, then in the corpus $K(\omega)$ of algebraic numbers every prime p which is a quadratic residue of 23 splits into two prime ideal factors

$$\pi,\ \pi' = \left(p,\ \frac{2r+23\pm\omega}{2}\right),$$

where r is a solution of the congruence

$$(2r+23)^2 \equiv -23 \pmod{4p}. \tag{4.31}$$

Interchanging the two values of r simply interchanges π and π'.

In $K(\omega)$ there are three ideal classes*, the principal class typified by the unit ideal, and two classes which may be typified by the ideal prime factors of 2,

$$\pi_2 = (2,\ \tfrac{1}{2}+\tfrac{1}{2}\omega), \quad \pi_2' = (2,\ \tfrac{1}{2}-\tfrac{1}{2}\omega). \tag{4.32}$$

We shall also require the ideal prime factors of 3,

$$\pi_3 = (3,\ \tfrac{1}{2}-\tfrac{1}{2}\omega), \quad \pi_3' = (3,\ \tfrac{1}{2}+\tfrac{1}{2}\omega), \tag{4.33}$$

where the notation has been so chosen that π_2, π_3 belong to the same ideal class, $\pi_2 \sim \pi_3$.

There are now two possibilities with respect to π and π'. (i) Both π and π' may be principal ideals, and (ii) π and π' may be non-principal ideals belonging to different ideal classes.

(i) If π is a principal ideal

$$\pi = (\tfrac{1}{2}a+\tfrac{1}{2}b\omega) \quad (a-b \text{ even}),$$

and

$$4p = \pi\pi' = a^2+23b^2,$$

so that

$$a^2-b^2 = 4(p-6b^2),$$

which shows that a and b must both be even, since if they were both odd a^2-b^2 would be $\equiv 0 \pmod 8$. Hence

$$p = h^2+23k^2, \tag{4.4}$$

* In the case of a prime $p \equiv 7 \pmod 8$ the class number is $\sum_{r=1}^{\frac{1}{2}(p-1)} \left(\frac{r}{p}\right) = 7-4 = 3$, in the case $p = 23$. See also E. Hecke, *Theorie der algebraischen Zahlen* (1923), 177–178.

and since decomposition into prime ideal factors is unique there is only one solution in positive integers of (4.4). Thus in this case

$$24p = (1+\omega)(1-\omega)(h+k\omega)(h-k\omega),$$

and (4.2) has the two solutions[*]

$$u = h+23k,\quad v = |h-k|;\qquad u = |h-23k|,\quad v = h+k.$$

In both cases one of the two congruences

$$u+v \equiv 0 \pmod{24},\qquad u-v \equiv 0 \pmod{24}$$

is satisfied; hence, in (4.11), m and n are either both even or both odd, and it follows from (4.1) that

(4.5) $$c_p = 2.$$

(ii) If π and π' are non-principal ideals we may choose that solution r of (4.31) for which

$$\pi_2 \sim \pi_3 \sim \pi,\qquad \pi_2' \sim \pi_3' \sim \pi'.$$

It then follows that $\pi_2'\pi$, $\pi_3'\pi$, $\pi_2\pi_3\pi$ are principal ideals, so that $8p$, $12p$, and $24p$ are expressible in the form u^2+23v^2, each in one way only. The case which is of interest here is

$$\pi_2\pi_3\pi = \left(\frac{3+3\omega}{2},\ 1-\omega\right)\left(p,\ \frac{2r+23+\omega}{2}\right) = \left(\frac{u+v\omega}{2}\right),$$

where u and v satisfy (4.2). It follows that integers h and k, h' and k' exist such that

$$\frac{3p+3p\omega}{2} = \frac{h+k\omega}{2}\,\frac{u+v\omega}{2},\qquad p-p\omega = \frac{h'-k'\omega}{2}\,\frac{u+v\omega}{2},$$

whence, using (4.2),

$$(u-v\omega)(1+\omega) = 4(h+k\omega),$$

$$(u-v\omega)(1-\omega) = 6(h'-k'\omega),$$

from which it follows that

$$u-v = 4k,\qquad u+v = 6k',$$

[*] Since $h^2-k^2 = p-24k^2$, it follows that both $h+k$ and $h-k$, and therefore also $h-23k$ and $h+23k$, are prime to 6; that is to say both pairs of values of u and v are of the form $6n\pm 1$.

so that either*

$$u = 6n+1, \quad v = 6m-1, \quad \text{or} \quad u = 6n-1, \quad v = 6m+1,$$

and $$3n-3m\pm 1 = 2k.$$

Thus $m+n$ is odd, and from (4 . 1)

$$c_p = -1. \tag{4.6}$$

Proof of the theorem.

5. So far the proof has been purely algebraic. We have now to make use of the relations

$$\tau(mn) = \tau(m)\tau(n), \quad \text{if } m \text{ is prime to } n, \tag{5.1}$$

$$\tau(np^2)-\tau(p)\tau(np)+p^{11}\tau(n) = 0, \quad \text{if } p \text{ is prime,} \tag{5.2}$$

which were conjectured by Ramanujan and proved by Mordell† by means of the theory of the modular functions.

(i) If p is a quadratic non-residue of 23,

$$\tau(p) \equiv 0 \quad \text{and} \quad p^{11} \equiv -1 \pmod{23};$$

hence, if n is prime to p,

$$\tau(np^{2k}) \equiv \tau(n), \quad \tau(np^{2k+1}) \equiv 0 \pmod{23}. \tag{5.31}$$

(ii) When $p = 23$, since $c_{23} = 1$, it follows from (5 . 1) and (5 . 2) that

$$\tau(23^k n) \equiv \tau(n) \pmod{23}. \tag{5.32}$$

(iii) If p is a quadratic residue of 23, so that $p^{11} \equiv 1$, then either $\tau(p) \equiv -1$ or $\tau(p) \equiv 2 \pmod{23}$.

When $\tau(p) \equiv -1$ and n is prime to p, it follows from (5 . 1) and (5 . 2) that

$$\tau(np^{3k}) \equiv \tau(n), \quad \tau(np^{3k+1}) \equiv -\tau(n), \quad \tau(np^{3k+2}) \equiv 0 \pmod{23}. \tag{5.33}$$

When $\tau(p) \equiv 2$ and n is prime to p,

$$\tau(np^k) \equiv (k+1)\tau(n) \pmod{23}. \tag{5.34}$$

* From (4 . 2) we have
$$u^2-v^2 = 24(p-v^2),$$
from which it is obvious that u and v must both be prime to 6.

† *Proc. Camb. Phil. Soc.*, 19 (1920), 117-124.

The congruences (5.31)–(5.34), together with (4.5) and (4.6), are equivalent to the theorem stated.

The relation (5.34) is interesting because it shows that every number from 0 to 22 is a possible residue of $\tau(n)$ (mod 23). In particular

$$\tau(59^k) \equiv k+1 \pmod{23}.$$

The three tables which follow give: I, the least value of n, in each case, for which $\tau(n) \equiv k$ (mod 23) ($k = 0, 1, \ldots, 22$); II, the primes less than 1000 for which $\tau(p) \equiv -1$ (mod 23); and III, the primes less than 1000 which are expressible in the form a^2+23b^2, together with the corresponding values of a and b. For these primes $\tau(p) \equiv 2$ (mod 23).

TABLE I.

k	n	k	n	k	n	k	n
0	4	6	$59^2.101$	12	$59^2.101.167$	18	2.59^4
1	1	7	$2.59.101.167.173$	13	$2.59^4.101$	19	11918
2	59	8	$59.101.167$	14	$2.59^2.101^2$	20	6962
3	3481	9	$59^2.101^2$	15	$2.59.101.167$	21	118
4	5959	10	$59^4.101$	16	$59.101.167.173$	22	2
5	59^4	11	$2.59^2.101.167$	17	$2.59^2.101$		

TABLE II.

2	3	13	29	31	41	47	71	73	127	131
139	151	163	179	193	197	233	239	257	269	277
311	331	349	353	397	409	439	443	461	487	491
499	509	541	547	577	587	601	647	653	673	683
739	761	811	823	857	859	863	887	929	947	967

TABLE III.

p	a	b	p	a	b	p	a	b
59	6	1	347	18	1	821	27	2
101	3	2	449	9	4	829	1	6
167	12	1	463	16	3	853	5	6
173	9	2	593	15	4	877	7	6
211	2	3	599	24	1	883	26	3
223	4	3	607	20	3	991	28	3
271	8	3	691	22	3	997	13	6
307	10	3	719	12	5	3821	39	10
317	15	2	809	21	4	3853	55	6

Other congruence relations.

6. Precisely the same method may be applied in the case of the modulus 11. For let

$$\chi(x) = \{(1-x)(1-x^2)(1-x^3)\ldots\}^2$$
$$= \Sigma\Sigma(-)^n x^{\frac{3}{4}(m^2+n^2)+\frac{1}{2}m},$$

taken over all (positive and negative) integers such that $m+n$ is even. Then, as before,

$$f(x) \equiv x\chi(x)\,\chi(x^{11}) \pmod{11}.$$

But, although it is easy to compile a table of residues* of $\tau(n)$ (mod 11) for small values of n, there does not seem to be a general formula of any interest. The values of $n \leqslant 30$ for which $\tau(n) \equiv 0$ (mod 11) are 8, 19, 24, 29.

It was known to Ramanujan† that

$$\tau(n) \equiv n\sigma(n) \pmod{5},$$

where $\sigma(n)$ is the sum of the divisors of n; in particular, if p is prime,

$$\tau(p) \equiv p(p+1) \pmod{5}.$$

And it is easy to deduce‡ from a formula which he gives that

$$\tau(p) \equiv p^{11}+1 \pmod{691}.$$

* The computation of such a table is much facilitated by using an explicit formula for the coefficients in the expansion of $x\chi(x^{12})$, given by Ramanujan, *Trans. Camb. Phil. Soc.*, 22 (1916), 159–184, Equation (119) (*Collected papers*, No. 18), and proved by Mordell, *Proc. Camb. Phil. Soc.*, 19 (1920), 117–124 (121). [*November*, 1929. In a brief note, "Congruence properties of Ramanujan's function $\tau(n)$ to the modulus 11", which will appear in Dr. Baidaff's *Boletin Matematico* early in 1930, I have given a table of residues of $\tau(p)$ (mod 11) for prime $p \leqslant 257$. The only primes in the table for which $\tau(p) \equiv 0$ are 19, 29, and 199.]

† This is evident from a quotation made by Miss G. K. Stanley, *Journal London Math. Soc.*, 3 (1928), 232–237 (§ 3), from an unfinished manuscript by Ramanujan.

‡ J. R. Wilton, "On Ramanujan's arithmetical function $\Sigma_{r,s}(n)$", *Proc. Camb. Phil. Soc.*, 25 (1929), 255–264. In this paper, proofs are given of the two congruences

$$\tau(n) \equiv n\sigma(n) \pmod{5},$$
$$\tau(n) \equiv \sigma_{11}(n) \pmod{691},$$

where $\sigma_{11}(n)$ is the sum of the eleventh powers of the divisors of n.

Thus, if p is a quadratic non-residue of 23,

$$\tau(p) \equiv p^{11}+1 \pmod{15893}.$$

The information given by the congruences which have been established is quite considerable. For example*, in the case of $\tau(19)$, we have

$$\tau(19) \equiv 0 \pmod{5}, \quad \equiv 0 \pmod{7}, \quad \equiv 0 \pmod{11}, \quad \equiv 0 \pmod{23},$$

$$\tau(19) \equiv -19 \pmod{691}.$$

Thus $$\tau(19) \equiv 4542615 \pmod{6118805}.$$

Ramanujan gives $$\tau(19) = 10661420.$$

[*] I have chosen $n = 19$ as being particularly favourable for calculation, but for every n for which the residue of $\tau(n)$ (mod 11) has been calculated, the theorems which have been proved are sufficient to determine the residue of $\tau(n)$ (mod 6118805).